Finitely Supported Mathematics
An Introduction
Finitely Supported Mathematics
Finitely Supported Mathematics
An Introduction
# Contents

1 **Introduction** .................................................. 1  
1.1 Motivation .................................................. 1  
1.2 Approaches Related to the Fraenkel-Mostowski Framework ....... 5  
1.3 Finitely Supported Mathematics ................................ 7  
1.4 Outline ................................................... 9  

2 **Fraenkel-Mostowski Set Theory: A Framework for Finitely Supported Mathematics** ........................................ 11  
2.1 Axiom of Choice ........................................... 11  
2.2 Permutative Renaming .................................... 15  
2.3 Sets with Atoms ........................................... 17  
2.4 Constructions of Sets with Atoms ............................. 19  
  2.4.1 Powersets ........................................... 19  
  2.4.2 Cartesian Products .................................... 20  
  2.4.3 Disjoint Unions ...................................... 20  
  2.4.4 Function Spaces ..................................... 21  
  2.4.5 Categorical Constructions ......................... 24  
2.5 Fraenkel-Mostowski Axioms ................................ 24  
2.6 Logical Notions in the FM Cumulative Universe ............... 28  
2.7 Inconsistency of Choice Principles .......................... 30  
2.8 Finiteness ................................................ 39  
2.9 Freshness ............................................... 41  
2.10 Abstraction ................................................ 43  
  2.10.1 Formal Definition .................................... 43  
  2.10.2 Motivation ......................................... 44  
  2.10.3 Properties ......................................... 46  

3 **Algebraic Structures in Finitely Supported Mathematics** ...... 49  
3.1 Multisets in Finitely Supported Mathematics .................... 49  
  3.1.1 Algebraic Properties of Multisets .................. 50  
  3.1.2 Multisets over Infinite Alphabets ................... 54
# Subject Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.3 An Extension of the Framework</td>
<td>60</td>
</tr>
<tr>
<td>3.2 Generalized Multisets in Finitely Supported Mathematics</td>
<td>62</td>
</tr>
<tr>
<td>3.2.1 Algebraic Properties of Generalized Multisets</td>
<td>63</td>
</tr>
<tr>
<td>3.2.2 Generalized Multisets over Infinite Alphabets</td>
<td>73</td>
</tr>
<tr>
<td>3.3 Order Theory in Finitely Supported Mathematics</td>
<td>77</td>
</tr>
<tr>
<td>3.3.1 Partially Ordered Sets</td>
<td>78</td>
</tr>
<tr>
<td>3.3.2 Galois Connections</td>
<td>83</td>
</tr>
<tr>
<td>3.3.3 Rough Set Approximations</td>
<td>87</td>
</tr>
<tr>
<td>3.3.4 Abstract Interpretation</td>
<td>90</td>
</tr>
<tr>
<td>3.3.5 Calculability: Approximations of Fixed Points</td>
<td>95</td>
</tr>
<tr>
<td>3.3.6 Complete Partially Ordered Sets</td>
<td>100</td>
</tr>
<tr>
<td>3.3.7 Recursive Equations over CPOs</td>
<td>104</td>
</tr>
<tr>
<td>3.4 Groups in Finitely Supported Mathematics</td>
<td>105</td>
</tr>
<tr>
<td>3.4.1 Basic Results</td>
<td>106</td>
</tr>
<tr>
<td>3.4.2 Isomorphism Theorems</td>
<td>109</td>
</tr>
<tr>
<td>3.4.3 Embedding Theorems</td>
<td>112</td>
</tr>
<tr>
<td>3.4.4 Finitely Supported Subgroups</td>
<td>115</td>
</tr>
<tr>
<td>3.5 General Comments</td>
<td>120</td>
</tr>
<tr>
<td>3.6 Comments on the Methods Used in This Chapter</td>
<td>123</td>
</tr>
<tr>
<td>3.7 Conclusion</td>
<td>125</td>
</tr>
<tr>
<td>4 Extended Fraenkel-Mostowski Set Theory</td>
<td>129</td>
</tr>
<tr>
<td>4.1 Axioms of Extended Fraenkel-Mostowski Set Theory</td>
<td>129</td>
</tr>
<tr>
<td>4.2 Inconsistency of the Axiom of Choice</td>
<td>132</td>
</tr>
<tr>
<td>4.3 Algebraic Properties of EFM Sets</td>
<td>133</td>
</tr>
<tr>
<td>4.4 Topological Properties of EFM Sets</td>
<td>138</td>
</tr>
<tr>
<td>4.4.1 Subgroup Lattices as Domains</td>
<td>138</td>
</tr>
<tr>
<td>4.4.2 Scott Topology over the Subgroup Lattice of a Group</td>
<td>139</td>
</tr>
<tr>
<td>4.4.3 Topological Properties of the Group of Permutations of Atoms in EFM Set Theory</td>
<td>142</td>
</tr>
<tr>
<td>4.5 Renamings in the Extended Fraenkel-Mostowski Framework</td>
<td>144</td>
</tr>
<tr>
<td>4.6 Comments</td>
<td>148</td>
</tr>
<tr>
<td>5 Process Calculi in Finitely Supported Mathematics</td>
<td>151</td>
</tr>
<tr>
<td>5.1 Introduction and Methods</td>
<td>151</td>
</tr>
<tr>
<td>5.2 A Case Study: The Monadic Fusion Calculus</td>
<td>152</td>
</tr>
<tr>
<td>5.3 FSM Semantics of the Fusion Calculus</td>
<td>156</td>
</tr>
<tr>
<td>5.4 FSM Semantics of Other Process Calculi</td>
<td>168</td>
</tr>
<tr>
<td>5.4.1 FSM Semantics of the π-calculus</td>
<td>168</td>
</tr>
<tr>
<td>5.4.2 FSM Semantics of the π₁-calculus</td>
<td>173</td>
</tr>
<tr>
<td>5.5 Comments</td>
<td>177</td>
</tr>
</tbody>
</table>

References 179
Acknowledgements

This book has developed out of a series of papers written during the last six years. We are grateful to the anonymous referees for the opportunity to know their views, for their comments and suggestions which improved our results and presentation.

We are grateful to our scientific ancestors and mentors who paved the path to this book, great scientists upon whose shoulders we stand. We thank all who helped us to advance in our research. In particular, our colleagues from the Formal Methods Laboratory in Iași. For several useful comments and valuable help in the preparation of the manuscript, we express our gratitude to Bogdan Aman.

We would like to thank Ronan Nugent and his team at Springer for their kind collaboration and assistance in the final stage of preparation.

Last but not least, special thanks go to our families and friends for their support and encouragement.
Chapter 1

Introduction

Abstract We start this chapter by presenting some motivation for using nominal sets and Fraenkel-Mostowski sets in the experimental sciences. We emphasize the subdivisions of the so-called Fraenkel-Mostowski framework by mentioning the Fraenkel-Mostowski permutation model of Zermelo-Fraenkel set theory with atoms, the Fraenkel-Mostowski axiomatic set theory, the theory of nominal sets, the theory of generalized nominal sets, and Extended Fraenkel-Mostowski set theory. Finally, we present an alternative mathematics for managing infinite structures in the experimental sciences. This is called Finitely Supported Mathematics and represents, informally, Zermelo-Fraenkel mathematics rephrased in terms of finitely supported structures.

1.1 Motivation

There does not exist a full philosophical consensus on the distinction between logical and non-logical notions. This fact leads to certain doubts regarding our understanding of the nature of logic and its relationship to mathematics. Some logicians have suggested that what is distinctive about logical notions is their invariance under permutations of the domain of objects. In order to clarify this invariance under permutations, we mention that the set of numbers between 1 and 9 is invariant under the permutation of these numbers (it does not matter how we switch these numbers, we end up with the same set), but the set of prime numbers between 1 and 9 is not invariant under any permutation of these first 9 numbers (for instance, the related set formed by 2, 3, 5 and 7 is not invariant under the permutation that switches numbers 5 and 8 and maps all the other numbers to themselves).

In a logical sentence, signs for negation, conjunction, disjunction and the quantifiers should be invariant under any permutation of words, and so they count as logical notions (or logical constants), while words like “dog”, “tall” and “blue” cannot be invariant under permutations of (a larger set of) words, and so they are not logical notions. The invariance criterion seems to fit with common intuition about
logical notions. Certain technical results increase our confidence in this invariance criterion: in [152] it is proved that all of the relations definable in the language of Principia Mathematica are invariant under permutations, while in [111] every permutation-invariant operation can be defined in terms of logical operations such as identity, variable substitution, disjunction, negation and existential quantification, and each operation so definable is invariant under permutations.

Alfred Tarski gave a lecture in 1966 for a general audience at Bedford College in London entitled “What are logical notions?” Tarski’s answer to this question is presented in [153]. Essentially, logical notions are considered to be relations between individuals and classes, as well as relations over an arbitrary non-empty domain D of individuals. Tarski identified logical relations as exactly those invariant under arbitrary permutations of D. This thesis characterizes logical notions and logical operations by invariance under permutations.

As Tarski himself pointed out, the permutation invariance criterion for logical notions can be seen as a generalization of Felix Klein’s idea that different geometries can be distinguished by the groups of transformations under which their basic notions are invariant [96]. In his Erlangen Program, Klein classified the notions to be studied in various geometries (such as Euclidean, affine and projective geometry) according to the groups of (one-one and onto) transformations under which they are invariant. With logic thought of as the most general theory, logical notions should be those invariant under the largest group of transformations, namely the class of permutations. The “generality” argument for Tarski’s thesis is given by Bonnay in [49]:

1. The distinctive feature of logic among other theories is that it is the most general theory one can think of.
2. The bigger the group of transformations associated with a theory, the more general the theory.
3. The biggest group of transformations is the class of all permutations.

Thus, it is concluded that logical notions are those invariant under permutation.

Tarski’s thesis and related results assimilate logical notions to mathematics. From Whitehead and Russell’s Principia Mathematica, we know that the whole of mathematics can be formalized within set theory. In [152], set theory is described as a mathematically universal language. For Tarski, this universality gives set theory a fundamental status in mathematics and meta-mathematics, and so the whole of mathematics can be expressed in the language of an appropriate set theory. In Tarski’s words, “... we need only one non-logical constant (...) for a two-termed relation which holds between an element and a set (...). Then the only concern lies in a careful selection of the axioms. They must be weak enough to escape the antinomies, but at the same time they must be strong enough to ensure, within our universe of discourse, the existence of sets which correspond to as large a class of sentential functions as possible.”

Logical operations and notions in Tarski’s sense meet the permutation invariance criterion. If they are described set-theoretically, they should have the same meaning (independent of the set-theoretical universe). In considering an appropriate set theory for them, we take into account that if semantic concepts cannot be reduced to
1.1 Motivation

Logical concepts, we cannot proceed in “harmony with the postulates of the unity of science and of physicalism”, and so Tarski preferred to link mathematical universality to domain universality [152].

We relate all these aspects to the recently developed Fraenkel-Mostowski (FM) set theory [74]. Our goal is to establish a connection between the concept of logical notions in Tarski’s sense and the sets from the Fraenkel-Mostowski universe. The main aspect is related to the interpretation of a theory as its invariance under permutations of the universe; this means that the theory does not distinguish individual objects and characterizes only those properties of a model which do not depend on its non-structural transformations.

In this book we present a start point for a future presentation of a logical notion of set, and of an appropriate theory. Inspired by FM set theory we develop a theory of invariant sets and invariant algebraic structures. In order to realize our goal we also involve and extend the theory of nominal sets [127].

The theory of nominal sets (which we call invariant sets) has its origins in an approach developed initially by Fraenkel and Mostowski in the 1930s [68, 106], in order to prove the independence of the axiom of choice and other axioms in classical Zermelo-Fraenkel (ZF) set theory. In the 2000s, the FM permutation model of Zermelo-Fraenkel set theory with atoms (ZFA) was axiomatized and presented as an independent set theory with atoms, named FM set theory [74]. The axioms of FM set theory are the ZFA axioms over an infinite set of atoms [74], together with the special axiom of finite support which claims that for each element $x$ in an arbitrary set we can find a finite set supporting $x$. Rather than using a non-standard set theory, one could alternatively work with nominal sets [127], which are defined within ZF as usual sets endowed with some group actions satisfying a finite support requirement. In some papers, the theory of nominal sets is also called Fraenkel-Mostowski (FM) set theory. While we emphasize some differences between the related theories in Section 1.2, we agree that all these theories belong to the FM framework.

In computer science, nominal sets were first used in order to properly model the syntax of formal systems involving variable-binding operations [74]; the finiteness property in the definition of nominal sets is motivated by the fact that syntax can involve only finitely many names. Nominal sets also serve as a good framework for database theory since atoms can be used as an abstraction for data values, which can appear in a relational database or in an XML document. Atoms can also be used to model sources of infinite data in other applications, such as software verification, where an atom can represent a pointer or the contents of an array cell. Atoms have the same properties as variables and names. The precise nature of names is unimportant since we focus only on their ability to identify and on their distinctness. The nominal sets approach became successful since it provides a balance between rigorous formalism and informal reasoning. This is illustrated in [126] where principles of structural recursion and induction are explained in the world of nominal sets.

Starting from the development in [74] where the FM permutative model of ZFA set theory is redefined/axiomatized for computer science, nominal sets found a lot of other applications in various areas of the experimental sciences. New nominal semantics for various process calculi were defined in [5, 6, 9, 11, 13]. The tran-
sition rules in the nominal semantics of the related process calculi are expressed compactly, using a mixing of quantifiers instead of side conditions. This means the freshness conditions in the transition rules are successfully eliminated by using a specific freshness quantifier. The nominal semantics and the usual semantics of the related process calculi have the same expressive power. Nominal sets theory was also applied to the theory of process calculi in [37], where the π-calculus was formalized in Isabelle using the nominal datatype package [157].

Nominal sets were independently rediscovered by the concurrency community, as a basis for syntax-free models of name-passing process calculi [110], and used in automata theory as a framework for describing automata on data words [45]. An extension of the notion of nominal set from [126] was used in [45] to minimize automata over infinite alphabets, such as Francez-Kaminski finite-memory automata [69]. The minimization of deterministic timed automata [27] was studied in [47] using a class of atoms represented by real numbers. History-dependent automata (HD-automata) described in [110] and [124] have been developed in order to check π-calculus expressions for bisimilarity. HD-automata are internal (in the sense of [29]) in the category of named sets [54] which is equivalent to the category of nominal sets according to [67, 75]). In [102] formal languages over infinite alphabets where words may contain binders are introduced. HD-automata are extended by adding stacks, and the recognizability of nominal languages is studied.

In [40] the monoids defined in the category of nominal sets (also called nominal monoids) are used in the study of languages (without binders) over infinite alphabets. The theory of syntactic monoids for languages of data words represents the same theory as the theory of finite monoids in the category of nominal sets, and under certain conditions, a language of data words is definable in first-order logic if and only if its syntactic monoid is aperiodic [42]. Techniques from the theory of nominal sets are used in [142] in order to implement a functional programming language incorporating facilities for manipulating syntax involving names and binding operations. Computation in nominal sets has also been defined in [44] by presenting a basic functional programming language called Nλ. An imperative programming language which extends while programs and works with nominal sets is introduced in [48]. Unlike in Nλ, in the programming language presented in [48] the author was able to correctly type a program for minimizing the deterministic orbit-finite automata introduced in [45]. Turing machines that operate over infinite alphabets whose letters are built of atoms that can only be tested for equality are studied in [46]. In this direction it is proved that deterministic Turing machines are strictly less expressive than nondeterministic ones.

A more recent paper [43] studies a variant of first-order logic in the framework of nominal sets and presents a notion of model for this logic (the so-called stratified models) which admits compactness. Nominal algebraic structures are presented in terms of finitely supported objects in [4, 8, 10, 14]. The Scott recursive domain equation \( D \cong (D \to D) \) has been investigated in the nominal framework in [141]. Nominal sets have also been used in game theory [2], in logic [73, 125], in topology [123] and in proof theory [157].
1.2 Approaches Related to the Fraenkel-Mostowski Framework

Although the nominal sets were introduced by Gabbay and Pitts, an earlier idea of using atoms in computer science belongs to Gandy [76]. Gandy proved that any machine satisfying four physical ‘principles’ is equivalent to some Turing machine. Gandy’s four principles define a class of computing machines, namely the ‘Gandy machines’. Gandy machines are represented by classes of ‘states’ and ‘transition operations between states’. States are represented by hereditary finite sets built up from an infinite set $U$ of atoms, and transformations are given by restricted operations from states to states. The class $HF$ of all hereditary finite sets over $U$ introduced in Definition 2.1 from [76] is described quite similarly to the von Neumann cumulative hierarchy of FM sets presented in Section 2.5 of this book. The single difference between these approaches is that each $HF_{n+1}$ is defined inductively involving ‘finite subsets of $U \cup HF_n$’, whilst each $FM_{\alpha+1}(A)$ is defined inductively by using ‘the disjoint union between $A$ and the finitely supported subsets of $FM_\alpha(A)$’; $HF$ is the union of all $HF_n$ (with the remark that the empty set is not used in this construction), and the family of all FM sets is the union of all $FM_\alpha$ from which we exclude the set $A$ of atoms. The support of an element $x$ in $HF$, obtained according to Definition 2.2(1) from [76], coincides with $\text{supp}(x)$ (with notations from Theorem 2.4) if we see $x$ as an FM set. Also, the effect of a permutation $\pi$ on a structure $x$ described in Definition 2.3 from [76] is defined analogously to the application of the $S_A$-action on $FM(A)$ to the element $(\pi, x) \in S_A \times FM(A)$. Obviously, Gandy’s principles can also be presented in the FM framework because any finite set is well defined in FM; however, an open problem regards the consistency of Gandy’s principles when ‘finite’ is replaced by ‘finitely supported’.

The construction of the universe of all FM sets (i.e. sets constructed according to the FM axioms) [74] is inspired by the construction of the universe of all admissible sets over an arbitrary collection of atoms [36]. The hereditary finite sets used in [76] are particular examples of admissible sets. The FM sets represent a generalization of hereditary finite sets because any FM set is an hereditary finitely supported set.

1.2 Approaches Related to the Fraenkel-Mostowski Framework

In the literature there exist some different approaches regarding the FM framework. We need to clarify the differences between these approaches.

1. **FM permutation model of ZFA set theory.** This model was introduced by Fraenkel [68] and extended by Lindenbaum and Mostowski [106]. Its original aim was to establish the independence of the axiom of choice from the other axioms of ZF set theory. There also exist several other permutations models of ZFA set theory [95] (such as Fraenkel’s basic and second model or Mostowski’s ordered model), which are defined by using countable infinite sets of atoms.

2. **FM axiomatic set theory.** This set theory was presented by Gabbay and Pitts [74] in order to provide a new formalism for managing fresh names and bindings. An advantage of modelling syntax in a model of FM set theory is that datatypes of syntax modulo $\alpha$-equivalence can be modelled inductively. This is
because FM set theory provides a model of variable symbols and $\alpha$-abstraction. FM axiomatic set theory is inspired by the FM permutation model of ZFA set theory. However, FM set theory, ZFA set theory and ZF set theory are independent axiomatic set theories. All of these theories are described by axioms and all of them have models. For example the Cumulative Hierarchy Fraenkel-Mostowski universe $FM(A)$ presented in Section 2.5 is a model of FM set theory, whilst some models of ZF set theory can be found in [92] and the permutation models of ZFA set theory can be found in [95]. The sets defined by using the FM axioms are called FM sets. A ZFA set is an FM set if and only if all its elements have hereditary finite supports. Note that the infinite set of atoms in FM set theory is not necessary countable. FM set theory is consistent whether the infinite set of atoms is countable or not. Gabbay and Pitts use a countable set of atoms in order to define a model of FM set theory for computer science [74], whilst Bojanczyk describes FM sets over a set of atoms which does not represent a homogeneous structure [41]. Also, in [47] Bojanczyk and Lasota use non-countable sets of atoms (like the set of real numbers) in order to study the minimization of deterministic timed automata introduced in [27].

3. Nominal sets. The theory of nominal sets represents a ZF alternative to FM set theory. These sets can be defined both in the ZF framework [127] and in the FM framework [74]. In ZF, fix an infinite set $A$, and call it the set of names. A nominal set is defined as a usual ZF set endowed with a particular group action of the group of permutations of $A$ that satisfies a certain finite support requirement. There exists also an alternative definition for nominal sets in the FM framework (when the set of names is related to the set of atoms in FM). They can be defined as sets constructed according to the FM axioms with the additional property of being empty supported (invariant under all permutations). These two ways of defining nominal sets finally lead to similar properties. According to the previous remark, we will use the terminology “invariant” for “nominal”, in order to establish a connection between the approaches in the FM framework and in the ZF framework, respectively. Another reason for choosing the terminology “invariant” instead of “nominal” is presented in Section 2.6. Moreover, we can say that any set defined according to the FM axioms (any FM set) can be seen as a subset of the nominal set $FM(A)$. However, an FM set is itself a nominal set only if it has an empty support. The theory of nominal sets makes sense even if the set of atoms is infinite and not countable. Informally, since ZFA set theory collapses into ZF set theory when the set of atoms is empty, we can say that the nominal sets represent a natural extension of sets. In computer science, nominal sets offer an elegant formalism for describing $\lambda$-terms modulo $\alpha$-conversion [74]. Informally, we can think of the elements of a nominal set as having a finite set of free names. The action of a permutation on such an element actually represents the renaming of the free names. Nominal sets are also used in algebra [14, 18], in semantics [5, 6, 11, 13], in logic [125], in topology [123], in proof theory [157], in programming [142], and in domain theory [141], [156]. A model of predicate logic defined by using nominal sets is presented in [62]. A survey of the applications of nominal sets in computer science can be found in [15].
4. **Generalized nominal sets.** The classical theory of nominal sets over a fixed set $A$ of atoms is generalized in [45] to a new theory of nominal sets over arbitrary unfixed sets of data values (which we call generalized nominal sets). The notion of ‘$S_A$-set’ (in Definition 2.2) is replaced by the notion of ‘set endowed with an action of a subgroup of the symmetric group of $D$’ for an arbitrary set of data values $D$, and the notion of ‘finite set’ is replaced by the notion of ‘set with a finite number of orbits according to the previous group action (orbit-finite set)’. This approach is useful for studying automata on data words [45], languages over infinite alphabets [42], or Turing machines that operate over infinite alphabets [46]. Computations in these generalized nominal sets is defined in [48], [44].

5. **Extended Fraenkel-Mostowski axiomatic set theory (EFM).** This set theory is introduced in [7] and represents an extension of FM set theory obtained by replacing the finite support axiom with a consequence of it which states that any subset of the set $A$ of atoms is either finite or cofinite. Thus, in EFM, the finite support axiom is replaced by requiring only an amorphous structure on $A$. Even if the finite support axiom from FM set theory is relaxed in EFM set theory, many properties of the group of all bijections of $A$, such as torsioness or locally finiteness, are preserved [7]. EFM set theory has been used in [16] in order to generalize the notion of permutative renaming introduced in Section 2 from [74].

### 1.3 Finitely Supported Mathematics

Since the experimental sciences are mainly interested in quantitative aspects, and since there exists no evidence for the presence of infinite structures, it becomes more useful to develop a mathematics which deals with a more relaxed notion of infiniteness. We present our attempt to build the necessary concepts and structures for a finitely supported mathematics.

Finitely Supported Mathematics (FSM) is introduced in this book in order to prove that many ZF finiteness properties still remain valid if we replace the term ‘finite’ with ‘infinite, but with finite support’. Some results of this type have already been presented in [18], where we proved that a class of multisets over infinite alphabets (interpreted in the framework of nominal sets) has similar properties to the classical multisets over finite alphabets. The main aim of FSM is to characterize infinite algebraic structures using their finite supports.

As their name says, nominal sets are used especially in order to manage notions like renaming, binding or fresh name. We see a new possibility of using the theory of nominal sets in order to characterize some infinite structures in terms of finitely supported objects.

FSM is ZF mathematics rephrased in terms of finitely supported structures, where the set of atoms has to be infinite (countable or not countable). ZF mathematics is actually Empty Supported Mathematics. In FSM, we use either ‘nominal sets’ (which from now on will be called ‘invariant sets’) or ‘finitely supported sets’ instead of ‘sets’. FSM is not at all the theory of nominal sets from [127] presented in a differ-
ent manner. However, the theory of nominal sets [127] could be considered as a tool for defining FSM which is, informally, a theory of ‘invariant algebraic structures’.

We do not employ axioms in order to describe FSM because FSM is already consistent with the ZF axioms. However, we describe FSM by using principles. The principles of constructing FSM (presented also in [17]) have historical roots in the definition of ‘logical notions’ in Tarski’s view [153]. The general principle of constructing FSM is that all the structures have to be invariant or finitely supported. So, as a general rule, we are not allowed to use in the proofs of the results of FSM any construction that does not preserve the property of finite support. This means we cannot obtain a property in FSM only by employing a ZF result without an appropriate proof presented according to the finite support requirement.

It is worth noting that every ZF set is a particular invariant set equipped with a trivial permutation action (Example 2.1(2)). Therefore, the general properties of invariant sets lead to valid properties of ZF sets. The converse is not always valid, namely not every ZF result can be directly rephrased in the world of invariant sets, in terms of finitely supported objects according to arbitrary permutation actions. This is because, given an invariant set $X$, there could exist some subsets of $X$ (and also some relations or functions involving subsets of $X$) which fail to be finitely supported. Therefore, the remark that everything that can be done in ZF can also be done in FSM is not valid. This means there may exist some valid results depending on several ZF structures which fail to be valid in FSM if we simply replace “ZF structure” with “FSM structure” in their statement.

Since invariant sets can be defined in the ZFA framework similarly as in the ZF framework (see the first paragraph in Section 2.3), the construction of FSM also makes sense over the ZFA axioms. Due to the connections between axiomatic FM set theory and the framework of nominal (invariant) sets, we find it convenient to say that FSM is the mathematics developed in the “FM framework”. Thus, the meaning of the term “FM framework” is “the framework used in order to construct a mathematics in which all the structures are finitely supported”. Obviously, anything that is constructed according to the FM axioms also makes sense in FSM.
1.4 Outline

The book is organized as follows:

**Chapter 2:** In this chapter we recall the basics of FM sets and invariant (nominal) sets as studied by Gabbay and Pitts in [71, 74, 127]. We review some basic notions from the FM framework like $S_A$-action, invariant (nominal) set, FM set, freshness (nominal) quantifier, support, finiteness, fresh element and abstraction. These notions are used in the following chapters. We also present some original results such as the relationship between the axioms of FM set theory and various forms of choice, and we prove some properties of invariant sets obtained by comparing various choice principles. Another goal of this chapter is to establish a connection between the theory of FM sets and the concept of logical notion presented by Tarski [153]. Concretely, we prove that any nominal set defined in the FM framework, i.e. any equivariant FM set, is a logical notion according to Tarski’s definition. Moreover, the freshness quantifier $\mathcal{N}$ is also a logical symbol.

**Chapter 3:** Our goal is to answer the question “Do we obtain valid results if we replace the notion of *infinite set* with the notion of *invariant/finitely supported set* in the classical ZF results?” In order to answer this question, we translate into FSM several algebraic concepts which were initially described using the axioms of ZF set theory. We focus on multisets, generalized multisets, partially ordered sets, Galois connections and groups because these are particularly relevant to the experimental sciences. The FSM properties of these algebraic structures are compared with their related ZF properties. We also develop a theory of abstract interpretation for programming languages within invariant sets, and we present some calculability results within finitely supported structures.

**Chapter 4:** We generalize FM set theory by giving a new set of axioms which defines Extended Fraenkel-Mostowski (EFM) set theory. The finite support axiom in FM set theory is replaced by a consequence of it which states only that each subset of the set $A$ of atoms is either finite or cofinite. Many algebraic and topological properties of sets which are valid in the FM framework remain valid in the EFM framework. Permutative renamings are defined and studied in the EFM framework.

**Chapter 5:** We describe an algorithm to define an FSM semantics for a certain process calculus. We present in detail the case of the fusion calculus. The transition rules of the FSM semantics of the fusion calculus are expressed compactly using the quantifier $\forall$ and the freshness quantifier $\mathcal{N}$ instead of the additional freshness conditions. Atoms are used to represent “names”, and FSM abstraction is used to replace the usual “binding operation”. According to the finite support requirement in FSM, we prove a complete equivalence between the new FSM semantics of the fusion calculus and the usual semantics of this process calculus.
Chapter 2
Fraenkel-Mostowski Set Theory: A Framework for Finitely Supported Mathematics

Abstract In this chapter we present the basics of the Fraenkel-Mostowski framework, by studying concepts like invariant set, Fraenkel-Mostowski set, freshness quantifier, support, finiteness, fresh element, and abstraction. We also prove some original results regarding the consistency of various forms of choice in Finitely Supported Mathematics. Another goal of this chapter is to establish a connection between the theory of Fraenkel-Mostowski sets and the concept of logical notion presented by A. Tarski. More precisely, we prove that any invariant set from the Fraenkel-Mostowski universe is a logical notion in Tarski’s view. Moreover, the freshness quantifier is a logical symbol.

2.1 Axiom of Choice

The Axiom of Choice (AC) is probably the most analyzed axiom in mathematics after Euclid’s Axiom of Parallels. The first formulation of AC is due to Zermelo [162]. It claims that given any family of non-empty sets \( \mathcal{F} \), it is possible to select a single element from each member of \( \mathcal{F} \). This statement is equivalent to the assertion that for any family of non-empty sets \( \mathcal{F} \), there exists at least one choice function on \( \mathcal{F} \), where a choice function on \( \mathcal{F} \) is a function \( f \) with domain \( \mathcal{F} \) such that, for each non-empty set \( X \) in \( \mathcal{F} \), \( f(X) \) is an element of \( X \). Zermelo’s purpose in introducing AC was to establish a central principle of Cantor’s set theory, namely, that every set admits a well-ordering and so can also be assigned a cardinal number. There are more than 200 mathematical results which are proved to be equivalent to the axiom of choice (see [95] and [135]) in the ZF (with the axiom of foundation) set theory. The best known are:

- The Cartesian product of a family of non-empty sets is non-empty;
- Every surjective function has a right inverse;
- For any family \( (X_i)_{i \in I} \) of non-empty sets there exists a family \( (F_i)_{i \in I} \) of non-empty, finite sets \( F_i \) with \( F_i \subseteq X_i \) for each \( i \in I \) (Axiom of multiple choice);
• Any non-empty inductive poset $P$ (i.e. any poset $P$ for which every totally ordered subset of $P$ has an upper bound in $P$) has a maximal element (Zorn’s lemma $\text{ZL}$);
• Each partially ordered set contains a maximal totally ordered subset (Hausdorff’s maximal principle);
• In the product topology, the closure of a product of subsets is equal to the product of the closures;
• Every partially ordered set has a maximal subset such that any two elements in the subset are incomparable (Antichain principle);
• Every set can be well-ordered (Zermelo’s well-ordering theorem);
• In any pair of cardinal numbers, one is less than the other, or they are equal (Trichotomy principle);
• The product of any family of compact topological spaces is compact (Tychonov’s theorem);
• Every vector space has a basis (Hamel’s theorem);
• For every infinite set $X$, there exists a bijective map between the sets $X$ and $X \times X$ (Tarski’s theorem);
• Every nontrivial ring $(R, +, \cdot, 1)$ contains a maximal ideal;
• Every lattice with a largest element has a maximal ideal;
• Every divisible module over a principal ideal domain is injective;
• Every infinite consistent set $\Sigma$ of first-order sentences has a model of cardinality no greater than that of $\Sigma$ (the model existence theorem for first-order logic).

Some weaker forms of the axiom of choice, also called choice principles, are collected in [88]:

• **Axiom of dependent choice (DC):** let $R$ be a non-empty relation on a set $X$ with the property that for each $x \in X$ there exists $y \in X$ with $xRy$. Then there exists a function $f : \omega \to X$ such that $f(n)Rf(n+1), \forall n \in \omega$;
• **Axiom of countable choice (CC):** given any countable family (sequence) of non-empty sets $\mathcal{F}$, it is possible to select a single element from each set of $\mathcal{F}$;
• **Axiom of partial countable choice (PCC):** given any countable family (sequence) of non-empty sets $\mathcal{F} = (X_n)_n$, there exists an infinite subset $M$ of $\mathbb{N}$ such that it is possible to select a single element from each member of the family $(X_m)_{m \in M}$;
• **Axiom of choice over finite sets (AC(fin)):** given any family of finite non-empty sets $\mathcal{F}$, it is possible to select a single element from each member of $\mathcal{F}$;
• **Axiom of countable choice over finite sets (CC(fin)):** given any countable family (sequence) of finite non-empty sets $\mathcal{F}$, it is possible to select a single element from each member of $\mathcal{F}$;
• **Axiom of partial countable choice over finite sets (PCC(fin)):** given any countable family (sequence) of non-empty finite sets $\mathcal{F} = (X_n)_n$, there exists an infinite subset $M$ of $\mathbb{N}$ such that it is possible to select a single element from each member of the family $(X_m)_{m \in M}$;
• **Boolean prime ideal theorem (PIT):** every Boolean algebra with $0 \neq 1$ has a maximal ideal (and hence a prime ideal);
2.1 Axiom of Choice

- **Boolean ultrafilter theorem (UFT)**: in a Boolean algebra, every filter can be enlarged to a maximal one;
- **Compactness of products of Hausdorff spaces (CPHS)**: products of compact Hausdorff spaces are compact;
- **Kinna-Wagner Selection Principle (KW)**: given any family $\mathcal{F}$ of sets of cardinality at least 2, there exists a function $f$ on $\mathcal{F}$ such that $f(X)$ is a non-empty proper subset of $X$ for each $X \in \mathcal{F}$;
- **Refinement of the Kinna-Wagner Selection Principle (RKW)**: given any set $X$ and the family $\mathcal{F}$ of all subsets of $X$ of cardinality at least 2, there exists a function $f$ on $\mathcal{F}$ such that $f(Y)$ is a non-empty proper subset of $Y$ for each $Y \in \mathcal{F}$;
- **Ordering principle (OP)**: every set can be totally ordered;
- **Order extension principle (OEP)**: every partial order relation on a set can be enlarged to a total order relation;
- **Axiom of Dedekind infiniteness (Fin)**: every infinite set $X$ allows an injection $i: \mathbb{N} \to X$.

According to [88], we have the following theorem:

**Theorem 2.1.** The following implications are valid in ZF set theory:

1. $\text{AC} \Rightarrow \text{DC} \Rightarrow \text{CC} \Leftrightarrow \text{PCC} \Rightarrow \text{CC(fin)}$;
2. $\text{PIT} \Leftrightarrow \text{UFT} \Leftrightarrow \text{CPHS}$;
3. $\text{AC} \Rightarrow \text{UFT} \Rightarrow \text{OEP} \Rightarrow \text{OP} \Rightarrow \text{AC(fin)} \Rightarrow \text{CC(fin)}$;
4. $\text{CC} \Rightarrow \text{Fin} \Rightarrow \text{PCC(fin)} \Rightarrow \text{CC(fin)}$;
5. $\text{KW} \Leftrightarrow \text{RKW} \Rightarrow \text{OP}$.

An important connection between AC and mathematical logic was established by Goodman and Myhill [82].

**Theorem 2.2.** AC implies the Law of Excluded Middle, which states that for any proposition, either that proposition is true, or its negation is true.

There exist a large number of results which cannot be proved without employing AC or the previous weaker versions of AC. We recall some of them. More details are and complete proofs can be found in [87, 88, 95, 134, 135]. We specify for each result which is the minimal form of choice required for its proof.

- The following definitions of finiteness are equivalent in ZF set theory with AC:
  1. $X$ is finite if it corresponds one-to-one and onto to a finite ordinal (usual finiteness);
  2. $X$ is finite if it has no injections into any of its proper subsets (Dedekind-Pierce finiteness);
  3. $\emptyset$ is finite, $\{x\}$ is finite for each $x$, if $X$ and $Y$ are finite then so is $X \cup Y$, and no other sets are finite (Kuratowski finiteness);
  4. $X$ is finite if every total ordering on it is a well-ordering (Tarski finiteness);
  5. $X$ is finite if for all increasing chains $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$ such that $X \subseteq \bigcup X_n$ there exists $n \in \mathbb{N}$ such that $X \subseteq X_n$;
6. $X$ is finite if for all directed collections $(X_i)_{i \in I}$ such that $X \subseteq \bigcup X_i$ there exists $i \in I$ such that $X \subseteq X_i$.

- Any union of countably many countable sets is itself countable – the proof requires $CC$;
- There exists a subset of the real numbers that is not Lebesgue measurable (Vitali’s theorem) – the proof requires $PIT$;
- In a metric space the notions of compactness and sequential compactness are equivalent (Bolzano-Weierstrass theorem) – the proof requires $CC$;
- Countable sums of Lindelof spaces are Lindelof – the proof requires $CC$;
- Every submodule of a free module over a principal ideal domain is also free (Kaplansky’s theorem) – the proof requires $ZL$;
- Every free left module is projective – the proof requires $AC$;
- Every field has an algebraic closure – the proof is a consequence of $PIT$;
- Every field extension has a transcendence basis – the proof requires $ZL$;
- Any automorphism of a subfield of an algebraically closed field $K$ can be extended to the whole of $K$ – the proof requires $ZL$;
- All bases of a vector space have the same cardinality – the proof requires $ZL$;
- Every linear functional $f$ defined on a subspace $U$ of a real vector space $V$ which is dominated by the sublinear function $p : V \to \mathbb{R}$ has a linear extension $F : V \to \mathbb{R}$ with the property that $F$ is dominated by $p$ on $V$ (Hahn-Banach theorem) – the proof requires a weaker form of $PIT$ which states that on every Boolean algebra there exists an additive, normed $[0, 1]$-valued measure;
- Every Hilbert space has an orthonormal basis – the proof requires $ZL$;
- Let $(X, \leq)$ be a poset, and $S : X \to \mathbb{R} \cup \{\infty\}$ a function. We assume that the following conditions are satisfied:
  1. Each increasing sequence $(x_n)$ in $X$ with the property that $(S(x_n))$ is strictly increasing is bounded;
  2. The function $S$ is increasing.

Then for each $x_0 \in X$ there exists $\bar{x} \in X$ such that $x_0 \leq \bar{x}$ and $S(x) = S(\bar{x})$ for each $x$ with the property that $\bar{x} \leq x$. (Brezis-Browder theorem) – the proof requires $DC$;
- Every complete metric space is a Baire space, i.e. a topological space with the property that the union of any countable collection of closed sets with empty interior has empty interior (Baire’s category theorem) – the proof requires $DC$;
- Every consistent set of first-order sentences can be extended to a maximal consistent set (Gödel’s completeness theorem) – the proof requires $PIT$;
- If every finite subset of a set of first-order sentences has a model, then the set has a model (Compactness theorem for first-order logic) – the proof requires $PIT$.

Many areas in mathematics, especially in functional analysis, real analysis, topology, the theory of differential equations, the theory of algebraic structures, measure theory, first-order logic, and category theory depend heavily on choice principles. The axiom of choice has a lot of elegant consequences, but this is an argument only for its mathematical interest and not for its correctness. Since its first postulation the axiom of choice became the subject of many controversies. The first controversy is
about the meaning of the word “exists” since this term is very vague. One group of mathematicians (called intuitionists) believes that a set exists only if each of its elements can be designated specifically or at least if there is a law by which each of its elements can be constructed. Another controversy is given by a geometrical consequence of AC known as Banach and Tarski’s paradoxical decomposition of the sphere. In [34] they showed that any solid sphere can be split into finitely many subsets which can themselves be reassembled to form two solid spheres, each of the same size as the original; and any solid sphere can be split into finitely many subsets in such a way as to enable them to be reassembled to form a solid sphere of arbitrary size. Questions about AC’s independence of the systems of set-theoretic axioms appeared naturally. In 1922 Fraenkel defined the permutation method to establish the independence of AC from a system of set theory with atoms [68]. That is, Fraenkel constructed a model in which the axioms of set theory excluding the axiom of choice are satisfied but this model contains a set which does not satisfy the axiom of choice. Fraenkel’s model was refined and extended by Lindenbaum and Mostowski [106], and, later, by Gabbay and Pitts [74] to what we call Fraenkel-Mostowski set theory. More precisely, Fraenkel-Mostowski set theory was initially given as a model of Zermelo-Fraenkel set theory with atoms. However, in [74] Fraenkel-Mostowski set theory was developed as an independent axiomatic set theory.

Fraenkel’s original permutation method was not sufficient to prove the independence of the axiom of choice from the axioms of ZF set theory. In [81] Gödel proved that the axiom of choice is consistent with the other axioms of set theory (von Neumann-Bernays-Gödel set theory). He proved that given a model for set theory in which there are no atoms and the axiom of foundation is true, there exists a model in which, in addition, the axiom of choice is true. Moreover, if Gödel’s model is modified so that either atoms exist or the axiom of foundation is false, the validity of the axiom of choice is not disturbed. Therefore, the axiom of choice is consistent with the other axioms of set theory regardless of whether atoms exist or not, and whether the axiom of foundation is valid or not. Fraenkel showed that the collections of sets of atoms need not necessarily have choice functions [68]. However, at that time he was unable to establish the same fact for the usual sets of mathematics, for example the set of real numbers. This problem remained unsolved until 1963 when Cohen proved the independence of AC (and of the axiom of countable choice) from the standard axioms of ZF set theory [55]. Cohen’s independence proof (known as the method of forcing) also made use of permutations in essentially the form in which Fraenkel had originally employed them.

### 2.2 Permutative Renaming

The example presented in this section gives us a good reason for working with FM set theory instead of classical ZF set theory.

Let us consider the terms $t$ of the untyped $\lambda$-calculus [35]:

$$t ::= a \mid tt \mid \lambda a.t$$
where $a$ ranges over an infinite set $A$ of names of variables. In this book the set $A$ will be fixed and its elements will be called atoms.

For $a,b \in A$ we consider the following three versions of the notion of variable renaming for $\lambda$-terms $t$:

- $[b|a]t$, the textual substitution of $b$ for all free occurrences of $a$ in $t$;
- $\{b|a\}t$, the capture-avoiding substitution of $b$ for all free occurrences of $a$ in $t$;
- $(ba) \cdot t$, the transposition of all occurrences (be they free, bound or binding) of $a$ and $b$ in $t$.

The $\alpha$-equivalence in the $\lambda$-calculus (denoted by $=_\alpha$) is defined as the least congruence on the set of $\lambda$-terms that identifies $\lambda a.t$ with $\lambda b.\{b|a\}t$. The notion of renaming defined by using transpositions can be used to characterize the $\alpha$-equivalence, as Theorem 2.3 shows. Moreover, when we work with this notion of renaming, we do not need to know whether any of the operations in the underlying signature for $\lambda$-terms are supposed to be variable-binders in order to define it.

**Theorem 2.3.** The relation $=_\alpha$ of $\alpha$-equivalence between $\lambda$-terms coincides with the binary relation $\sim$ inductively generated by the following axioms and rules:

\[
\begin{align*}
  a \in A & \quad t_1 \sim t_1', t_2 \sim t_2' \\
  a \sim a' & \quad t_1t_2 \sim t_1't_2' \\
  (ba) \cdot t & \sim (ba') \cdot t', b \neq a,a' \text{ and } b \text{ do not occur in } t,t' \\
  \lambda a.t & \sim \lambda a't'.
\end{align*}
\]

*Proof.* It is easy to check that $(ba) \cdot (-)$ preserves $=_\alpha$, and hence $=_\alpha$ is closed under the axioms and rules defining $\sim$. So, $\sim$ is contained in $=_\alpha$. The converse inclusion follows by proving that $\sim$ is a congruence relating $\lambda a.t$ and $\lambda b.\{b|a\}t$. This follows because $(ba) \cdot (-)$ preserves $\sim$, and, if $b$ does not occur in $t$, then $(ba) \cdot t \sim \{b|a\}t$.

The last result can easily be proved by induction on term size. $\square$

This theorem shows that matters to do with variable binding can be phrased in terms of the elementary operation of variable-transposition, $(ba) \cdot (-)$, rather than the more complicated operation of variable-substitution. Both textual and capture-avoiding substitution are more complicated that transposition because they depend on the auxiliary definition of what are the free variables of a term. Generally, we can define $\pi \cdot t$ to be the result of permuting the atoms in $t$ according to a bijection $\pi : A \rightarrow A$. As it is presented in [74], this ‘permutation action’ permits one to formalize an important abstractness property of meta-theoretic assertions involving the notion of ‘variable’, namely that the validity of assertions about syntactical objects should be sensitive only to distinctions between variable names, rather than to the particular names themselves. Formally, this represents the equivariance property of an assertion $p(t)$ about terms $t$ claiming that $\forall \pi,t.(p(t) \Leftrightarrow p(\pi \cdot t))$. The validity of the previous statement depends on the nature of the assertion $p(t)$.
Let $A$ be a fixed infinite (countable or non-countable) ZF set. The following results also make sense if $A$ is considered to be the set of atoms in the ZFA framework (characterized by the axiom “$y \in x \Rightarrow x \notin A$”) and if ‘ZF’ is replaced by ‘ZFA’ in their statement. Thus, we mention that the theory of invariant sets makes sense both in ZF and in ZFA. The results in this section are similar to those in [127], with the remark that we do not assume the set of atoms to be countable.

In Section 2.1 we proved that the equivalence of various definitions of finiteness is a consequence of AC. According to Theorem 2.13, AC is inconsistent in FSM. For the avoidance of doubt, where the word “finite” appears in this book without reference to any of the definitions of finiteness from Section 2.1, it means “it bijects with a finite ordinal”. More details are in Section 2.8.

Definition 2.1. i) A transposition is a function $(ab): A \to A$ defined by $(ab)(a) = b$, $(ab)(b) = a$ and $(ab)(n) = n$ for $n \neq a, b$.

ii) A permutation of $A$ is a bijection of $A$ which interchanges only finitely many elements.

Let $S_A$ be the set of all permutations of $A$; in our approach $S_A$ is not defined as the entire set of bijections on $A$, but as the set of those bijections on $A$ which leave unchanged all but finitely many elements of $A$. However, one can prove that a bijection on $A$ is finitely supported if and only if it leaves unchanged all but finitely many elements of $A$ (see Proposition 2.7). Therefore, in FSM any bijection on $A$ has to be a permutation in the sense of Definition 2.1.

We claim that any permutation of $A$ can be expressed by composing finitely many transpositions. Indeed, let $\sigma \in S_A$ be a function that permutes only a finite number of atoms $\{a_1, \ldots, a_n\}$ such that the atoms $A \setminus \{a_1, \ldots, a_n\}$ are left unchanged. Formally, we can say that $\sigma$ is a permutation of the set $\{a_1, \ldots, a_n\}$, and so $\sigma$ can be expressed as a product of at most $n - 1$ transpositions [133]. $S_A$ is a group under the usual composition of permutations. Actually, $S_A$ is a proper subgroup of the symmetric group on $A$; this is the reason why we chose to denote the set of finitary bijections on $A$ by $S_A$. The composition of permutations is denoted by $\circ$.

Definition 2.2. • Let $X$ be a ZF set. An $S_A$-action on $X$ is a group action of the group of permutations $S_A$ on the set $X$. More precisely, an $S_A$-action on $X$ is a function $\cdot: S_A \times X \to X$ having the properties that $Id \cdot x = x$ and $\pi \cdot (\pi' \cdot x) = (\pi \circ \pi') \cdot x$ for all $\pi, \pi' \in S_A$ and $x \in X$.

• An $S_A$-set is a pair $(X, \cdot)$ where $X$ is a ZF set and $\cdot: S_A \times X \to X$ is an $S_A$-action on $X$. We simply use $X$ whenever no confusion arises.

Definition 2.3. Let $(X, \cdot)$ be an $S_A$-set. We say that $S \subseteq A$ supports $x$ whenever for each $\pi \in \text{Fix}(S)$ we have $\pi \cdot x = x$, where $\text{Fix}(S) = \{ \pi \in S_A | \pi(a) = a, \forall a \in S\}$.

When for an element $x$ in an $S_A$-set we can find a finite set $S$ supporting it, we also say that “$x$ has the finite support property”, “$x$ is finitely supported” or “$x$ is $S$-supported”.
Definition 2.4. Let \( (X, \cdot) \) be an \( S_A \)-set. We say that \( X \) is an invariant set if for each \( x \in X \) there exists a finite set \( S_x \subset A \) which supports \( x \).

Invariant sets are also called nominal sets [127] (if we work in the ZF framework) or equivariant sets [74] (if they are defined as elements in the cumulative hierarchy \( FM(A) \)).

Theorem 2.4. Let \( X \) be an \( S_A \)-set, and for each \( x \in X \) let us define \( \mathcal{F}_x = \{ S \subseteq A | S \text{ finite, } S \text{ supports } x \} \). If \( \mathcal{F}_x \) is non-empty, then it has a least element. We call this element the support of \( x \), and we denote it by \( \text{supp}(x) \).

Proof. We define \( \text{supp}(x) = \cap \{ S \subseteq A | S \text{ finite, } S \text{ supports } x \} = \cap_{S \in \mathcal{F}_x} S \). We prove that if \( S_1 \) and \( S_2 \) are both finite and support \( x \), then \( S_1 \cap S_2 \) supports \( x \). Indeed, let \( \pi \) be a permutation from \( \text{Fix}(S_1 \cap S_2) \). We prove that \( \pi \cdot x = x \). Since any permutation \( \pi \) is generated by composing finitely many transpositions, it is enough to prove the finite support property of \( x \) only for transpositions. This means we must prove that for each \( a, b \notin S_1 \cap S_2 \) we have \( (ab) \cdot x = x \). The cases \( a, b \notin S_1 \) and \( a, b \notin S_2 \) are obvious because \( S_1 \) and \( S_2 \) support \( x \), and by Definition 2.3 we have \( (ab) \cdot x = x \). Now let \( a \notin S_1 \) and \( b \notin S_2 \). Since \( S_1 \cup S_2 \) is finite and \( A \) is infinite, we can find \( c \in A \setminus (S_1 \cup S_2) \) and \( a \neq c \neq b \). Since \( a, c \notin S_1 \) and \( S_1 \) supports \( x \), it follows that \( (ca) \cdot x = x \). Since \( c, b \notin S_2 \) and \( S_2 \) supports \( x \), we have \( (cb) \cdot x = x \). It follows that \( (ab) \cdot x = (ab) \cdot ((cb) \cdot x) = ((ab) \circ (cb)) \cdot x = ((cb) \circ (ac)) \cdot x = (cb) \cdot ((ac) \cdot x) = x \).

The case when \( a \notin S_2 \) and \( b \notin S_1 \) is similar. Therefore, \( \text{supp}(x) \) supports \( x \), and \( \text{supp}(x) \) is minimal among the finite sets supporting \( x \).

\( \square \)

Corollary 2.1. Let \( X \) be an invariant set, and for each \( x \in X \) define \( \mathcal{F}_x = \{ S \subseteq A | S \text{ finite, } S \text{ supports } x \} \). Then \( \mathcal{F}_x \) has a least element which also supports \( x \). We call this element the support of \( x \), and we denote it by \( \text{supp}(x) \).

Definition 2.5. Let \( (X, \cdot) \) be an invariant set. An element \( x \in X \) is called equivariant if it has an empty support, i.e. \( \pi \cdot x = x \) for each \( \pi \in S_A \).

Proposition 2.1. Let \( (X, \cdot) \) be an \( S_A \)-set, and let \( \pi \in S_A \) be an arbitrary permutation. Then for each finitely supported element \( x \in X \) we have that \( \pi \cdot x \) is finitely supported, and \( \text{supp}(\pi \cdot x) = \pi(\text{supp}(x)) \).

Proof. Let \( \pi \in S_A \) be an arbitrary permutation, and \( x \in X \) a finitely supported element. First we show that \( \pi(\text{supp}(x)) \) supports \( \pi \cdot x \). Let \( \sigma \in \text{Fix}(\pi(\text{supp}(x))) \). This means \( \sigma(\pi(a)) = \pi(a) \) for all \( a \in \text{supp}(x) \). Also \( \pi^{-1}(\sigma(\pi(a))) = \pi^{-1}(\pi(a)) = a \), \( \forall a \in \text{supp}(x) \). So we get \( \pi^{-1} \circ \sigma \circ \pi \in \text{Fix}(\text{supp}(x)) \). Now \( \text{supp}(x) \) always supports \( x \) (by Theorem 2.4). According to Definition 2.3, we have \( (\pi^{-1} \circ \sigma \circ \pi) \cdot x = x \).

Since \( \cdot \) is a group action and the composition of permutations is associative, the last equality is equivalent to \( \sigma \cdot (\pi \cdot x) = \pi \cdot x \). Hence whenever \( x \in X \) is finitely supported we have that \( \pi \cdot x \) is finitely supported. Moreover, \( \text{supp}(\pi \cdot x) \subseteq \pi(\text{supp}(x)) \) for each \( x \in X \) which is finitely supported and each \( \pi \in S_A \) (1). We now apply (1) for elements \( \pi^{-1} \in S_A \) and \( \pi \cdot x \in X \); we already know the latter is finitely supported.

We get \( \text{supp}(\pi^{-1} \cdot \pi \cdot x) \subseteq \pi^{-1}(\text{supp}(\pi \cdot x)) \). Composing with \( \pi \) in the last relation we obtain \( \pi(\text{supp}(x)) \subseteq \text{supp}(\pi \cdot x) \).

\( \square \)
Let have that \( X \) is finitely supported and \( \text{supp}(X) \) is called finitely supported if and only if \( \text{supp}(X) \) is an invariant set with \( \text{supp}(a) = \{a\} \) for each \( a \in A \).

2. The set \( A \) of atoms is an \( S_A \)-set with the \( S_A \)-action \( \cdot : S_A \times A \to A \) defined by \( \pi \cdot a := \pi(a), \forall \pi \in S_A, a \in A \). Moreover, \((A, \cdot)\) is an invariant set with \( \text{supp}(a) = \emptyset \) for each \( a \in A \).

3. The set \( S_A \) is an \( S_A \)-set with the \( S_A \)-action \( \cdot : S_A \times S_A \to S_A \) defined by \( \pi \cdot \sigma := \pi \circ \sigma \circ \pi^{-1}, \forall \pi, \sigma \in S_A \). Moreover, \((S_A, \cdot)\) is an invariant set with \( \text{supp}(\sigma) = \{a \in A | \sigma(a) \neq a\} \) for each \( \sigma \in S_A \).

4. Any ordinary ZF-set \( X \) (\( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \) or \( \mathbb{R} \), for example) is an \( S_A \)-set with the \( S_A \)-action \( \cdot : S_A \times X \to X \) defined by \( \pi \cdot x := x, \forall \pi \in S_A, x \in X \). Moreover, \( X \) is an invariant set with \( \text{supp}(x) = \emptyset \) for each \( x \in X \).

### 2.4 Constructions of Sets with Atoms

#### 2.4.1 Powersets

If \((X, \cdot)\) is a \( S_A \)-set, then \( \wp(X) = \{Y | Y \subseteq X\} \) is also an \( S_A \)-set with the \( S_A \)-action \( \star : S_A \times \wp(X) \to \wp(X) \) defined by \( \pi \star Y := \{\pi \cdot y | y \in Y\} \) for all permutations \( \pi \) of \( A \), and all subsets \( Y \) of \( X \). Note that \( \wp(X) \) is not necessarily an invariant set even if \( X \) is. For example \( A \) is an invariant set, but \( \wp(A) \) is not an invariant set because the subsets of \( A \) which are at the same time infinite and coinfinite are not finitely supported.

For each invariant set \((X, \cdot)\) we denote by \( \wp_{\text{fs}}(X) \) the set formed from those subsets of \( X \) which are finitely supported according to the action \( \star \). According to Proposition 2.1, \( (\wp_{\text{fs}}(X), \star |_{\wp_{\text{fs}}(X)}) \) is an invariant set, where \( \star |_{\wp_{\text{fs}}(X)} : S_A \times \wp_{\text{fs}}(X) \to \wp_{\text{fs}}(X) \) is defined by \( \pi \star |_{\wp_{\text{fs}}(X)} Y := \pi \star Y \) for all \( \pi \in S_A \) and \( Y \in \wp_{\text{fs}}(X) \).

**Definition 2.6.** Let \((X, \cdot)\) be an invariant set. A subset \( Z \) of \( X \) is called **finitely supported** if and only if there exists a finite set \( S \subseteq A \) such that \( S \) supports \( Z \) with respect to the \( S_A \)-action \( \star : S_A \times \wp(X) \to \wp(X) \) defined by \( \pi \star Y := \{\pi \cdot y | y \in Y\} \) for all permutations \( \pi \) of \( A \) and all subsets \( Y \) of \( X \). Whenever \( S \) supports \( Z \) with respect to the \( S_A \)-action \( \star \), we just say \( S \) supports \( Z \).

**Remark 2.1.** Let \((X, \cdot)\) be an invariant set. A subset \( Z \) of \( X \) is finitely supported in the sense of Definition 2.6 if and only if \( Z \in \wp_{\text{fs}}(X) \).

Note that an equivariant subset of an invariant set is itself an invariant set.

**Proposition 2.2 ([71]).** Let \( X \) be a finite subset of an invariant set \((U, \cdot)\). Then we have that \( X \) is finitely supported and \( \text{supp}(X) = \bigcup \{\text{supp}(x) | x \in X\} \).

**Proof.** Let \( X = \{x_1, \ldots, x_k\} \), and \( S = \text{supp}(x_1) \cup \ldots \cup \text{supp}(x_k) \). Obviously, \( S \) supports \( X \). Indeed, let us consider \( \pi \in \text{Fix}(S) \). We have that \( \pi \in \text{Fix}(\text{supp}(x_i)) \) for
each \( i \in \{1, \ldots, k\} \). Therefore, \( \pi \cdot x_i = x_i \) for each \( i \in \{1, \ldots, k\} \) because \( supp(x_i) \) supports \( x_i \) for each \( i \in \{1, \ldots, k\} \), and so \( supp(X) \subseteq S \). It remains to prove that \( S \subseteq supp(X) \). Consider \( a \in S \). This means there exists \( j \in \{1, \ldots, k\} \) such that \( a \in supp(x_j) \). Let \( b \) be an atom such that \( b \notin supp(X) \) and \( b \notin supp(x_i) \), \( \forall i \in \{1, \ldots, k\} \). Such an atom exists because \( A \) is infinite, whilst \( supp(X) \) and \( supp(x_i) \), \( i \in \{1, \ldots, k\} \), are all finite. We prove by contradiction that \( (b a) \cdot x_j \notin X \). Indeed, suppose that \( (b a) \cdot x_j \in X \). In this case there is \( y \in X \) with \( (b a) \cdot x_j = y \). Since \( a \in supp(x_j) \), we have \( b \in (b a)(supp(x_j)) \). However, according to Proposition 2.1, we have \( supp(y) = (b a)(supp(x_j)) \). We obtain that \( b \in supp(y) \) for some \( y \in X \), which is a contradiction with the choice of \( b \). Therefore, \( (b a) \cdot X \neq X \), where \( * \) is the standard \( S_A \)-action on \( \mathcal{O}(U) \) which will be defined in Subsection 2.4.1. Since \( b \notin supp(X) \), we prove by contradiction that \( a \in supp(X) \). Indeed, suppose that \( a \notin supp(X) \). It follows that the transposition \( (b a) \) fixes each element from \( supp(X) \), i.e. \( (b a) \in Fix(supp(X)) \). Since \( supp(X) \) supports \( X \), by Definition 2.3, it follows that \( (b a) \cdot X = X \), which is a contradiction. Thus, \( a \in supp(X) \), and so \( S \subseteq supp(X) \). □

**Corollary 2.2.** Let \( X \) be a finite invariant set. Then \( X \) is necessarily a trivial invariant set, i.e. there exists only one possible \( S_A \)-action on \( X, \cdot : S_A \times X \to X \) defined by \( \pi \cdot x = x, \forall x \in X \).

*Proof.* Let \( X \) be a finite invariant set. We can equivalently say that \( X \) is a finite subset of the invariant set \((X, \cdot)\). Let \( X = \{x_1, \ldots, x_k\} \). According to Proposition 2.2, we have \( supp(X) = supp(x_1) \cup \ldots \cup supp(x_k) \). However, since \( X \) is itself equivariant, we have that \( supp(X) = \emptyset \). It follows that \( supp(x_1) \cup \ldots \cup supp(x_k) = \emptyset \), and so \( supp(x_i) = \emptyset \) for all \( i \in \{1, \ldots, k\} \). Thus, \( \pi \cdot x_i = x_i \) for all \( x_i \in X \) and all \( \pi \in S_A \), and so \( X \) is a trivial invariant set. □

### 2.4.2 Cartesian Products

Let \((X, \cdot)\) and \((Y, \circ)\) be \( S_A \)-sets. As in classical ZF set theory we define the Cartesian product \( X \times Y \) as the set of ordered pairs \( (x, y) = \{x, \{x, y\}\} \) for \( x \in X \) and \( y \in Y \). \( X \times Y \) is also an \( S_A \)-set with the \( S_A \)-action \( * : S_A \times (X \times Y) \to (X \times Y) \) defined by \( \pi \star (x, y) = (\pi \cdot x, \pi \circ y) \) for all \( \pi \in S_A \) and all \( x \in X \), \( y \in Y \). If \((X, \cdot)\) and \((Y, \circ)\) are invariant sets, then \((X \times Y, *)\) is also an invariant set. Also, according to Proposition 2.2, we have that \( supp((x, y)) = supp(x) \cup supp(y) \) for each \( x \in X \) and \( y \in Y \).

### 2.4.3 Disjoint Unions

Let \((X, \cdot)\) and \((Y, \circ)\) be \( S_A \)-sets. We define the disjoint union of \( X \) and \( Y \) by \( X + Y = \{(0, x) | x \in X\} \cup \{(1, y) | y \in Y\} \). \( X + Y \) is an \( S_A \)-set with the \( S_A \)-action \( * : S_A \times (X + Y) \to (X + Y) \) defined by \( \pi \star z = (0, \pi \cdot x) \) if \( z = (0, x) \) and \( \pi \star z = (1, \pi \circ y) \) if
z = (1, y). If (X, ·) and (Y, ◦) are invariant sets, then (X + Y, ⋆) is also an invariant set: each z ∈ X + Y is either of the form (0, x) and supported by the finite set supporting x in X, or is of the form (1, y) and supported by the finite set supporting y in Y.

2.4.4 Function Spaces

Recall that a function f : X → Y is a particular relation. Precisely, a function f : X → Y is a subset f of X × Y characterized by the property that for each x ∈ X there is exactly one y ∈ Y such that (x, y) ∈ f. A function f between two invariant sets X and Y is finitely supported if it is finitely supported as a subset of the Cartesian product X × Y in the sense of Definition 2.6. Whenever X and Y are invariant sets we have that X × Y is an invariant set. Now we can give the following definition for finitely supported functions:

Definition 2.7. Let X and Y be invariant sets. A function f : X → Y is finitely supported if f ∈ φ_fS(X × Y) with the notations in Subsection 2.4.1.

Let Y^X = {f ⊆ X × Y | f is a function from the underlying set of X to the underlying set of Y}.

Proposition 2.3. Let (X, ·) and (Y, ◦) be invariant sets. Then Y^X is an S_A-set with the S_A-action ◆ : S_A × Y^X → Y^X defined by (π ◆ f)(x) = π ◦ (f(π^{-1} · x)) for all π ∈ S_A, f ∈ Y^X and x ∈ X. A function f : X → Y is finitely supported in the sense of Definition 2.7 if and only if it is finitely supported with respect to the permutation action ◆.

Proof. We already know that functions from X to Y are subsets of the Cartesian product X × Y, which is an invariant set. Also φ(X × Y) is an S_A-set and π ◆ f = {(π · x, π ◦ y) | (x, y) ∈ f}. Thus, π ◆ f is a function with the domain π · X = X. Moreover, (π ◆ f)(π · x) = π ◦ f(x). Let x' = π · x, and so x = π^{-1} · x'. We obtain (π ◆ f)(x') = π ◦ (f(π^{-1} · x')). The application x → x' is bijective, and it follows that (π ◆ f)(x) = π ◦ (f(π^{-1} · x)) for all π ∈ S_A, f ∈ Y^X and x ∈ X. Therefore, each function f : X → Y is finitely supported with respect to the permutation action ◆ if and only if f ∈ φ_fS(X × Y).

Proof. Let (X, ·) and (Y, ◦) be invariant sets. Let f ∈ Y^X and π ∈ S_A be arbitrary elements. Let ◆ : S_A × Y^X → Y^X be the S_A-action on Y^X, defined by (π ◆ f)(x) = π ◦ (f(π^{-1} · x)) for all π ∈ S_A, f ∈ Y^X and x ∈ X. Then π ◆ f = f if and only if for all x ∈ X we have f(π · x) = σ ◦ f(x).

Proof. Let σ ∈ S_A be a permutation such that σ ◆ f = f. From Proposition 2.3, we know that for each x ∈ X we have (σ ◆ f)(σ · x) = σ ◦ f(x). Since σ ◆ f = f, it follows that f(σ · x) = σ ◦ f(x) for all x ∈ X. Conversely, let us suppose that for σ ∈ S_A and all x ∈ X we have f(σ · x) = σ ◦ f(x). For each x ∈ X we have (σ ◆ f)(x) = σ ◦ (f(σ^{-1} · x)) = f(σ ◆ (σ^{-1} · x)) = f(x).
Corollary 2.3. Let \((X, \cdot)\) and \((Y, \circ)\) be invariant sets. A function \(f \in Y^X\) is equivariant with respect to the \(S_A\)-action \(\star : S_A \times Y^X \rightarrow Y^X\) defined by: \((\pi \star f)(x) = \pi \circ (f(\pi^{-1} \cdot x))\) for all \(\pi \in S_A\), \(f \in Y^X\) and \(x \in X\), if and only if there exists a finite set \(S\) of atoms such that for all \(x \in X\) we have \(f(\pi \cdot x) = \pi \circ f(x)\).

Definition 2.7 can be generalized in the following way.

Definition 2.8. Let \(X\) and \(Y\) be invariant sets, and let \(Z\) be a finitely supported subset of \(X\). A function \(f : Z \rightarrow Y\) is finitely supported if \(f \in \mathcal{G}_f(X \times Y)\).

The following characterization can be proved analogously to Proposition 2.3 and Proposition 2.4.

Proposition 2.5. Let \((X, \cdot)\) and \((Y, \circ)\) be invariant sets, and let \(Z\) be a finitely supported subset of \(X\). Let \(f : Z \rightarrow Y\) be a function. The function \(f\) is finitely supported in the sense of Definition 2.8 if and only if there exists a finite set \(S\) of atoms such that for all \(x \in Z\) and all \(\pi \in \text{Fix}(S)\) we have \(\pi \cdot x \in Z\) and \(f(\pi \cdot x) = \pi \circ f(x)\).

Proof. Suppose that \(f\) is finitely supported in the sense of Definition 2.8. There exists a finite set \(S\) of atoms such that \(\pi \star f = f\) for all \(\pi \in \text{Fix}(S)\), where \(\star\) represents the \(S_A\)-action on \(\mathcal{G}(X \times Y)\) defined as in Subsection 2.4.1. Let \(x \in Z\) and \(\pi \in \text{Fix}(S)\) be arbitrary elements. Then there exists an unique \(y \in Y\) such that \((x, y) \in f\). Since \(\pi \star f = f\), we have \((\pi \cdot x, \pi \circ y) \in f \subseteq (Z \times Y)\). Thus, \(\pi \cdot x \in Z\) and \(f(\pi \cdot x) = \pi \circ y = \pi \circ f(x)\).

Conversely, assume that there exists a finite set \(S\) of atoms such that for all \(x \in Z\) and all \(\pi \in \text{Fix}(S)\) we have \(\pi \cdot x \in Z\) and \(f(\pi \cdot x) = \pi \circ f(x)\). We claim that \(\pi \star f = f\) for all \(\pi \in \text{Fix}(S)\). Fix some \(\pi \in \text{Fix}(S)\), and consider \((x, y)\) an arbitrary element in \(f\). We have \(f(x) = y\), and so \((\pi \cdot x, \pi \circ y) \in f\). However, \(\pi \triangleright (x, y) = (\pi \cdot x, \pi \circ y) \in f\), where \(\triangleright\) represents the \(S_A\)-action on \(X \times Y\) defined as in Subsection 2.4.2. This means \(\pi \star f = f\).

Note that not every function between two nominal sets is finitely supported.

Proposition 2.6.

1. If \(f : A \rightarrow \mathbb{N}\) is a function such that \(S_f = \{a \in A \mid f(a) \neq 0\}\) is finite, then \(f\) is finitely supported and \(\text{supp}(f) = S_f\).
2. If \(f : A \rightarrow \mathbb{N}\) is a function such that \(S_f = \{a \in A \mid f(a) \neq 0\}\) is neither finite nor cofinite, then \(f\) may be non-finitely supported.

Proof. 1. According to Example 2.1(4), \(\mathbb{N}\) is an invariant set equipped with the trivial \(S_A\)-action. We claim that \(S_f = \{x \in A \mid f(x) \neq 0\}\) supports \(f\). Let \(\pi \in \text{Fix}(S_f)\).

According to Proposition 2.4, we have to prove that \(f(\pi(a)) = f(a)\), \(\forall a \in A\). Let \(a \in A\) be an arbitrary element. If \(f(a) \neq 0\), we have \(a \in S_f\), and \(\pi(a) = a\) because \(\pi\) fixes \(S_f\) pointwise. Therefore, \(f(\pi(a)) = f(a)\). Now let \(a \in A\) with \(f(a) = 0\). Let us suppose that \(f(\pi(a)) \neq 0\). It follows that \(\pi(a) \in S_f\) and

\[1\] The case when \(Z\) is equivariant reduces to Proposition 2.4 because the equivariant subsets have similar properties to the invariant sets.
\[ \pi(\pi(a)) = \pi(a). \] Since \( \pi \) is bijective, we get \( \pi(a) = a \) and \( f(\pi(a)) = f(a) = 0 \) which contradicts our assumption that \( f(\pi(a)) \neq 0 \). Therefore, \( f(\pi(a)) = 0 \). We proved that \( S_f \) supports \( f \). It remains to prove that \( S_f \) is minimal between the finite sets supporting \( f \). Let \( V \) be a finite set supporting \( f \). We claim \( S_f \subseteq V \). Let \( b \in S_f \), i.e. \( f(b) \neq 0 \). Suppose that \( b \notin V \). Let \( c \) be an arbitrary element from \( CV \overset{def}{=} A \setminus V \). Since \( b \notin V \), we have \( (bc) \in \text{Fix}(V) \). However, \( V \) supports \( f \). This means \( f((bc)(a)) = f(a), \forall a \in A \). In particular, \( f(c) = f(b) \neq 0 \). Therefore, \( c \in S_f \), and \( CV \subseteq S_f \). Since \( CV \) is infinite, we obtain that \( S_f \) is cofinite which contradicts the assumption that \( S_f \) is finite. Therefore, \( b \in V \), and \( S_f \subseteq V \).

2. Such an \( f \) can be defined by using the fact that the subsets of \( A \) that are at the same time infinite and cofinite fail to be finitely supported. For example, \( f \) could be a function that is one-to-one on a subset of \( A \) which is simultaneously infinite and cofinite. \( \Box \)

**Proposition 2.7.** Let \( f : A \to A \) be a finitely supported bijection on \( A \). Then \( \{a \in A \mid f(a) \neq a\} \) is finite and \( \text{supp}(f) = \{a \in A \mid f(a) \neq a\} \).

**Proof.** First, we prove that for each \( a \in A \) we have \( a \notin \text{supp}(f) \iff f(a) = a \). Let \( a \notin \text{supp}(f) \). Assume that \( f(a) \neq a \). Let us consider two atoms \( b, c \notin \text{supp}(f) \) such that \( a, b, c \), are all different (such atoms exist because \( \text{supp}(f) \) is finite, whilst \( A \) is infinite). Since \( \text{supp}(f) \) supports \( f \) and \( (ab) \in \text{Fix}(\text{supp}(f)) \), we have \( (ab) \star f = f \), where \( \star \) is the \( S_A \)-action on \( A^A \) presented in Proposition 2.3. Analogously, \( (ac) \star f = f \). According to Proposition 2.4, we have \( f(b) = f((ab)(a)) = (ab)(f(a)) \). However, \( f(a) \neq a \). Since \( f \) is a bijection, it follows that \( f(a) = b \) (otherwise, we would have \( f(b) = f(a) \) with \( b \neq a \)). However, from \( f((ac)(a)) = (ac)(f(a)) \), it follows that \( f(c) = (ac)(b) = b = f(a) \), which contradicts the bijectivity of \( f \). Thus, \( f(a) = a \). This means \( S = \{a \in A \mid f(a) \neq a\} \subseteq \text{supp}(f) \). Since \( \text{supp}(f) \) is finite, we have that \( S \) is finite.

Now, we prove that the finite set \( S \) supports \( f \). Indeed, let us consider \( \pi \in \text{Fix}(S) \), i.e. \( \pi(a) = a \) whenever \( f(a) \neq a \). We claim that \( f(\pi(x)) = \pi(f(x)), \forall x \in A \). Indeed, fix an arbitrary element \( x \in A \). If \( f(x) \neq x \), then \( \pi(x) = x \) and \( f(\pi(x)) = f(x) \). However, since \( f \) is injective, we also have \( f(f(x)) \neq f(x) \), and so \( \pi(f(x)) = f(x) \). Thus, \( f(\pi(x)) = \pi(f(x)) \). On the other hand, if \( f(x) = x \), then \( f(\pi(x)) = \pi(x) \). Suppose that \( f(\pi(x)) \neq \pi(x) \). This means \( \pi(\pi(x)) = \pi(x) \), and so \( \pi(x) = x \). Then \( f(\pi(x)) = f(x) = x = \pi(x) \), which contradicts the assumption that \( f(\pi(x)) \neq \pi(x) \). We obtain that \( f(\pi(x)) = \pi(x) \), and so \( f(\pi(x)) = \pi(f(x)) \). According to Proposition 2.4, we have that \( S \) supports \( f \). Since \( \text{supp}(f) \) is minimal between the finite sets supporting \( f \), it follows that \( S = \text{supp}(f) \). \( \Box \)

In [126] it is presented the following finite support principle.

**Theorem 2.5.** Any function or relation that is defined from finitely supported functions and relations using classical higher-order logic is itself finitely supported.

An equivariance principle is presented here as Theorem 2.6.

**Theorem 2.6.** Any function or relation that is defined from equivariant functions and relations using classical higher-order logic is itself equivariant.
It is worth noting that in applying the finite support/equivariance principle, one must take into account all the parameters upon which a particular construction depends. Thus, we believe the formal involvement of the finite support/equivariance principle (i.e. the precise verification of whether the conditions for applying the finite support/equivariance principle are properly satisfied) is sometimes at least as difficult as a direct proof. Moreover, many times it is necessary to present a more constructive method of defining the supports in order to ensure that some structures are (uniformly) finitely supported or in order to establish some relationship results between the related supports. Our book is also addressed to non-expert readers. Therefore, we rephrase the results in this book such that they can be understood even without presenting any additional notions regarding higher-order logic or more complicated finite-support/equivariance principles.

2.4.5 Categorical Constructions

Let $\text{Nom}$ be the category whose objects are the invariant sets and whose morphisms are the equivariant functions. $\text{Nom}$ is a Cartesian closed category. Moreover, we have the following result [156].

**Theorem 2.7.** Let $\mathbb{I}$ be the category whose objects are the finite subsets of $A$ and whose morphisms are the injections between them. Then the category $\text{Nom}$ is equivalent to the full subcategory of $\text{Set}^\mathbb{I}$ consisting of presheaves that preserve pullbacks.

A complete categorical study of invariant sets is out of our scope. However, for an in-depth study on these lines we recommend [127] or Chapter 2 from [123].

2.5 Fraenkel-Mostowski Axioms

Let us consider the set $A$ of atoms in the ZFA framework. As in [74] we can construct a single, ‘large’ $S_A$-set, i.e. an $S_A$-class (a class equipped with an $S_A$-action) $FM(A)$ all of whose elements have the finite support property. One benefit is that if a particular construction can be expressed in this language, then the action of permutations is inherited from the ambient universe $FM(A)$ without our having to define it explicitly and without our having to prove the associated finite support property.

Recall the usual von Neumann cumulative hierarchy of sets:

- $v_0 = \emptyset$
- $v_{\alpha+1} = \mathcal{P}(v_\alpha)$
- $v_\lambda = \bigcup_{\alpha < \lambda} v_\alpha$ ($\lambda$ a limit ordinal).

More generally, given a set $U$ we can analogously define a cumulative hierarchy of sets involving atoms from $U$ [74]:

- $v_0(U) = \emptyset$
• \( v_{\alpha+1}(U) = U + \varnothing(v_{\alpha}(U)) \)
• \( v_{\lambda}(U) = \bigcup_{\alpha<\lambda} v_{\alpha}(U) \) (\( \lambda \) a limit ordinal).

where \(+\) denotes the disjoint union of sets defined in Subsection 2.4.3. Let \( v(U) \) be the union of all \( v_{\alpha}(U) \). The class of sets built on atoms \( U \) is \( v(U) \).

We can construct the notion of finitely supported element in such an hierarchy by taking \( U \) to be the \( S_A \)-set \( A \) of atoms and by replacing \( \varnothing(-) \) by \( \varnothing_{fs}(-) \) (with the notations in Subsection 2.4.1):

• \( FM_0(A) = \emptyset \)
• \( FM_{\alpha+1}(A) = A + \varnothing_{fs}(FM_{\alpha}(A)) \)
• \( FM_{\lambda}(A) = \bigcup_{\alpha<\lambda} FM_{\alpha}(A) \) (\( \lambda \) a limit ordinal).

According to the results in Section 2.4, each \( FM_{\alpha}(A) \) is an invariant set. When we consider the union of all \( FM_{\alpha}(A) \) we get one ‘large’ \( S_A \)-set (i.e. an \( S_A \)-class) in which every element has finite support. The union of all \( FM_{\alpha}(A) \) is called the Cumulative Hierarchy Fraenkel-Mostowski (CHFM) universe, and is denoted by \( FM(A) \). Using the names \( atm \) and \( set \) for the functions \( x \mapsto (0,x) \) and \( x \mapsto (1,x) \) (the notations are preserved from Subsection 2.4.3) we have that every element \( x \) of \( FM(A) \) is either of the form \( atm(a) \) with \( a \in A \), or of the form \( set(X) \) where \( X \) is a finitely supported set formed at an earlier ordinal stage than \( x \). We call elements of the form \( set(X) \) CHFM sets and the elements of the form \( atm(a) \) atoms.

The \( S_A \)-action \( \cdot \) on the CHFM universe \( FM(A) \) can be defined recursively by:

\[
\pi \cdot atm(a) = atm(\pi(a)), \quad \pi \cdot set(X) = set(\{\pi \cdot x | x \in X\}).
\]

An element \( x \in v(A) \) is a CHFM set if and only if the following conditions are satisfied:

• \( y \) is a CHFM set or an atom for all \( y \in x \)
• \( x \) has finite support.

Therefore, we can say that a ZFA set is a CHFM set if and only if all its elements have hereditary finite supports. A CHFM set \( x \) is not itself closed under the \( S_A \)-action on \( FM(A) \) unless \( supp(x) = \emptyset \). Hence a CHFM set is not necessarily an invariant set in the sense of Definition 2.4. However, any CHFM set is a finitely supported element of the large invariant set \( FM(A) \). Also, a CHFM set with empty support is itself an invariant set. Thus, the invariant sets in the CHFM cumulative hierarchy can be defined as those empty-supported elements of the CHFM universe \( FM(A) \).

We are especially interested in those CHFM sets which are invariant sets. We define an invariant CHFM set as a CHFM set with empty support. Obviously, if \( X \) is an invariant CHFM set, then the restriction of the \( S_A \)-action \( \cdot \) on \( FM(A) \) to \( S_A \times X \) will have codomain equal to \( X \) because \( \pi \cdot X = X \) for all \( \pi \in S_A \). Therefore, invariant CHFM sets will be \( S_A \)-sets and invariant sets as well.

The underlying logic of ZFA is the usual first-order logic with equality. Its signature contains just a binary predicate set membership \( \in \) and a constant symbol \( A \). We write “\( \Rightarrow \)” to mean “implies”, and “\( \iff \)” to mean “if and only if”.
Definition 2.9. The following axioms give a complete characterization of Zermelo-Fraenkel set theory with atoms:

1. \( \forall x.(\exists y,y \in x) \Rightarrow x \notin A \) (only non-atoms can have elements)
2. \( \forall x,y.(x \notin A \land y \notin A \land \exists z.(z \in x \iff z \in y)) \Rightarrow x = y \) (axiom of extensionality)
3. \( \forall x,y,z.z = \{x,y\} \) (axiom of pairing)
4. \( \forall x.\exists y,y = \{z | z \subseteq x\} \) (axiom of power set)
5. \( \forall x.\exists y,y \notin A \land y = \{z | \exists w.(z \in w \land w \in x)\} \) (axiom of union)
6. \( \forall x.\exists y.(y \notin A \land y = \{f(z) | z \in x\}, \text{for each functional formula } f(z) \) (axiom of replacement)
7. \( \forall x.\exists y.(y \notin A \land y = \{z | z \in x \land p(z)\}), \text{for each formula } p(z) \) (axiom of separation)
8. \( (\forall x.\forall y.x \in p(y)) \Rightarrow p(x) \Rightarrow \forall x.p(x) \) (induction principle)
9. \( \exists x.(\emptyset \in x \land (\forall y.y \in x \Rightarrow y \cup \{y\} \in x)) \) (axiom of infinity)
10. \( A \text{ is not finite}. \)

We provide an axiomatic presentation of FM set theory.

1. \( \forall x.\exists y.(y \in x) \Rightarrow x \notin A \)
2. \( \forall x,y.(x \notin A \land y \notin A \land \exists z.(z \in x \iff z \in y)) \Rightarrow x = y \)
3. \( \forall x,y,z.z = \{x,y\} \)
4. \( \forall x.\exists y,y = \{z | z \subseteq x\} \)
5. \( \forall x.\exists y,y \notin A \land y = \{z | \exists w.(z \in w \land w \in x)\} \)
6. \( \forall x.\exists y.(y \notin A \land y = \{z | z \in x \land p(z)\} \), for each formula \( p(z) \)
7. \( \forall x.\exists y.(y \notin A \land y = \{f(z) | z \in x\}, \text{for each functional formula } f(z) \)
8. \( (\forall x.\forall y.x \in p(y)) \Rightarrow p(x) \Rightarrow \forall x.p(x) \)
9. \( \exists x.(\emptyset \in x \land (\forall y.y \in x \Rightarrow y \cup \{y\} \in x)) \)
10. \( A \text{ is not finite}. \)
11. \( \forall x.\exists S \subset A. S \text{ is finite and } S \text{ supports } x. \) (finite support property)

It is clear that \( \nu(A) \) is a model of ZFA set theory, and \( FM(A) \) is a model of FM set theory. Classical ZF sets can be defined in FM set theory. For example the set of natural numbers \( \mathbb{N} = \{0,1,2,\ldots\} \) is defined by \( 0 = \emptyset \) and \( i + 1 = i \cup \{i\} \).

There exist some different approaches in the literature. Some authors define the FM sets in the same way we define the invariant sets, whilst other authors define the FM sets as elements in the CHFM universe \( FM(A) \) which do not necessarily need to be invariant sets.

We define an \( FM \text{ set} \) as an element in \( FM(A) \) which is not an atom (i.e. as a CHFM set). We define an \( IFM \text{ set} \) as an invariant set with a special \( S_A \text{-action} \) induced by the \( S_A \text{-action} \) on \( FM(A) \). More precisely, an IFM set is a set from ZFA which is closed under the \( S_A \text{-action} \) on \( FM(A) \) and all of whose elements are finitely supported. The \( S_A \text{-action} \) on an IFM set will be called an \( interchange \text{ function} \). From now on, the CHFM universe will simply be called ‘the FM (cumulative) universe’.

Definition 2.10. i) An element from the FM universe \( FM(A) \) which is not an atom is called a \( Fraenkel-Mostowski \text{ set} (FM \text{ set}) \).
ii) An interchange function on a set $X$ constructed according to the axioms of ZFA set theory is a function $\cdot : S_A \times X \to X$ defined inductively by $\pi \cdot a := \pi(a)$ for all atoms $a \in A$ and $\pi \cdot x := \{\pi \cdot y | y \in x\}$, which satisfies the axiom that for all $x \in X$ there exists a finite subset $S \subset A$ such that $(ab) \cdot x = x$ for all $a, b \notin S$.

iii) An IFM set is a pair $(X, \cdot)$, where $X$ is a set defined according to the axioms of ZFA set theory and $\cdot : S_A \times X \to X$ is an interchange function on $X$.

Clearly, $FM(A)$ is an IFM set.

Remark 2.2. Since $S_A$ is a group, the interchange function $\cdot : S_A \times X \to X$ is an action of group $S_A$ on set $X$. Thus, we can express an IFM set $(X, \cdot)$ as a set provided by the action $\cdot$ of $S_A$ on $X$.

Every IFM set is also an invariant set. The converse is not valid.

Example 2.2. • The set of atoms $A$ with the $S_A$-action defined as in Example 2.1(1) is an IFM set whilst the set of atoms $A$ with the $S_A$-action defined as in Example 2.1(2) is an invariant set but not an IFM set.

• If $A$ is an IFM set (with the $S_A$-action defined as in Example 2.1(1)), then $\varnothing f_3(A)$ and $A \cup \varnothing f_3(A)$ are also IFM sets.

• If $A$ is an IFM set, then $FM_\alpha(A)$ is also an IFM set for each ordinal number $\alpha$.

From now on, we consider the set $A$ of atoms as the IFM set $A$ equipped with the $S_A$-action defined as in Example 2.1(1).

The property of the interchange function given in Definition 2.10 always allows one to find a finite set supporting $x$, for each element $x$ in an arbitrary IFM set.

The following theorem follows immediately from Corollary 2.1.

Theorem 2.8. Let $X$ be an IFM set, and for each $x \in X$ we define $\mathcal{F}_x = \{S \subset A | S \text{ finite, } S \text{ supports } x\}$. Then $\mathcal{F}_x$ has a least element which also supports $x$.

Example 2.3. We present some examples of how we can determine the support for various subsets of $A$:

1. If $B \subset A$ and $B$ is finite, then $supp(B) = B$.
2. If $C \subset A$ and $C$ is cofinite, then $supp(C) = A \setminus C$.
3. If $D \subset A$ is neither finite nor cofinite, then we cannot find a finite set supporting $D$.

Indeed, let us assume that $S$ supports $D$ (this means that we have $\pi(D) = D$ for each $\pi \in Fix(S)$). If $D$ is of the form $\{a, c, e, \ldots\}$ (see Remark 2.3), then at least $\{a, c, e, \ldots\}$ or $\{b, d, f, \ldots\}$ (where $\{b, d, f, \ldots\}$ is $C_D = A \setminus D$) must be fixed by each $\pi$. This means that $S$ cannot be finite. If we denote $\varnothing fin(A) = \{X | X \subset A, X \text{ finite}\}$ and $\varnothing cofin(A) = \{X | X \subset A, A \setminus X \text{ finite}\}$, we obtain $\varnothing(A) = \varnothing fin(A) \cup \varnothing cofin(A)$ in FM set theory and also in FSM. Thus, we do not accept in FSM the subsets of $A$ which are at the same time infinite and cofinite.

Remark 2.3. In Example 2.3, $\{a, c, e, \ldots\}$ is only a convention for writing $D$. We do not make a choice of atoms in the construction of $D$, of the form: $a$ is the first atom from $A$, $c$ is the third atom from $A$ etc. We use the form $\{a, c, e, \ldots\}$ for $D$.
because, by intuition, it is easy to see what is \( C_D \) in this case. However, the atoms that compose \( D \) are arbitrarily presented in the structure of \( D \), with no preliminary choice; the only condition is that both \( D \) and \( C_D \) have to be infinite.

The following example (also considered in [74]) shows us how we can express the usual \( \lambda \)-calculus in FSM.

**Example 2.4.** 1. If \( X' \) is the set of \( \lambda \)-terms \( t \), then we inductively define the action \( \star \) of \( S_A \) on \( X' \) by:

- **variable**: \( \pi \star a = \pi(a) \) whenever \( a \) is a variable (corresponding to atoms) and \( \pi \) is a permutation of atoms.
- **application**: \( \pi \star (tt') = (\pi \star t)(\pi \star t') \) for all \( \lambda \)-terms \( t \) and \( t' \) and all \( \pi \in S_A \).
- **abstraction**: \( \pi \star (\lambda a.t) = \lambda (\pi(a)).(\pi \star t) \) for all variables \( a \), all \( \lambda \)-terms \( t \) and all \( \pi \in S_A \).

\((X', \star)\) is an invariant set (and also an IFM set), and the support of a \( \lambda \)-term \( t \) is the finite set of atoms occurring in \( t \), whether as free, bound or binding occurrences.

2. Let \( X \) be the set of \( \alpha \)-equivalence classes of the \( \lambda \)-calculus terms \( t \). We can define an action \( \cdot \) of \( S_A \) on \( X \) by: \( \pi \cdot [t]_\alpha = [\pi \star t]_\alpha \) for all \( \lambda \)-terms \( t \) and all \( \pi \in S_A \) (where \([t]_\alpha\) represents the \( \alpha \)-equivalence class of the \( \lambda \)-term \( t \)). If two \( \lambda \)-terms \( t \) and \( t' \) are \( \alpha \)-equivalent, it is clear that \( \pi \star t =_\alpha \pi \star t' \), and so the action \( \cdot \) is well defined.

\((X, \cdot)\) is an invariant set (and also an IFM set). If \( t \) is chosen to be a representative of its \( \alpha \)-equivalence class, then \( \text{supp}(t) \) coincides with \( \text{fn}(t) \), where \( \text{fn}(t) \) is the set of free variables of \( t \) defined by the \( \lambda \)-calculus rules.

According to Example 2.4, we remark that an \( \alpha \)-equivalence class of terms does not contain bound names. We cannot define a function \( bn : X \to \wp(\text{fn}(A)) \) which would be able to extract exactly the bound names for term \( t \) [74]. Thus, \( \alpha \)-equivalent terms are identified in the FM framework since two \( \alpha \)-equivalent terms have the same set of free variables.

The construction of function spaces in Subsection 2.4.4 makes sense in the framework of FM sets as well as in the framework of invariant sets. Therefore, Definition 2.7, Proposition 2.3 and Proposition 2.4 can be rephrased as well in terms of FM sets. More technical details can be found in [74]. For example, a valid version of Proposition 2.4 is the following statement: “Let \( X \) and \( Y \) be two sets in the FM cumulative universe. Let \( f \in Y^X \) and \( \pi \in S_A \) be arbitrary elements. Then \( \pi \star f = f \) if and only if for all \( x \in X \) we have \( \pi \cdot x \in X \) and \( f(\pi \cdot x) = \pi \cdot f(x) \)”.

**2.6 Logical Notions in the FM Cumulative Universe**

According to [140], invariance under permutation reflects the formality of notions from logic. Thus, invariant notions are formal in the sense that they do not depend on the identity of objects. For example, in a formal language, the extension of the existential quantifier \( \exists \) consists of all non-empty subsets of the domain. Obviously,
all the one-to-one applications of the domain onto itself transform any non-empty subset of the domain in another non-empty subset of the domain. Therefore, the interpretation of the existential quantifier is invariant under every permutation.

Tarski’s thesis regarding logicality makes sense for objects in the finite relational type structure over a domain of basic objects \( D \), where the objects at each level are relations of one or more arguments between objects of lower levels. Rather than considering the entire set of permutations of a universe built as a cumulative hierarchy over \( D \), we can consider only those permutations of the objects in \( D \). Thus, the logical notions (and the logical operations of the type structure) are those invariant under arbitrary permutations of objects from \( D \).

Putting together the previous remark and the approach from [140] we can provide a practical method for verifying logicality in cumulative hierarchies. The general idea is to study the effect of permutations over sets. More precisely, we consider some domain \( D \) of basic objects, and construct a hierarchy of sets starting with the objects in \( D \). After that, we consider any permutation of objects from \( D \), and see what effect these permutations have on the sets of various levels. The sets that are fixed under all permutations are exactly the sets that can be denoted by a logical symbol. It is easy to see that the identity relation between basic objects and its negation are fixed under every permutation. At a higher level, the sets of sets that are fixed include the set of all non-empty sets (which is related to the existential quantifier) and the set consisting of just the empty set (which is related to the negated universal quantifier) This means that all of them can be denoted by logical symbols, and thus they represent formal (invariant) notions.

Formally, Tarski’s logicality criterion can be expressed as “Given a domain \( D \) of basic objects, an operation \( f \) in the type hierarchy over \( D \) is logical if and only if it is invariant under all permutations on \( D \).”

The Fraenkel-Mostowski approach corresponds to Tarski’s view. In order to define the cumulative Fraenkel-Mostowski universe \( FM(A) \), we start with a collection of basic objects (the set \( A \) of atoms) and construct a cumulative hierarchy of sets above them. As proved in Section 2.5, each element in \( FM(A) \) is finitely supported. Since in the FM universe any element has to be finitely supported, we conclude that any bijection on \( A \) has to be finitely supported. However, according to Proposition 2.7, a bijection on \( A \) is finitely supported if and only if it leaves unchanged all but finitely many atoms of \( A \). Thus, a bijection on \( A \) is finitely supported if and only if it is a permutation of \( A \) in the sense of Definition 2.1. Therefore, in the FM universe, \( S_A \) coincides with the set of one-to-one transformations of \( A \) onto itself in Tarski’s view. According to the recursive definition of the \( S_A \)-action \( \cdot \) on \( FM(A) \) (see Section 2.5), we can say that an element having the form \( \pi \cdot x \) (where \( \pi \in S_A, x \in FM(A) \)) is a new element \( y \in FM(A) \) obtained by replacing each atom \( a \) from the structure of \( x \) by \( \pi(a) \). Thus, an element of the form \( \pi \cdot x \) can be associated with ‘the effect of the transformation \( \pi \) on the element \( x \’ \) in Tarski’s view. We conclude that the empty-supported elements in \( FM(A) \) (i.e. those invariant sets defined in the FM cumulative universe) are invariant under all permutations of \( A \), and so the related elements are logical notions. We can present this in a more formal way.

**Theorem 2.9.** IFM sets are logical (in Tarski’s view).
The FM sets, i.e. the arbitrary elements from the FM cumulative universe, are not necessary logical in Tarski’s sense. They satisfy only a “weak” form of logicality, meaning that they are fixed only by those permutations that satisfy an additional requirement. More precisely, an FM-set $x$ is invariant under all permutations that fix its support pointwise. Furthermore, this is the “strongest” possible form of invariance because the support of an element is the least set supporting it. However, given an IFM set $X$, the set of all finitely supported subsets of $X$, generally denoted by $\wp^{\text{fs}}(X)$, is logical, i.e. invariant under all permutations of atoms. This follows by a direct refinement of Proposition 2.1 (adapted for the FM cumulative universe) which states than for any finitely supported subset $Y$ of $X$ we have that $\pi \star Y$ is supported by $\pi \star \text{supp}(Y)$ for any $\pi \in S_A$. Thus, the set of all finitely supported subsets of $X$ is closed under the effect of any permutation from $S_A$. We formalize this as follows.

**Proposition 2.8.** Let $X$ be an IFM set. Then the set of all finitely supported subsets of $X$, i.e. $\wp^{\text{fs}}(X)$, is logical.

A new quantifier related to FM set theory, denoted by $\mathcal{U}$, is introduced in Definition 2.14. In a formal language, the extension of the quantifier $\mathcal{U}$ consists of all cofinite subsets of the domain $A$. Obviously, all the one-to-one applications of $A$ onto itself transform any cofinite subset of the domain in another cofinite subset of the domain. Therefore, the interpretation of $\mathcal{U}$ is invariant under every permutation. We formalize this as the following result.

**Theorem 2.10.** The newly defined quantifier $\mathcal{U}$ of FM set theory is logical (in Tarski’s view).

This section justifies the definition of invariant sets (instead of nominal sets) in FSM. Actually, invariant sets in FSM are similar to nominal sets in computer science. This section also completes the original research presented in [24].

### 2.7 Inconsistency of Choice Principles

According to [74], the full axiom of choice fails in FSM. In [74] the authors require the set of atoms to be countable for calculability reasons. However, we state that FSM is consistent even when the set of atoms is uncountable and infinite. In this section we prove some stronger results. Regardless of whether the set of atoms is countable, not only is the full axiom of choice inconsistent in FSM, but many other choice principles presented in Section 2.1 are also inconsistent in FSM [25].

Note that the choice principles from Section 2.1 can be presented in FSM by requiring that all the constructions which appear in their statement are finitely supported. For example:

- **AC** has the form “Given any invariant set $X$, and any finitely supported family $\mathcal{F}$ of non-empty finitely supported subsets of $X$, there exists a finitely supported choice function on $\mathcal{F}$.”
2.7 Inconsistency of Choice Principles

- **ZL** has the form “Let $P$ be a non-empty invariant poset\(^2\) with the property that every finitely supported totally ordered subset of $P$ has an upper bound in $P$. Then $P$ has a maximal element.”

- **DC** has the form “Let $R$ be a non-empty finitely supported relation on a finitely supported subset $Y$ of an invariant set $X$ having the property that for each $x \in Y$ there exists $y \in Y$ with $xRy$. Then there exists a finitely supported function $f : \omega \to Y$ such that $f(n)Rf(n+1)$, $\forall n \in \omega$.”

- **CC** has the form “Given any invariant set $X$, and any countable family $\mathcal{F} = (X_n)_n$ of subsets of $X$ such that the mapping $n \mapsto X_n$ is finitely supported, there exists a finitely supported choice function on $\mathcal{F}$.”

- **PCC** has the form “Given any invariant set $X$, and any countable family $\mathcal{F} = (X_n)_n$ of subsets of $X$ such that the mapping $n \mapsto X_n$ is finitely supported, there exists an infinite subset $M$ of $\mathbb{N}$ with the property that there is a finitely supported choice function on $(X_m)_{m \in M}$.”

- **AC(fin)** has the form “Given any invariant set $X$, and any finitely supported family $\mathcal{F}$ of non-empty finite subsets of $X$, there exists a finitely supported choice function on $\mathcal{F}$.”

- **CC(fin)** has the form “Given any invariant set $X$, and any countable family $\mathcal{F} = (X_n)_n$ of finite subsets of $X$ such that the mapping $n \mapsto X_n$ is finitely supported, there exists a finitely supported choice function on $\mathcal{F}$.”

- **PCC(fin)** has the form “Given any invariant set $X$, and any countable family $\mathcal{F} = (X_n)_n$ of finite subsets of $X$ such that the mapping $n \mapsto X_n$ is finitely supported, there exists an infinite subset $M$ of $\mathbb{N}$ with the property that there is a finitely supported choice function on $(X_m)_{m \in M}$.”

- **PIT** has the form “Every invariant Boolean algebra\(^3\) with $0 \neq 1$ has a maximal finitely supported ideal.”

- **UFT** has the form “Any finitely supported filter of an invariant Boolean algebra can be extended to a finitely supported ultrafilter.”

- **KW** has the form “Given any invariant set $X$, and any finitely supported family $\mathcal{F}$ of non-empty finitely supported subsets of $X$ of cardinality at least 2, there exists a finitely supported function $f$ on $\mathcal{F}$ such that $f(Y)$ is a proper non-empty subset of $Y$ for each $Y \in \mathcal{F}$.”

- **RKW** has the form “Given any invariant set $X$, and $\mathcal{F}$ the family of all non-empty finitely supported subsets of $X$ of cardinality at least 2, there exists a finitely supported function $f$ on $\mathcal{F}$ such that $f(Y)$ is a proper non-empty subset of $Y$ for each $Y \in \mathcal{F}$.”

- **OP** has the form “For every invariant set $X$ there exists a finitely supported total order relation on $X$.”

- **OEP** has the form “Every finitely supported partial order relation on an invariant set can be enlarged to a finitely supported total order relation.”

---

\(^2\) An invariant poset is an invariant set equipped with an equivariant partial order relation, cf. Definition 3.21.

\(^3\) An invariant Boolean algebra is an invariant set $(L, \cdot)$ endowed with an equivariant lattice order $\sqsubseteq$ and with the additional condition that $L$ is distributive and uniquely complemented, c.f. Definition 3.24.
- **Fin** has the form “Given any infinite finitely supported subset \( X \) of an invariant set, there exists a finitely supported injection from \( \mathbb{N} \) to \( X \).”

**Theorem 2.11.** In FSM, the following implications remain valid.

1. AC ⇒ DC ⇒ CC ⇒ CC(fin);
2. AC ⇒ UFT ⇒ OEP ⇒ OP ⇒ AC(fin) ⇒ CC(fin);
3. Fin ⇒ PCC(fin);
4. KW ⇔ RKW ⇒ OP.

**Proof.** Theorem 2.1 is valid in FSM if we are able to rephrase it such that all the objects that appear in its proof are finitely supported. In order to make our point we follow [88]:

Each set \( S_x \) used in Theorem 2.12 (1) from [88] to prove that AC ⇒ DC is supported by \( supp(x) \cup supp(\rho) \); the family \( (S_x)_{x \in X} \) and the mapping \( x \mapsto S_x \) are supported by \( supp(\rho) \), and the sequence \( (x_n)_n \) is supported by \( supp(x_0) \cup supp(s) \) where \( s \) is the finitely supported choice function on the family \( S_x \).

In order to prove that DC ⇒ CC we restate Theorem 2.12(2) from [88] in FSM. Let \( X \) be an invariant set and \( F = (X_n)_{n>0} \) be a family of subsets of \( X \) such that the mapping \( n \mapsto X_n \) is finitely supported (i.e. all \( X_n \) are supported by the same set). Define \( Y_n = \prod_{1 \leq m \leq n} X_m \) and \( Y = \bigcup_{n>0} Y_n \). All \( Y_n \) and \( Y \) are supported by the finite set which supports the mapping \( n \mapsto X_n \) because \( supp(n \mapsto X_n) \) supports \( Y \) and each permutation is a bijective function. Therefore, according to DC, there exists a sequence \( (y_n)_{n>0} \) in \( Y \) such that \( y_n \rho y_{n+1} \), and all \( y_n \) are supported by the same set \( S \) (i.e. the mapping \( n \mapsto y_n \) is supported by \( S \)). If we assume that \( y_1 = (x_1), x_1 \in X_1 \), then, according to the definition of \( \rho \), we have that \( y_2 \) is a pair \( (x_1, x_2) \), with \( x_2 \in X_2, y_3 \) is a 3-tuple \( (x_1, x_2, x_3) \), with \( x_3 \in X_3 \), and so on. Therefore, each \( y_n \) is an \( n \)-tuple of the form \( (y_{n-1}, x_n) \), \( x_n \in X_n \). By induction, since we know that all \( y_n \) are supported by the same \( S \), it follows that all \( x_n \) are supported by the same \( S \). The family \( (x_n)_{n>0} \) is a finitely supported family in \( \prod_{n>0} X_n \), and so CC is a valid statement in FSM. Note that the assumption that \( y_1 = (x_1) \in X_1 \) is made for convenience. If there exists some \( k > 1 \) such that \( y_1 \in \prod_{m<k} X_m \), then, in a similar way (using the definition of \( \rho \)), we prove that \( \prod_{k \leq l} X_l \) is non-empty. Hence \( \prod_{n>0} X_n \) is also non-empty because the Cartesian product of the finite family \( \{X_i \mid i \leq k \} \) is obviously non-empty.

The proof of Theorem 4.39 from [88] can be reformulated in FSM since each finite subset \( F \) of \( X \) is finitely supported, and the mappings \( F \mapsto X_F \) and \( (E,F) \mapsto A_{\rho(E,F)} \) are finitely supported by \( supp(F) \cup supp(R) \) and \( supp(E) \cup supp(F) \cup supp(R) \), respectively; it follows that UFT ⇒ OEP holds in FSM. According to Theorem 4.39 in [88], we obtain directly that OEP ⇒ OP holds in FSM. Now,

---

4 The notations are those used in the proof of Theorem 2.12 from [88].
5 The notations are those used in the proof of Theorem 4.39 from [88].
if we assume that OP holds in FSM, and we consider a finitely supported family $\mathcal{F}$ of non-empty finite subsets of an invariant set $U$, then $X = \bigcup \mathcal{F}$ is supported by $\text{supp}(\mathcal{F})$. Since there exists a finitely supported linear order on $U$, it follows that there exists a finitely supported linear order $< \in X$, and so each (finite) set $Y \in \mathcal{F}$ has a least element $y_Y$. We can define a choice function $f$ on $\mathcal{F}$ by $f(Y) = y_Y$ for all $Y \in \mathcal{F}$. We claim that $\text{supp}(\mathcal{F}) \cup \text{supp}(<) \text{ supports } f$. Let $\pi \in \text{Fix}(\text{supp}(\mathcal{F}) \cup \text{supp}(<))$ and let us fix $Y \in \mathcal{F}$. Since $\pi \cdot Y \in \mathcal{F}$, according to Proposition 2.5, it remains to prove that $f(\pi \cdot Y) = \pi \cdot y_Y$ (where $\cdot$ is defined as in Subsection 2.4.1). We know that, because $\pi$ fixes $\text{supp}(\mathcal{F})$ pointwise, there exists some $Z \in \mathcal{F}$ such that $\pi \cdot Y = Z$. For each $z \in Z$ we obtain an element $y \in Y$ such that $z = \pi \cdot y$. However, $y_Y < y$ according to the definition of $y_Y$. Since $\pi$ fixes $\text{supp}(<)$ pointwise, we have $\pi \cdot y_Y < \pi \cdot y = z$. Moreover, $\pi \cdot y_Y \in (\pi \cdot Y) = Z$. Since $z$ was arbitrarily chosen from $Z$, we obtain that $\pi \cdot y_Y$ is the smallest element of $Z$. Therefore, $f(\pi \cdot Y) = f(Z) = \pi \cdot y_Y = \pi \cdot f(Y)$. It follows that the result OP $\Rightarrow$ AC(fin) is valid in FSM.

In order to prove Theorem 2.11(3), assume that Fin is a valid statement. Let $(X_n)_n$ be a sequence of finite subsets of an invariant set such that the mapping $n \mapsto X_n$ is finitely supported (i.e. all $X_n$ are supported by the same $S$). The set $X = \bigcup \{X_n \times \{n\}\}$ in Theorem 2.14(2) from [88] is obviously finitely supported by $\text{supp}(n \mapsto X_n)$. Therefore, $X$ has a countable subset $Y = (y_k)_k$ with the property that the mapping $k \mapsto y_k$ is finitely supported. The set $M = \{n \in \mathbb{N} \mid Y \cap (X_n \times \{n\}) \neq \emptyset\}$ in the proof of Theorem 2.14(2) from [88] is infinite, well defined in FSM, and equivariant because it is a subset of $\mathbb{N}$. For each $m \in M$ define $k_m = \min \{k \in \mathbb{N} \mid y_k \in (X_m \times \{m\})\}$. Then $y_{k_m} = (x_m, m)$ for a unique $x_m \in X_m$. Fix some $m \in M$. For each $\pi \in \text{supp}(k \mapsto y_k)$ we have $\pi \cdot y_{k_m} = (\pi \cdot x_m, \pi \cdot m) = (\pi \cdot x_m, m)$; moreover, we also have $\pi \cdot y_{k_m} = y_{k_m} = (x_m, m)$. This means $\text{supp}(k \mapsto y_k)$ supports $x_m$. Therefore, the sequence $(x_m)_{m \in M}$ is finitely supported (and the mapping $m \mapsto x_m$ is finitely supported). It follows that Fin $\Rightarrow$ PCC(fin) holds in FSM.

In order to prove Theorem 2.11(4), we restate Theorem 4.40 from [88] in FSM. We assume that KW is valid in FSM, and consider an invariant set $(X, \cdot)$. Let $\mathcal{F}$ be the set of all finitely supported subsets $Y$ of $X$ with cardinality greater than or equal to 2. Since permutations are bijective functions, we claim that $\mathcal{F}$ is equivariant. Indeed, for each $\pi \in S_A$ we have that $\pi \cdot Y$ is finitely supported if $Y$ is finitely supported (see Proposition 2.1), and $\pi \cdot Y$ has at least two elements if $Y$ has at least two elements. The implication KW $\Rightarrow$ RKW follows immediately by applying KW to the finitely supported family $\mathcal{F}$. Now, assume that RKW is a valid choice principle, and consider an invariant set $(X, \cdot)$. Let $\mathcal{F}$ be a finitely supported family of finitely supported subsets $Y$ of $X$ with cardinality greater than or equal to 2. Let $\mathcal{F}'$ be the set of all finitely supported subsets $Y$ of $X$ with cardinality greater than or equal to 2. For $\mathcal{F}'$ there exists a finitely supported function $f$ on $\mathcal{F}'$ such that $f(Y)$ is a proper non-empty subset of $Y$ for each $Y \in \mathcal{F}'$. However, $\mathcal{F} \subseteq \mathcal{F}'$. Since the

\[< \text{ is the restriction to } X \text{ of the linear order on } U. \text{ If we denote by } R \text{ the finitely supported linear order on } U, \text{ then } < \text{ is supported by } \text{supp}(R) \cup \text{supp}(X).\]
\[\text{The relation } \pi \cdot y_Y < \pi \cdot y \text{ makes sense because } \pi \in \text{Fix}(\text{supp}(\mathcal{F})) \text{ and } \text{supp}(\mathcal{F}) \text{ supports } X, \text{ and so both } \pi \cdot y_Y \text{ and } \pi \cdot y \text{ are elements from } X.\]
function \( g = f|_\mathcal{F} \) is supported by \( \text{supp}(\mathcal{F}) \cup \text{supp}(f) \) (see Proposition 2.5), we obtain that \( g \) is the required Kinna-Wagner selection function on \( \mathcal{F} \).

Now, assume that \( \textbf{RKW} \) is valid in FSM, and consider an invariant set \((X,\cdot)\). Let \( \supseteq \) be the set of all finitely supported subsets \( Y \) of \( X \) with cardinality greater than or equal to 2. By \( \textbf{RKW} \), there exists a family \( \{U_Y\}_{Y \in \supseteq} \) of non-empty proper finitely supported subsets of \( Y \) such that the mapping \( Y \mapsto U_Y \) is finitely supported. This means \( \pi \ast U_Y = U_{\pi \ast Y} \) for all \( \pi \in \text{Fix}(\text{supp}(Y \mapsto U_Y)) \) (see Proposition 2.5). Denote \( Y \setminus U_Y \) by \( V_Y \). Obviously, each \( V_Y \) is supported by the union between the support of \( Y \) and the support of the related \( U_Y \). We claim that \( Y \mapsto V_Y \) is supported by \( \text{supp}(Y \mapsto U_Y) \). Indeed, let \( \pi \in \text{Fix}(\text{supp}(Y \mapsto U_Y)) \). It follows that \( V_{\pi \ast Y} = (\pi \ast Y) \setminus U_{\pi \ast Y} = (\pi \ast Y) \setminus (\pi \ast U_Y) = \pi \ast (Y \setminus U_Y) = \pi \ast V_Y \). Therefore, \( \pi \ast V_Y = V_{\pi \ast Y} \) for all \( \pi \in \text{Fix}(\text{supp}(Y \mapsto U_Y)) \), that is, \( Y \mapsto V_Y \) is supported by \( \text{supp}(Y \mapsto U_Y) \). Consider the set \( Z \) of all finitely supported linear preorder relations \( R \) on \( X \). According to Proposition 2.1, \( Z \) is equivariant. For each \( R \in Z \) and each \( x \in X \) consider the component \( [x]_R = \{y \in X | xRy \wedge yRx\} \) of \( x \) in \((X,R)\). We have that each \( [x]_R \) is supported by \( \text{supp}(x) \cup \text{supp}(R) \). Let \( \mathcal{K} \) be the set of all components \( [x]_R \) of \((X,R)\) with at least two elements. Since \( \pi \ast [x]_R = [\pi \cdot x]_R \) for all \( \pi \in \text{Fix}(\text{supp}(R)) \) and each permutation is bijective, we have that \( \pi \ast [x]_R \in \mathcal{K} \) for each \( \pi \in \text{Fix}(\text{supp}(R)) \) and each \( [x]_R \in \mathcal{K} \). This means \( \text{supp}(R) \) supports \( \mathcal{K} \). Let \( \mathfrak{K} \) be the Hartogs number of \( Z \), i.e. \( \mathfrak{K} \) is the least upper bound of the set \( \{\alpha | \alpha \text{ is an ordinal with } |\alpha| \leq |Z|\} \) [85]. According to [88], the Hartogs number of \( Z \) is the smallest \( \mathfrak{K} \) with \( \mathfrak{K} \not\subseteq |Z| \). Via transfinite recursion, we define\(^8\) a map \( f : \mathfrak{K} \to Z \) by:

- \( f(0) = X \times X \);
- \( f(\alpha + 1) = f(\alpha) \setminus \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\} \);
- \( f(\alpha) = \bigcap_{\beta < \alpha} f(\beta) \), if \( \alpha \) is a limit ordinal.

If \( \text{supp}(f(\alpha)) \) exists, we claim that \( f(\alpha + 1) \) is supported by \( \text{supp}(f(\alpha)) \cup \text{supp}(Y \mapsto U_Y) \). Let \( \pi \in \text{Fix}(\text{supp}(f(\alpha)) \cup \text{supp}(Y \mapsto U_Y)) \). Let us consider \((v,u) \in \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\}\). This means there exists \( K_0 \notin \mathcal{K}_{f(\alpha)} \) such that \((v,u) \in V_{K_0} \times U_{K_0}\). Since \( \pi \in \text{Fix}(\text{supp}(Y \mapsto U_Y)) \), we have \((\pi \cdot v, \pi \cdot u) \in V_{\pi \ast K_0} \times U_{\pi \ast K_0}\). However, we proved that \( \text{supp}(f(\alpha)) \) supports \( \mathcal{K}_{f(\alpha)} \). Since \( \pi \in \text{Fix}(\text{supp}(f(\alpha)) \cup \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\}\) and \( K_0 \notin \mathcal{K}_{f(\alpha)} \), we have \( \pi \ast K_0 \in \mathcal{K}_{f(\alpha)} \). Thus, \( \pi \ast (v,u) \in \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\} \). Now, consider \((v',u') \in f(\alpha + 1)\). Clearly, \( \pi \ast (v',u') \in f(\alpha) \) because we have \( \pi \ast (v',u') \in \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\} \). If \( \pi \ast (v',u') \in \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\} \), then we have \( \pi \ast (v',u') = \pi^{-1} \ast (\pi \ast (v',u')) \in \cup \{V_K \times U_K | K \in \mathcal{K}_{f(\alpha)}\} \) which contradicts the choice of \((v',u')\). This means \( \pi \ast (v',u') \notin f(\alpha + 1)\).

Clearly, \( \text{supp}(f(0)) = \emptyset \), \( f(1) \) is supported by \( \text{supp}(Y \mapsto U_Y) \), and so on. Therefore, \( f(\alpha + 1) \) is supported by \( \text{supp}(Y \mapsto U_Y) \) (which does not depend on \( \alpha \)) for each \( \alpha \in \mathfrak{K} \). This means \( f \) is finitely supported.

Since \( \mathfrak{K} \not\subseteq |Z| \), \( f \) cannot be injective. Thus, there exists some \( \alpha \in \mathfrak{K} \) with \( f(\alpha + 1) = f(\alpha) \). For this \( \alpha \), \( \mathcal{K}_{f(\alpha)} \) must be empty, i.e. \( f(\alpha) \) is the required finitely supported linear order on \( X \). This means \( \textbf{RKW} \Rightarrow \textbf{OP} \) is a valid result in FSM. \( \square \)

---

\(^8\) Such a map can be correctly defined in FSM because \( Z \) is equivariant and, hence, it has the same properties as an invariant set.
**Theorem 2.12.** The choice principle $\text{Fin}$ is inconsistent in FSM.

*Proof.* Let us assume that $\text{Fin}$ is valid in FSM. Therefore, we can find a finitely supported injection $f: \mathbb{N} \to A$. Let us consider $m, n \in \mathbb{N}$ such that $m \neq n$ and $f(m), f(n) \notin \text{supp}(f)$. Hence $(f(m)f(n)) \neq f$. Let us denote $(f(m)f(n))$ by $\pi$. Since the $S_A$-action $\cdot$ on $\mathbb{N}$ is defined as in Example 2.1(4), according to Proposition 2.3, we have $f(m) = (\pi \cdot f)(m) = \pi(f(m)) = f(n)$ which contradicts the injectivity of $f$. Thus, $\text{Fin}$ is inconsistent in FSM. \[\square\]

**Theorem 2.13.** The choice principle $\text{AC(fin)}$ is inconsistent in FSM.

*Proof.* Let us assume that $\text{AC(fin)}$ is valid in FSM. We consider the set $P := \varnothing_2(A) = \{X|X \subset A, X \text{ finite, } |X| = 2\}$. This means $P$ is the set of all pairs of elements from $A$. Since $P$ is equivariant (i.e. empty supported), our construction makes sense in FSM. Suppose that $\text{AC(fin)}$ is valid, which means there exists a finitely supported choice function $f$ on $P$. Let $Y = \{a_1, \ldots, a_n, b_1, \ldots, b_n\}$ be a finite set supporting $f$, where each $\{a_i, b_i\} \in P$. Since $P$ is infinite, we may select a pair $\{c, d\} = X$ from $P$ such that $c$ and $d$ are different from all $a_i, b_i$. Let $\pi \in S_A$ be a permutation which fixes each $a_i$ and $b_i$ and interchanges $c$ and $d$. Then $\pi$ fixes $f$. Since $f$ is a choice function on $P$, and $X \in P$, we have $f(X) \in X$, that is, $f(X) = c$ or $f(X) = d$. Since $\pi$ interchanges $c$ and $d$, we have $\pi(f(X)) \neq f(X)$. However, $\pi(X) = X$, and since $\pi$ fixes $Y$ pointwise (and, hence, $\pi$ fixes $f$), we have $\pi(f(X)) = f(\pi(X)) = f(X)$ according to Proposition 2.5. Thus, we get a contradiction, and $\text{AC(fin)}$ cannot be valid. \[\square\]

**Corollary 2.4.** The choice principles $\text{UFT}$, $\text{OEP}$ and $\text{OP}$ are inconsistent in FSM.

**Remark 2.4.** Note that the inconsistency of $\text{UFT}$ in FSM can also be proved without using Theorem 2.11. From Proposition 5.2.2 in [123] (which remains valid even when the set of atoms is not countable), there exists an invariant Boolean algebra having a finitely supported filter that cannot be extended to a finitely supported ultrafilter. Therefore, $\text{UFT}$ fails in the framework of invariant sets. We mention that the proof provided in [123] is slightly different than the proof presented in Theorem 2.11. However, we use Proposition 5.2.2 from [123] in order to prove that $\text{PIT}$ is inconsistent in FSM. \[\text{9}\]

**Theorem 2.14.** The choice principle $\text{PIT}$ is inconsistent in FSM.

*Proof.* By contradiction, assume that the choice principle $\text{PIT}$ is valid in FSM. Thus, every invariant Boolean algebra with $0 \neq 1$ has a maximal finitely supported ideal, and hence a maximal finitely supported filter. We prove that any equivariant filter of an arbitrary invariant Boolean algebra can be extended to a finitely supported maximal filter. Indeed, consider an invariant Boolean algebra $(B, \wedge, \vee, \cdot)$ and

---

9 Note that we cannot involve an equivalence result between $\text{UFT}$ and $\text{PIT}$ in FSM, similarly as in the ZF framework, unless we are able to prove such a result with respect to the finite support requirement from FSM.
let $\mathcal{F}$ be an equivariant filter in $B$. Therefore, $\mathcal{F}' = \{x' \mid x \in \mathcal{F}\}$ (where $x'$ represents the complement of $x$) is an equivariant ideal in $B$. We define the relation $\sim_{\mathcal{F}'}$ on $B$ by $x \sim_{\mathcal{F}'} y$ if and only if $(x \land y') \lor (y \land x') \in \mathcal{F}'$. Since the operations $\land$, $\lor$ and complement are all equivariant functions, and because $\mathcal{F}'$ is an equivariant subset of $B$, it follows that $\sim_{\mathcal{F}'}$ is also an equivariant subset of $B \times B$. Moreover, the quotient lattice $B/\mathcal{F} \overset{\text{def}}{=} B/\sim_{\mathcal{F}'}$ is an invariant set (with the $S_A$-action $\ast$ defined by $\pi \ast [x]_{\mathcal{F}'} = [\pi \cdot x]_{\mathcal{F}'}$, for all $\pi \in S_A, x \in B$). Thus, because $(B/\mathcal{F}, \overline{\lambda}, \overline{\nu})$ is also a Boolean algebra (according to the general theory of Boolean algebras), from Corollary 2.3, it follows that $(B/\mathcal{F}, \overline{\lambda}, \overline{\nu})$ is an invariant Boolean algebra, where the equivariant operations $\overline{\lambda}, \overline{\nu}$ on $B/\mathcal{F}$ are defined by $[x]_{\mathcal{F}'} \overline{\lambda} [y]_{\mathcal{F}'} = [x \land y]_{\mathcal{F}'}$, and $[x]_{\mathcal{F}'} \overline{\nu} [y]_{\mathcal{F}'} = [x \lor y]_{\mathcal{F}'}$, for all $[x]_{\mathcal{F}'}, [y]_{\mathcal{F}'} \in B/\mathcal{F}$. According to PIT, there exists a finitely supported maximal filter $G$ in $B/\mathcal{F}$. Consider the natural map from $B$ onto the corresponding quotient space, $f : B \to B/\mathcal{F}$ defined by $f(x) = [x]_{\mathcal{F}'}$, for all $x \in B$. By its definition, we have that $f$ is equivariant. According to Corollary 2.3, we have that $f^{-1}(G)$ is finitely supported by $\text{supp}(G)$. Moreover, $f^{-1}(G)$ is a maximal filter in $B$ such that $\mathcal{F} \subseteq f^{-1}(G)$. Thus, $f^{-1}(G)$ is a finitely supported maximal filter in $B$ that enlarges $\mathcal{F}$.

However, as it is proved in Proposition 5.2.2 form [123], there exists an invariant Boolean algebra having an equivariant filter that cannot be extended to a finitely supported ultrafilter. The related filter is the filter $f$ defined on page 151, line 1 from [123]. We obtain a contradiction, and so PIT fails in FSM.

Remark 2.5. It is worth noting that the relationship theorems from [88] cannot be always rephrased in FSM. For example, for proving the inconsistency of PIT we could not apply a result of form $\text{PIT} \implies \text{UFT}$ in FSM. More precisely, the result stated as Theorem 4.37 (1) $\implies$ (2) from [88] could not be translated in FSM.

This is because if the filter $\mathcal{F}$ in the invariant Boolean algebra $B$ (with the notations preserved from the related theorem) is only finitely supported (and not equivariant), then $B/\mathcal{F}$ is not necessarily an invariant set (it is only a finitely supported subset of $\wp(B)$), and so PIT cannot be applied to $B/\mathcal{F}$ which is not an invariant complete lattice.

Theorem 2.15. The choice principle $\text{ZL}$ is inconsistent in FSM.

Proof. Let us assume that $\text{ZL}$ is valid in FSM. Consider the invariant set $(A, \cdot)$ defined in Example 2.1(1) and the invariant set $\mathcal{F} := \wp_2(A)$ defined in the proof of Theorem 2.13. From Theorem 2.13, we know that there is no choice function on $\mathcal{F}$. Let $P$ be the set consisting of all finitely supported functions $f : \mathcal{F}' \to \cup \mathcal{F}$, where $\mathcal{F}' \subseteq \wp(f_\mathcal{F}(\mathcal{F}))$ and $f(X) \in X$ for all $X \in \mathcal{F}'$. Obviously, $P$ is non-empty. Indeed, if we pick $a, b \in A$, and we consider $\mathcal{F}' = \{\{a, b\}\}$, then the function $f : \mathcal{F}' \to \cup \mathcal{F}$ defined by $f(\{a, b\}) = a$ is supported by $\{a, b\}$, and so $f$ belongs to $P$. Moreover, we claim that $P$ is an invariant set. This means that $\pi \ast f \in P$, $\forall \pi \in S_A, f \in P$. Fix some $\pi \in S_A$ and $f \in P$ with $\text{domain}(f) = \mathcal{F}' \subseteq \wp(f_\mathcal{F}(\mathcal{F}))$. According to Proposition 2.1, $\pi \ast \mathcal{F}'$ is a finitely supported subset of $\mathcal{F}$. Moreover, $\pi \ast f$ is a function defined on $\pi \ast \mathcal{F}'$. Since $f$ is a finitely supported element from the $S_A$-set $\wp(\mathcal{F} \times \cup \mathcal{F})$, therefore, $\pi \ast f$ is also finitely supported.
according to Proposition 2.1, we have that $\pi \star f \in \mathcal{O}_{f_{\text{fs}}} (\mathcal{F} \times \cup \mathcal{F})$. Moreover, also $(\pi \star f)(\pi \star X) = \pi \cdot f(X) \in \pi \star X$ for all $X \in \mathcal{F}'$. Thus, $\pi \star f \in P$.

Consider the order $\sqsubseteq$ on $P$ defined by: ‘$f \sqsubseteq g$ iff $\text{domain}(f) \subseteq \text{domain}(g)$ and the restriction of $g$ to $\text{domain}(f)$ coincides with $f$’. Since $\text{domain}(\pi \star f) = \pi \star \text{domain}(f)$ for all $f \in P$ and $(\pi \star f)(\pi \star X) = \pi \cdot f(X)$ for all $X \in \text{domain}(f)$, a direct calculation show us that $\sqsubseteq$ is equivariant.

Since the union of the functions belonging to any finitely supported totally ordered subset $P'$ of $P$ is itself a finitely supported function (supported by $\text{supp}(P')$) and is an upper bound of $P'$ with respect to the relation $\sqsubseteq$, it follows that $P$ satisfies the conditions in the hypothesis of Zorn’s lemma. Thus, $P$ has a maximal element denoted by $g_0$. We claim that $\text{domain}(g_0) = \mathcal{F}$. Indeed, suppose there exists $X \in \mathcal{F}$ with $X \notin \text{domain}(g_0)$. Consider the function $g' = g_0 \cup \{(X,x)\} = \{(Y,g_0(Y)) \mid Y \in \text{domain}(g_0)\} \cup \{(X,x)\}$ where $x \in X$ is a fixed element. Clearly, $g'$ is a function defined on the finitely supported subset $\text{domain}(g_0) \cup \{X\}$ of $\mathcal{F}$. According to Proposition 2.5, $g'$ is supported by $\text{supp}(g_0) \cup \text{supp}(X) \cup \text{supp}(x)$. Therefore, $g'$ is an element of $P$ such that $g_0 \sqsubseteq g'$ and $g_0 \neq g'$. This contradicts the maximality of $g_0$.

Thus, $\text{domain}(g_0) = \mathcal{F}$, and so $g_0$ is a choice function on $\mathcal{F}$ which represents a contradiction. As a consequence, ZL is inconsistent in FSM. \hfill \Box

**Theorem 2.16.** The choice principles CC and PCC are inconsistent in FSM.

**Proof.** Let us suppose that CC is valid in FSM. We consider the countable family $(X_n)_n$ where $X_n$ is the set of all injective $n$-tuples from $A$. Since $A$ is infinite, it follows that each $X_n$ is non-empty. In FSM each $X_n$ is equivariant because $A$ is an invariant set and each permutation is a bijective function. Therefore, the family $(X_n)_n$ is equivariant and the mapping $n \mapsto X_n$ is also equivariant.

If we assume that CC is valid, then according to the formulation of CC in FSM, there exists a finitely supported choice function $f$ on $(X_n)_n$. Let $f(X_n) = y_n$ with each $y_n \in X_n$. Let $\pi \in \text{Fix}(\text{supp}(f))$. According to Proposition 2.5, and because each element $X_n$ is equivariant according to its definition, we obtain that $\pi \cdot y_n = \pi \cdot f(X_n) = f(\pi \star X_n) = f(X_n) = y_n$, where by $\star$ we denoted the $S_A$-action on $(X_n)_n$, and by $\cdot$ we denoted the $S_A$-action on $\cup X_n$. Therefore, each element $y_n$ is supported by $\text{supp}(f)$. However, since each $y_n$ is a finite tuple of atoms, we have $\text{supp}(y_n) = y_n$, $\forall n \in \mathbb{N}$. Since $\text{supp}(y_n) \subseteq \text{supp}(f)$, $\forall n \in \mathbb{N}$, we obtain $y_n \subseteq \text{supp}(f)$, $\forall n \in \mathbb{N}$. Since each $y_n$ has exactly $n$ elements, this contradicts the finiteness of $\text{supp}(f)$.

If we assume that PCC is valid, then according to the formulation of PCC in FSM, there exists an infinite subset $M$ of $\mathbb{N}$ and a finitely supported choice function $g$ on $(X_m)_{m \in M}$. Let $g(X_m) = y_m$ with each $y_m \in X_m$. As in the paragraph above we obtain $y_m \subseteq \text{supp}(g)$ for all $m \in M$. Since $y_m$ has exactly $m$ elements for each $m \in M$, and since $M$ is infinite, we contradict the finiteness of $\text{supp}(g)$. \hfill \Box

**Remark 2.6.** According to [51], the following implication holds in the ZF framework: PCC(fin) implies “Every infinite set $X$ has an infinite subset $Y$ such that $X \setminus Y$ is also infinite”. A similar result holds for Fin according to [105] and for KW according to [88]. However, we cannot directly conclude that such an implication holds in (can be reformulated in) FSM where only finitely supported objects are allowed.
We cannot say (without an appropriate proof which is consistent in FSM) that the following statement is valid: “Given any invariant set $X$, and any finitely supported family $\mathcal{F}$ of non-empty finite subsets of $X$, there exists a finitely supported choice function on $\mathcal{F}$ (i.e. $\text{AC}(\text{Fin})$ in FSM)’ implies ‘Every infinite invariant set $X$ has an infinite finitely supported subset $Y$ such that $X \setminus Y$ is also finitely supported and infinite’. Therefore, we cannot directly conclude that $\text{AC}(\text{fin})$ is false in FSM just because the statement “Every infinite set $X$ has an infinite subset $Y$ such that $X \setminus Y$ is also infinite” is false in FSM. Such a result requires a separate proof reformulated in terms of finitely supported objects. An example of how a ZF theorem is translated into the framework of invariant sets is Theorem 2.11.

Remark 2.6 justifies the non-triviality of Theorem 2.11, Theorem 2.12, Theorem 2.13, Theorem 2.14, Theorem 2.15 and Theorem 2.16. This non-triviality follows because we cannot prove an FSM result only by employing a ZF result without an additional proof that involves only finitely supported constructions. There exist many results which are valid in the ZF framework, but fail in FSM. Some related examples are presented in Section 3.6.

According to Theorem 2.11, since $\text{AC}(\text{fin}), \text{CC}$ and $\text{Fin}$ are inconsistent in FSM, the choice principles $\text{AC}, \text{DC}, \text{CC}, \text{PCC}, \text{UFT}, \text{OP}, \text{KW}, \text{RKW}$ and $\text{OEP}$ presented in Section 2.1 (and reformulated in terms of finitely supported objects) are also inconsistent in FSM. Since the theory of invariant sets makes sense even if the set of atoms is not countable, the inconsistency results presented in this section do not overlap on some related properties in the basic or in the second Fraenkel models of ZFA set theory (which are constructed by using countable sets of atoms) [95].

Also, the results in this paper do not follow immediately from [127] because in [127] the nominal sets are defined over countable sets of atoms, whilst we defined invariant sets over possible non-countable sets of atoms; in the viewpoint of [127] (i.e. if the set of atoms is countable) the inconsistency of the countable choice principles would be trivial. Since no information about the countability of the set of atoms is available in a general theory of invariant sets, the consistency of $\text{CC}(\text{fin})$ in FSM remains an open problem.

Note that, according to the definition of an FM set, the previous choice principles can as well be reformulated in terms of FM sets by informally replacing “finitely supported subset of an invariant set” with “FM set”. For example, $\text{AC}$ can be reformulated in the form: “Given any finitely supported family $\mathcal{F}$ of non-empty FM sets, there exists a finitely supported choice function on $\mathcal{F}$”, and so on. The inconsistency of various choice principles in the FM cumulative universe can be proved in a similar way as we proved the inconsistency of the related choice principles in FSM. It is obvious that the choice principles presented in Section 2.1 are inconsistent with the axioms of FM set theory.

If we look back, Theorem 2.11 seems to lose its importance. All the related choice principles compared in Theorem 2.11 are inconsistent in FSM. The reader might ask why we chose to present the difficult Theorem 2.11 instead of finding a simpler direct method to prove the inconsistency of each choice principle in FSM. The answer is represented by the remark that the proof of Theorem 2.11 also provides some other interesting choice and order properties of invariant sets.
From the proof of Theorem 2.11(4), we obtain the following.

**Theorem 2.17.** Let \((X, \cdot)\) be an invariant set. Let \(\mathcal{F}\) be the set of all finitely supported subsets \(Y\) of \(X\) with cardinality greater than or equal to 2. If there exists a family \((U_Y)_{Y \in \mathcal{F}}\) of non-empty proper finitely supported subsets of \(Y\) such that the mapping \(Y \mapsto U_Y\) is finitely supported, then there exists a finitely supported linear order on \(X\).

From the proof of Theorem 2.11(2), we obtain the following.

**Theorem 2.18.** Let \((U, \cdot)\) be an invariant set. Let us consider a finitely supported family \(\mathcal{F}\) of non-empty finite subsets of \(U\). If there exists a finitely supported linear order on \(U\), then there exists a finitely supported function defined on \(\mathcal{F}\) with the property that \(f(Y) \in Y\) for all \(Y \in \mathcal{F}\).

From the proof of Theorem 2.11(3), we obtain the following.

**Theorem 2.19.** Let \((X_n)\) be a sequence of finite subsets of an invariant set such that the mapping \(n \mapsto X_n\) is finitely supported (i.e. all \(X_n\) are supported by the same \(S\)). Let \(X = \bigcup (X_n \times \{n\})\). If there exists a finitely supported injection \(i : \mathbb{N} \to X\), then there exists an infinite subset \(M\) of \(\mathbb{N}\) and a sequence \((x_m)_{m \in M}\) with the properties that \(x_m \in X_m\), \(\forall m \in M\) and the mapping \(m \mapsto x_m\) is finitely supported.

### 2.8 Finiteness

In Section 2.1 we proved that the equivalence of various definitions of finiteness in ZF is a consequence of AC. According to Theorem 2.13, AC is inconsistent in FSM. Thus, the equivalence of various forms of finiteness may fail in the world of invariant sets. However, we are able to present some relationship results between several forms of finiteness in FSM. We consider the following definitions of finiteness.

**Definition 2.11 ([156]).** Let \(X\) be a finitely supported subset of an invariant set \(Y\).

- \(X\) is (1)-finite if it bijects with a finite ordinal;
- \(X\) is (2)-finite if either \(X = \emptyset\), \(X\) coincides with \(\{x\}\) for some \(x\), or \(X\) is of the form \(X_1 \cup X_2\) for some (2)-finite sets \(X_1\) and \(X_2\);
- \(X\) is (3)-finite if for any finitely supported directed family \(\mathcal{F}\) of finitely supported sets with the property that \(X\) is contained in the union of the members of \(\mathcal{F}\) there exists \(Z \in \mathcal{F}\) such that \(X \subseteq Z\);
- \(X\) is (4)-finite if for all increasing chains \(X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots\) such that the mapping \(n \mapsto X_n\) is finitely supported and \(X \subseteq \bigcup X_n\) there exists \(n \in \mathbb{N}\) such that \(X \subseteq X_n\);
- \(X\) is (5)-finite if it has no finitely supported injections into any of its proper subsets.

Similarly to [156] we are able to prove the following result.
Theorem 2.20. Let $X$ be a finitely supported subset of an invariant set $Y$. The following implications hold: $X$ is (1)-finite $\iff$ $X$ is (2)-finite $\iff$ $X$ is (3)-finite $\implies$ $X$ is (4)-finite $\implies$ $X$ is (5)-finite. No other implications hold in general.

Proof.  
• (1)-finite $\implies$ (2)-finite. If $X$ bijects with the finite ordinal $n$, then $X$ is of the form $\{x_0,x_1,\ldots,x_{n-1}\}$. By induction on $n$, it follows that $X$ is (2)-finite.

• (2)-finite $\implies$ (3)-finite. Let $\mathcal{F}$ be a directed family such that $X$ is contained in the union of the members of $\mathcal{F}$. If $X = \emptyset$, then $X$ is contained in any member of $\mathcal{F}$. If $X = \{x\}$, then there exists $Z \in \mathcal{F}$ such that $x \in Z$ and $X \subseteq Z$. Finally, if $X = X_1 \cup X_2$ where $X_1$ and $X_2$ are (2)-finite, then by induction there exist $Z_1, Z_2 \in \mathcal{F}$ such that $X_1 \subseteq Z_1$ and $X_2 \subseteq Z_2$. However, $\mathcal{F}$ is directed and there exists $Z_3 \subseteq \mathcal{F}$ such that $Z_1 \subseteq Z_3$ and $Z_2 \subseteq Z_3$. Therefore, $X \subseteq Z_3$.

• (3)-finite $\implies$ (1)-finite. Let $\mathcal{F}$ be the family of all (1)-finite subsets of $X$ ordered by inclusion. Since $X$ is finitely supported, it follows that $\mathcal{F}$ is supported by $\text{supp}(X)$. Moreover, since all the elements of $\mathcal{F}$ are finite sets, it follows that all the elements of $\mathcal{F}$ are finitely supported. Clearly, $\mathcal{F}$ is directed and $X$ is the union of the members of $\mathcal{F}$. Since $X$ is (3)-finite, there exists $Z \in \mathcal{F}$ such that $X \subseteq Z$. Therefore, $X$ is (1)-finite.

• (3)-finite $\implies$ (4)-finite. Let $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$ be an increasing chain such that the mapping $n \mapsto X_n$ is finitely supported and $X \subseteq \bigcup X_n$. It follows that $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$ is a finitely supported directed family all of whose elements are also (uniformly) finitely supported by $\text{supp}(n \mapsto X_n)$. Therefore, there exists $n \in \mathbb{N}$ such that $X \subseteq X_n$.

• (4)-finite $\not\implies$ (1)-finite. We have to provide a counterexample. We claim that the set $A$ of atoms is (4)-finite. We have to prove that each finitely supported increasing chain of subsets of $A$ must eventually become stationary. Indeed, if there exists an increasing chain $X_0 \subseteq X_1 \subseteq \ldots \subseteq A$ such that $n \mapsto X_n$ is supported by the finite set $S$, then each element $X_i$ of the chain must be supported by the same $S$. However, there are only finitely many such subsets of $A$ namely the subsets of $S$ and the supersets of $A \setminus S$. Therefore, there exists $n_0 \in \mathbb{N}$ such that $X_n = X_{n_0}, \forall n \geq n_0$. It follows that $A = X_{n_0}$ and $A$ is (4)-finite. However, $A$ is not (1)-finite.

• (4)-finite $\implies$ (5)-finite. Suppose that $X$ is (5)-infinite. Therefore, there exists a finitely supported injection $f : X \to X$ and an element $x \in X$ such that $x \notin \text{Im}(f)$. For each $n \in \mathbb{N}$ let $X_n = \{x, f(x), \ldots, f^n(x)\}$. Since $f$ is injective and $x \notin \text{Im}(f)$, it follows that $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$. Moreover, each element $X_n$ is supported by $\text{supp}(f) \cup \text{supp}(x)$. Let $Z_n = (X \setminus \bigcup_{i \in \mathbb{N}} X_i) \cup X_n$. Clearly, $X = \bigcup Z_n$. Moreover, each element $Z_n$ is supported by $\text{supp}(f) \cup \text{supp}(x) \cup \text{supp}(X)$. Therefore, the mapping $n \mapsto Z_n$ is finitely supported. However, there exists no $n \in \mathbb{N}$ such that $X = Z_n$, and so $X$ is not (4)-finite.

• (5)-finite $\not\implies$ (4)-finite. We have to provide a counterexample. The set $\mathcal{G}_{\text{fin}}(A) = \{B \subseteq A \mid |B| \text{ finite}\}$ is (4)-infinite. Indeed, consider $X_n = \{B \in \mathcal{G}_{\text{fin}}(A) \mid |B| \leq n\}$. Clearly, $X_0 \subseteq X_1 \subseteq \ldots \subseteq X_n \subseteq \ldots$ is an equivariant chain and $\mathcal{G}_{\text{fin}}(A) = \bigcup X_n$. However, there exists no $n \in \mathbb{N}$ such that $\mathcal{G}_{\text{fin}}(A) = X_n$. Therefore, $\mathcal{G}_{\text{fin}}(A)$ is (4)-infinite. We prove by contradiction that $\mathcal{G}_{\text{fin}}(A)$ is (5)-finite. Suppose
f : \wp_{\text{fin}}(A) \to \wp_{\text{fin}}(A) is an injection supported by the finite set S and there exists \(X_0 \in \wp_{\text{fin}}(A)\) such that \(X_0 \notin \text{Im}(f)\). We can form a sequence that starts at \(X_0\) and continues by setting \(X_{n+1} = f(X_n)\). Since \(f\) is injective and \(X_0 \notin \text{Im}(f)\), this sequence never repeats. However, \(X_{n+1} = \text{supp}(X_{n+1}) = \text{supp}(f(X_n)) \subseteq \text{supp}(f) \cup \text{supp}(X_n) = S \cup X_n\). Therefore, \(X_n \subseteq S \cup X_0, \forall n \in \mathbb{N}\). Since \(S \cup X_0\) has only a (1)-finite number of subsets, we contradict the statement that the sequence \((X_n)_n\) never repeats. Therefore, \(\wp_{\text{fin}}(A)\) is (5)-finite. 

\[\square\]

### 2.9 Freshness

**Definition 2.12.** If \(x \in A\) and \(y \in Y\) where \(Y\) is an invariant set, we say that \(x\) is fresh for \(y\) and denote this by \(x \# y\) if \(\{x\} \cap \text{supp}(y) = \emptyset\).

Since \(A\) is infinite, for any arbitrary element in an invariant set, we can always find a name outside its support. This means \(\forall x. \exists a \in A. a \# x\).

We can generalize this definition to arbitrary invariant sets.

**Definition 2.13.** Let \(X\) and \(Y\) be invariant sets. If \(x \in X\) and \(y \in Y\), we say that \(x\) is fresh for \(y\) and denote this by \(x \# y\) if \(\text{supp}(x) \cap \text{supp}(y) = \emptyset\).

From Proposition 2.1 and from the bijectivity of each permutation, the following Lemma follows immediately.

**Lemma 2.1.** Let \((X, \cdot)\) and \((Y, \circ)\) be invariant sets. If \(x \in X\) and \(y \in Y\) with \(x \# y\), then \(\pi \cdot x \# \pi \circ y\) for all \(\pi \in S_A\).

**Remark 2.7.** The following properties are consequences of the definition of support:

1. If \(a, b \in A\), then \((a \neq b \iff a \# b)\).
2. If \(a, b \in A\) and \(a, b \# x\), then \((ab) \cdot x = x\).

**Definition 2.14.** Let \(P\) be a predicate on \(A\). We say that \(\mathcal{N} a. P(a)\) if \(P(a)\) is true for all but finitely many elements of \(A\). \(\mathcal{N}\) is called the freshness quantifier.

Definition 2.14 also makes sense if \(P\) is a predicate in the logic of ZFA. It is worth noting that this quantifier was first introduced in [74]. In that paper, \(\mathcal{N}\) is called “the new quantifier”. It is denoted by a reflected sans-serif Roman letter by analogy with \(\forall\) the reflected A of “for all” and \(\exists\) the reflected E of “exists”.

**Proposition 2.9.** Let \(X\) be an invariant set and \(R \subseteq A \times X\) an equivariant subset. For each \(x \in X\) the following are equivalent:

1. \(\forall a. (a \# x \Rightarrow (a, x) \in R)\);
2. \(\forall a. (a, x) \in R\);
3. \(\exists a. (a \# x \land (a, x) \in R)\).
Proof. We prove that $[\forall a.(a \# x \Rightarrow (a,x) \in R)] \Rightarrow [\forall a.(a,x) \in R] \Rightarrow [\exists a.(a \# x \land (a,x) \in R)] \Rightarrow [\forall a.(a \# x \Rightarrow (a,x) \in R)].$

We know that the set $\{a \in A \mid a \# x\}$ is cofinite. If we suppose that $\forall a.(a \# x \Rightarrow (a,x) \in R)$, we have $\{a \in A \mid a \# x\} \subseteq \{a \in A \mid (a,x) \in R\}$, and so the set $\{a \in A \mid (a,x) \in R\}$ is cofinite, which means $\forall a.(a,x) \in R$.

Now, if we suppose $\forall a.(a,x) \in R$, then $\{a \in A \mid (a,x) \in R\}$ is cofinite, and so $\{a \in A \mid a \# x\} \cap \{a \in A \mid (a,x) \in R\}$ is the intersection of two cofinite subsets of the infinite set $A$ and so cannot be empty. Indeed, if we assume that the intersection $B \cap C$ of two cofinite subsets of $A$ is empty, we have $C_{B \cap C} = A$, and so $C_B \cup C_C = A$; since $C_B$ and $C_C$ are finite, we obtain $A$ is finite which contradicts the infiniteness of $A$. Therefore, $\exists a.(a \# x \land (a,x) \in R)$.

Let us suppose now that $\exists a.(a \# x \land (a,x) \in R)$ and let $b$ be an arbitrary atom such that $b \# x$. We have $(b,a) \cdot R = R$ because $R$ is equivariant. Since $(a,x) \in R$, we have $(b,a) \cdot (a,x) \in R$. However, $(b,a) \cdot (a,x) = ((b,a)(a) \cdot x) = (b,(b,a) \cdot x)$. Since $a,b \# x$, we also have $(b,a) \cdot x = x$, and hence $(b,x) = (b,a) \cdot (a,x) \in R$. \hfill \Box

Proposition 2.10. Let $p$ and $p'$ be properties of atomic names for which $\{a \in A \mid p\}$ and $\{a \in A \mid p'\}$ are finitely supported subsets of $A$. The following properties hold:

1. $\neg (\forall a. p)$ if and only if $\forall a. (\neg p)$;
2. $\forall a. (p \land p')$ if and only if $(\forall a. p) \land (\forall a. p')$.

Proof. Let $S = \{a \in A \mid p(a)\}$ and $S' = \{a \in A \mid p'(a)\}$. Since $S, S' \in \rho_{fs}(A)$, it follows that $S, S'$ have to be either finite or cofinite. Thus, $S$ is not cofinite if and only if $S$ is finite. However, $S$ is finite if and only if $S \subseteq C_S = A - S$ is cofinite. The first item of the proposition holds. Since the union of two sets is finite if and only if they are both finite, we have that $S \cap S'$ is cofinite if and only if both $S$ and $S'$ are cofinite. The second item of the proposition follows. \hfill \Box

From the propositional logic, the following corollary follows immediately.

Corollary 2.5. Let $p$ and $p'$ be properties of atomic names for which $\{a \in A \mid p\}$ and $\{a \in A \mid p'\}$ are finitely supported subsets of $A$. The following properties hold:

1. $\forall a. (p \lor p')$ if and only if $(\forall a. p) \lor (\forall a. p')$;
2. $(\forall a. p) \Rightarrow (\forall a. p')$ if and only if $\forall a. (p \Rightarrow p')$.

Some similar freshness properties also hold in the frameworks of ZFA and FM set theories.

Proposition 2.11. Suppose that $p((x_i)_i)$ is a formula in the logic of ZFA or FM, where the free variables of $p$ are listed in the set $(x_i)_i$, and $(x_i)_i$ are arbitrary distinct variables. Then $\forall a,b \in A. (p((x_i)_i) \Leftrightarrow p((ab) \cdot (x_i)_i))$, where $p((ab) \cdot (x_i)_i)$ denotes the result of substituting $(ab) \cdot x_j$ for all free occurrences $x_j$ from the set $(x_i)_i$ in $p$.

Proposition 2.11 is an equivariance property. A complete proof of this property can be found in [74]. The idea of proving this is to proceed by induction on the structure of the formula $p$, using the properties: $x = y \Rightarrow (ab) \cdot x = (ab) \cdot y$, $x \in y \Rightarrow (ab) \cdot x \in$
Proposition 2.12. Let \((x_i)_i\) be a set of distinct variables, and \(p\) a formula in the logic of FM. We have the following implications:

\[
[\forall a.\,(a\#(x_i)_i \Rightarrow p)] \Rightarrow [\forall a.\,p] \Rightarrow [\exists a \in A.\,(a\#(x_i)_i \land p)].
\]

**Proof.** We know the set \(\{a \in A \mid a\#(x_i)_i\}\) is cofinite. If we assume \(\forall a.\,(a\#(x_i)_i \Rightarrow p)\), we have \(\{a \in A \mid a\#(x_i)_i\} \subset \{a \in A \mid p\}\), and so \(\forall a.\,p\). Now, if we assume \(\forall a.\,p\), then \(\{a \in A \mid p\}\) is cofinite, and so \(\{a \in A \mid a\#(x_i)_i\} \cap \{a \in A \mid p\}\) is the intersection of two cofinite subsets of the infinite set \(A\), which cannot be empty. \(\square\)

Proposition 2.13. Let \((x_i)_i\) be a set of distinct variables, and \(p\) a formula in the logic of FM. If the free variables of the formula \(p\) are contained in the set of distinct variables \(\{a, (x_i)_i\}\), we have \(\exists a \in A.\,(a\#(x_i)_i \land p) \Rightarrow [\forall a.\,(a\#(x_i)_i \Rightarrow p)]\).

**Proof.** Let us suppose that for some \(a \in A\) we have \(a\#(x_i)_i \land p\). Then, by Proposition 2.11, we obtain that for every atom \(b\) we have \(p(b, (ab) \cdot (x_i)_i)\), where \(p(b, (ab) \cdot (x_i)_i)\) denotes the formula obtained when we substitute \(b\) for all free occurrences of \(a\) in \(p\), and \((ab) \cdot x_j\) for all free occurrences of \(x_j\) in \(p\). Now if we suppose \(b\#(x_i)_i\), we get \((ab) \cdot (x_i)_i = (x_i)_i\) (because we also have \(a\#(x_i)_i\)), and so we obtain \(p(b, (x_i)_i)\). \(\square\)

Propositions 2.12 and 2.13 correspond in the FM framework to Proposition 2.9.

### 2.10 Abstraction

#### 2.10.1 Formal Definition

We define abstraction in FSM by generalizing the notion of abstraction in the \(\lambda\)-calculus.

**Definition 2.15.** Let \(X\) be an invariant set and \(u \in X\). If \(B \subseteq A\), we define \(u\|B \overset{\text{def}}{=} \{\pi \cdot u \mid \pi \in \text{Fix}(B)\}\); \(u\|B\) is called the freshness orbit of \(u\) on \(B\).

**Remark 2.8.** \(u\|B\) is an equivalence class of the sets that are equal up to a renaming of atoms which are not in \(B\) (because for \(\pi \in \text{Fix}(B)\) we have \(u\|B = (\pi \cdot u)\|B\)). For example, we have \(a\|\{b\} = \{a, c, d, e, \ldots\}\).

Let us assume that the set of atoms \(A\) is an IFM set, i.e. \(A\) is equipped with the interchange function \(\cdot : S_A \times X \rightarrow X\) defined by \(\pi \cdot a = \pi(a)\) for all \(\pi \in S_A\) and all \(a \in A\).

**Definition 2.16.** Let \(X\) be an invariant set.
1. For \( a \in A \) and \( x \in X \) we define an abstractive element to be of the form \([a]x\), where \([a]x = \cap \{V \subseteq A \times X \mid (a,x) \in V \wedge \text{supp}(V) \subseteq \text{supp}(x) \setminus \{a\}\} \).

2. We define the abstraction function to be the function \( \text{abs} : A \times X \to [A]X = \{[a]x \mid a \in A \wedge x \in X\} \) defined by \((a,x) \to [a]x\).

**Theorem 2.21.** Let \( X \) be an invariant set. Then \([a]x = (a,x)\prod(\text{supp}(x) \setminus \{a\})\), for all \( a \in A \) and \( x \in X \). This means that \([a]x\) is the freshness orbit of \((a,x)\) on \( \text{supp}(x) \setminus \{a\} \).

**Proof.** Let \( U = (a,x)\prod(\text{supp}(x) \setminus \{a\}) \) and \( \pi \in \text{Fix}(\text{supp}(x) \setminus \{a\}) \). We have that \( \pi \cdot U = \{(\pi \cdot a', \pi \cdot x') \mid (a', x') \in U\} \). However, \((a', x') \in U\) only when \( a' = \pi' \cdot a \) and \( x' = \pi' \cdot x \) with \( \pi' \in \text{Fix}(\text{supp}(x) \setminus \{a\}) \). Since \( \text{Fix}(\text{supp}(x) \setminus \{a\}) \) is a group, we have \( \pi \cdot U = U \), which means that \( \text{supp}(U) \subseteq \text{supp}(x) \setminus \{a\} \). Since \((a,x) \in U\), we obtain that \( U \) is a member of the family whose intersection is involved in order to define \([a]x\). Thus, \([a]x \subseteq U\).

Conversely, we have \((a,x) \in [a]x \) and \( \pi \cdot [a]x = [a]x \) for all \( \pi \in \text{Fix}(\text{supp}(x) \setminus \{a\}) \). Therefore, for all \( \pi \in \text{Fix}(\text{supp}(x) \setminus \{a\}) \), we have \((\pi(a), \pi(x)) \in [a]x \), and so \( U \subseteq [a]x\). \(\square\)

**Corollary 2.6.** Let \( X \) be an invariant set, \( a \in A \) and \( x \in X \). Then we have \([a]x = \{((y, (ya) \cdot x)) \mid y \in A, y \neq a \text{ and } y \neq x\} \cup \{(a,x)\}\).

### 2.10.2 Motivation

The definition of abstractive element presented in this section is well motivated by the results presented in Section 2.2. In Theorem 2.3 we proved that the rule for \( \alpha \)-equivalence of \( \lambda \)-terms can be presented in terms of the operation of transposing two variables in a term. By employing the freshness quantifier, the related rule has the following form.

**Lemma 2.2.** The rule for \( \alpha \)-equivalence of \( \lambda \)-abstractions in Theorem 2.3

\[
(ba) \cdot t \sim (ba') \cdot t', \quad b \neq a, a' \text{ and } b \text{ do not occur int }, t'
\]

\[
\lambda a.t \sim \lambda a'.t'
\]

is the same as the rule

\[
\forall b.((ba) \cdot t \sim (ba') \cdot t')
\]

\[
\lambda a.t \sim \lambda a'.t'
\]

**Proof.** Let \( \Lambda \) be the set of \( \lambda \)-terms \( t \) presented in Example 2.4(1). Let us define \( R = \{(b, (a,t,a',t')) \mid (ba) \cdot t \sim (ba') \cdot t'\} \). \( R \) is an IFM set with the \( S_A \)-action defined in Example 2.1(1). \( \Lambda \) is also an invariant set (it is even an IFM set) with the \( S_A \)-action defined in Example 2.4(1). Therefore, \((A \times \Lambda \times A \times \Lambda)\) and \( A \times (A \times \Lambda \times A \times \Lambda) \) are invariant sets. For simplicity we shall denote all the \( S_A \)-actions by \( \cdot \). It is easy to prove that \( R \) is an equivariant subset of \((A \times (A \times \Lambda \times A \times \Lambda))\). Indeed, let \((b, (a,t,a',t'))\) be an arbitrary element of \( R \), and \( \pi \) an arbitrary element of \( S_A \).
Moreover, when choosing an element $c$, $A$ and symmetry result directly from the definition of $\sim$. According to Lemma 2.3, we have that $\pi$ coincides with $\alpha$-equivalence (Theorem 2.3) we have that $\pi \cdot (a, t, a', t') = (\pi(b), (\pi(a) \cdot (a', t')))$. Moreover, because $\sim$ coincides with $\alpha$-equivalence (Theorem 2.3) we have that $\pi \cdot (b, a) \cdot t \sim \pi \cdot (b' \cdot t')$, which means $(\pi \circ (b, a)) \cdot t \sim (\pi \circ (b', a')) \cdot t'$ from which $\pi \circ (b, a) \cdot t \sim (\pi \circ (b', a')) \cdot t'$ and finally $\pi \cdot (b, a) \cdot t \sim (\pi \circ (b', a')) \cdot t'$. This means $\pi \cdot (b, (a, t, a', t')) \in R$, and so $R$ is equivariant. The assertion “$b \neq a, a'$ and $b$ does not occur in $t, t'$” is the same as “$b \# a, a', t, t'$”. The desired result follows from Proposition 2.9.

This lemma suggests how to generalize the notion of $\alpha$-equivalence from the syntax trees of $\lambda$-terms to arbitrary objects in FSM. Let $X$ be an invariant set. Let $\sim_A$ be the binary relation on $A \times X$ defined by:

$$(a, x) \sim_A (b, y) \text{ if and only if } \mathcal{N}.((ca) \cdot x = (cb) \cdot y).$$

It is easy to prove that $\sim_A$ is an equivalence relation on $A \times X$. The reflexivity and symmetry result directly from the definition of $\sim_A$. The transitivity of $\sim_A$ is obtained from Proposition 2.10(2).

For an invariant set $X$ and arbitrary elements $x \in X$ and $a \in A$, the element $[a]x$ from Definition 2.16 (which has to be the natural generalization of $\lambda a. x$) should be the equivalence class of $(a, x)$ modulo $\sim_A$ (according to Lemma 2.2).

**Lemma 2.3.** Let $X$ be an invariant set, $x, y \in X$ and $a, b \in A$. Then $(a, x) \sim_A (b, y)$ if and only if either $a = b$ and $x = y$, or $b \neq a$, $b \# x$ and $y = (b, a) \cdot x$.

**Proof.** Let $x, y \in X$ and $a, b \in A$ with $(a, x) \sim_A (b, y)$. If $b = a$, then, clearly, $x = y$. So suppose $b \neq a$. If $(a, x) \sim_A (b, y)$ we have that $(da) \cdot x = (db) \cdot y$ for all but finitely many atoms $d$. Let $U$ be a finite set of atoms such that $(da) \cdot x = (db) \cdot y$ for all $d \in A - U$. Since $S = \text{supp}(a) \cup \text{supp}(x) \cup \text{supp}(b) \cup \text{supp}(y)$ is finite, we can choose an element $c \in A - (U \cup S)$. Thus, exists $c \# a, b, y$ and $(ca) \cdot x = (cb) \cdot y$ (1).

Since $c \# y$ and $b = (cb) \cdot c$, by Lemma 2.1, we also have $b \# (ca) \cdot y$ and hence $b \# (ca) \cdot x$. From Lemma 2.1, we have $(ca) \cdot b \# (ca) \cdot ((ca) \cdot x)$, and so $(ca) \cdot b \# x$. However, $b \# a, c$, and we obtain $(ca) \cdot b = b$ and $b \# x$.

We must prove that $y = (b, a) \cdot x$. First we make the remark that $(cb) \circ (ca) = (ba) \circ (cb)$ (2) which follows by easy calculation.

We have $y = (cb) \cdot ((ca) \cdot y) \overset{(1)}{=} (cb) \cdot ((ca) \cdot x) \overset{(2)}{=} (ba) \cdot ((cb) \cdot x) \overset{b \# x}{=} (ba) \cdot x$.

Conversely, let $y = (ba) \cdot x$ (3) and $b \# x$.

Since $A$ is not finite, the set of atoms $c$ for which $c \# a, x, b, y$ is cofinite. First we remark that $(cb) \circ (ba) = (ca) \circ (cb)$ (4) which follows by easy calculation.

Moreover, when $c \# a, x, b, y$ we also have $(cb) \cdot y \overset{(3)}{=} (cb) \cdot ((ba) \cdot x) \overset{(4)}{=} (ca) \cdot ((cb) \cdot x) \overset{c \# b}{=} (ca) \cdot x$. Therefore, $\mathcal{N}.((ca) \cdot x = (cb) \cdot y)$, which means $(a, x) \sim_A (b, y)$.

According to Lemma 2.3, we have that $(a, x) / \sim_A = \{(b, (ba) \cdot x) \mid b \in A \wedge (b = a \vee b \# x)\}$ which is exactly the element $[a]x$ in the view of Corollary 2.6.

Therefore, the abstractive element $[a]x$ coincides with the equivalence class of $(a, x)$ modulo $\sim_A$, and represents a natural generalization of $\lambda$-calculus abstraction.
2.10.3 Properties

We prove that \([A]X\) is an invariant set in the sense of Definition 2.4 whenever \(X\) is an invariant set.

**Proposition 2.14.** Let \((X, \cdot)\) be an invariant set. \([A]X\) can be organized as an \(S_A\)-set with the underlying set represented by the equivalence classes \((a, x)/\sim_A\) in \(A \times X\) and the \(S_A\)-action \(\cdot\) defined by \(\pi \cdot [a]x = [\pi(a)] \cdot x\) for all \(\pi \in S_A\) and all \([a]x \in A[X]\).

**Proof.** We prove first that the function \(\pi \cdot [a]x = [\pi(a)] \cdot x\) for all \(\pi \in S_A\) and all \([a]x \in A[X]\) is well defined, i.e. it does not depend on the chosen representatives for the equivalence classes modulo \(\sim_A\). Let \((a, x)\) and \((b, y)\) be two elements in the same equivalence class modulo \(\sim_A\), i.e. \([a]x = [b]y\). Then either \(a = b\) and \(x = y\), or \(b \neq a\) and \(y = (b \cdot x)\). If \(a = b\) and \(x = y\), then, clearly, \(\pi(a) = \pi(b)\) and \(\pi \cdot x = \pi \cdot y\). So suppose \(b \neq a\), \(b \neq x\) and \(y = (b \cdot x)\). Since \(\pi\) is one-to-one, it is clear that \(\pi(b) \neq \pi(a)\). According to Lemma 2.1, we also have \(\pi(b) \neq \pi(a)\). Now \(\pi \cdot y = \pi \cdot ((b \cdot x)\cdot x = ((\pi(b) \cdot \pi(a)) \cdot x = ((\pi(b) \cdot \pi(a))) \cdot (\pi \cdot x)\). From Lemma 2.3, we obtain \([\pi(a)] \cdot \pi \cdot x = [\pi(b)] \cdot \pi \cdot y\). Since the function \(\cdot\) is an \(S_A\)-action on \(X\), it is clear that \(\cdot [a]x\) is also an \(S_A\)-action on \([A]X\). \(\square\)

**Proposition 2.15.** Let \(X\) be an invariant set, \(a \in A\) and \(x \in X\). Then \([A]X\) is also an invariant set. Moreover, we have \(supp([a]x) = supp(x) \setminus \{a\}\).

**Proof.** Let \(V \subseteq A\) be a finite set which supports the element \((a, x)\) from \(A \times X\). Let \(\pi \in Fix(V)\). Therefore, \(\pi \cdot (a, x) = (a, x)\), which means \(\pi(a) = a\) and \(\pi \cdot x = x\). We have \(\pi \cdot [a]x = [\pi(a)] \pi \cdot x = [a]x\) which means \(V\) supports \([a]x\) in \([A]X\). However, \(supp([a]x)\) is the least finite set supporting \([a]x\). Whenever \(V\) supports \([a]x\), we have that \(V\) supports \([a]x\), and so \(supp([a]x) \subseteq V\). We know that \(supp((a, x)) = \cap \{V \mid V \text{ supports } (a, x)\}\), and hence \(supp([a]x) \subseteq supp((a, x)) = supp(x) \setminus \{a\}\) (1).

Let \(S \subseteq A\) be a finite set which supports \([a]x\) in \([A]X\). Let \(\pi \in Fix(S \cup \{a\})\). Since \(S\) supports \([a]x\), we have \(\pi \cdot [a]x = [a]x\). We also have \(\pi(a) = a\). According to Proposition 2.14, we obtain \([a]x = \pi \cdot [a]x = [\pi(a)] \pi \cdot x = [a] \pi \cdot x\). According to Lemma 2.3, we have \(\pi \cdot x = x\). Therefore, \(S \cup \{a\}\) supports \(x\) in \([A]X\). However, \(supp(x)\) is the least finite set supporting \(x\). Whenever \(S\) supports \([a]x\), we have that \(S \cup \{a\}\) supports \(x\), and so \(supp(x) \subseteq \{a\} \cup supp([a]x)\). Since we have already proved that \(supp([a]x) \subseteq supp(x) \cup \{a\}\), it remains to show that \(a \notin supp([a]x)\), that is, \(a \notin [a]x\). Since \(A\) is not finite, we can choose an atom \(b\) such that \(b \# a\). According to Lemma 2.3, we have \((b, (b \cdot a) \cdot x) \sim_A (a, x)\), and so \((b \cdot a) \cdot x = ((b \cdot a)(a))((b \cdot a) \cdot x) = [b](b \cdot a) \cdot x = [a]x\). However, \(b \# a\), and hence, by (1), we have \(b \# [a]x\). According to Lemma 2.1, we have \((b \cdot a) \cdot b \# (b \cdot a) \cdot [a]x\), and so \(a \# [a]x\). \(\square\)

**Example 2.5.**
- \([a](A \setminus \{a\}) = \{(a, A \setminus \{a\}), (b, A \setminus \{b\}), (c, A \setminus \{c\})\},\ldots\)
- \([a]\{a, b\} = \{(a, \{a, b\}), (c, \{c, b\}), (d, \{d, b\}), (e, \{e, b\}), \ldots\}.

From Lemma 2.3, we obtain the following result.
Proposition 2.16. Let \( X \) be an invariant set. Let \( a, b \in A \) and \( x, y \in X \). We have 
\[
[a]x = [b]y \text{ if and only if one of the following statements is true:}
\]
- \( a = b \) and \( x = y \);
- \( a \neq b \), \( b \# x \) and \( y = (b \cdot a) \cdot x \).

Corollary 2.7. Let \( X \) be an invariant set. Let \( a, b \in A \) and \( x, y \in X \). If we have 
\( c \# a, b, x, y \) and \( [a]x = [b]y \) then 
\( (ac) \cdot x = (bc) \cdot y \).

In the previous results about abstraction we can consider \( X \) to be the invariant set \( FM(A) \) and the elements of \( X \) to be the FM sets. Hence whenever \( x \) is an FM set the element \([a]x\) can be defined as in Definition 2.16. The element \([a]x\) will be equal to 
\[
\{(y, (ya) \cdot x) \mid y \in A, y \neq a \text{ and } y \# x\} \cup \{(a, x)\}
\]
which is an FM set because of axiom number 6 of FM set theory. Whenever \( a \in A \) and \( x \) is an FM set, we have 
\( \text{supp}([a]x) = \text{supp}(x) \setminus \{a\} \). Proposition 2.16 and Corollary 2.7 are valid when \( X \) is \( FM(A) \), i.e. \( x, y \) are FM sets.
Chapter 3
Algebraic Structures in Finitely Supported Mathematics

Abstract Finitely Supported Mathematics (FSM) is the mathematics developed in the framework of invariant/finitely supported structures. The aim of this chapter is to translate into FSM several algebraic concepts which were initially described using the Zermelo-Fraenkel axioms of set theory. We focus on multisets, generalized multisets, partially ordered sets and groups because these concepts are particularly relevant for experimental science. Moreover, we provide the main principles of translating a given algebraic concept into FSM. These principles are based on the remark that only finitely supported objects are allowed in FSM. We present in detail some FSM properties of the related algebraic structures, emphasizing the analogy between the results obtained in the framework of invariant sets and those obtained in the usual Zermelo-Fraenkel framework. This chapter may be read without using notions from higher-order logic, category theory, or the general equivariance principles for formulas in classical higher-order logic.

3.1 Multisets in Finitely Supported Mathematics

Ordinary sets are composed of pairwise different elements, which means no two elements are the same. If we accept multiple but finitely many occurrences of any element we get the notion of multiset, which comes to generalize the notion of set. There are many possibilities to define the notion of multiset; the most used procedure is counting the multiplicity of each element. In fact a multiset on $\Sigma$ is a function from $\Sigma$ to the set of positive integers $\mathbb{N}$, where each element in $\Sigma$ is associated with its multiplicity. For example, the invariants of a finite abelian group can be represented as a multiset. The prime factorization of a natural number $n$ is another multiset whose elements are primes. Even processes in an operating system can be seen as a multiset, and the examples can continue.

Multisets are used in computer science for quantitative analysis and models of resources. References [97, 98] are the earliest known references to the applications of multisets in computer science. Multisets and permutations of multisets are applied
3.1.1 Algebraic Properties of Multisets

**Definition 3.1.** Given a finite alphabet $\Sigma$, any function $f : \Sigma \to \mathbb{N}$ is called a multiset over $\Sigma$. The value of $f(a)$ is said to be the multiplicity of $a$. The set of all multisets over $\Sigma$ is denoted by $\mathbb{N}(\Sigma)$.

The additive structure of $\mathbb{N}$ induces an additive operation (sum) on multisets. On $\mathbb{N}(\Sigma)$ we define an additive law by:

$$+ : \mathbb{N}(\Sigma) \times \mathbb{N}(\Sigma) \to \mathbb{N}(\Sigma).$$
\[(f, g) \mapsto f + g\]

where \(f + g : \Sigma \to \mathbb{N}\) is defined pointwise by \((f + g)(a) = f(a) + g(a)\) for all \(a \in \Sigma\).

Since \(N(\Sigma)\) is formed by all functions from \(\Sigma\) to \(\mathbb{N}\), it is clear that \((N(\Sigma), +)\) is an abelian monoid, the identity being the empty multiset \(\theta\) such that \(\theta(a) = 0\) for all \(a \in \Sigma\). Since \((N(\Sigma), +)\) is an abelian monoid, it follows that \((N(\Sigma), +)\) is an \(\mathbb{N}\)-semimodule, i.e., a semimodule over the semiring \(\mathbb{N}\), with the scalar multiplication:

\[\cdot : \mathbb{N} \times N(\Sigma) \to N(\Sigma),\]

\[(n, f) \mapsto n \cdot f\]

where \(n \cdot f : \Sigma \to \mathbb{N}\) is defined pointwise by \((n \cdot f)(a) = n \cdot f(a)\), for all \(a \in \Sigma\) and \(n \in \mathbb{N}\).

**Proposition 3.1.** \((N(\Sigma), +)\) is a free abelian \(\mathbb{N}\)-semimodule.

**Proof.** If \(a \in \Sigma\), we consider the multiset \(\tilde{a} : \Sigma \to \mathbb{N}\) defined by

\[\tilde{a}(b) = \begin{cases} 1, & \text{for } b = a; \\ 0, & \text{for } b \in \Sigma \setminus \{a\}. \end{cases}\]

It is easy to check that every multiset \(f \in N(\Sigma)\) can be expressed as

\[f = \sum_{a \in \Sigma} f(a) \cdot \tilde{a}.\]

Since \(\Sigma\) is finite, the sum is finite. In fact, the set of multisets \(\tilde{\Sigma} = \{\tilde{a} \mid a \in \Sigma\}\) is a basis for the \(\mathbb{N}\)-semimodule \(N(\Sigma)\) since \(\{\tilde{a} \mid a \in \Sigma\}\) is also linearly independent. \(\square\)

Since \(N(\Sigma)\) is the free \(\mathbb{N}\)-semimodule with basis \(\tilde{\Sigma}\), it satisfies the universality property described in Proposition 3.2. We denote by \(j : \Sigma \to N(\Sigma)\) the function which maps each \(a \in \Sigma\) into \(\tilde{a} \in \tilde{\Sigma}\). It is clear that \(j\) is the composition of the standard inclusion \(i : \tilde{\Sigma} \to N(\Sigma)\), \(i(\tilde{a}) = \tilde{a}\) for all \(\tilde{a} \in \tilde{\Sigma}\), with the bijection of \(\Sigma\) onto \(\tilde{\Sigma}\) defined by \(a \mapsto \tilde{a}\).

**Proposition 3.2.** If \(M\) is any abelian monoid and \(f : \Sigma \to M\) an arbitrary function, then there is a unique homomorphism of abelian monoids \(g : N(\Sigma) \to M\) with \(g \circ j = f\), i.e., \(g(\tilde{a}) = f(a)\) for all \(a \in \Sigma\).

**Definition 3.2.** 1. • Adjoin one element to \(\Sigma\) and denote it by 1. A word on \(\Sigma\) is either the element 1 or a formal expression \(x_1x_2\ldots x_n\) where \(n \in \mathbb{N}\) and \(x_i \in \Sigma\).

• The juxtaposition of two words \(w = x_1x_2\ldots x_n\) and \(w' = y_1y_2\ldots y_m\) is the word \(w\#w' := x_1x_2\ldots x_ny_1y_2\ldots y_m\). Moreover, we define \(w\#1 = 1\#w = w\) for all words \(w\).

2. The free monoid \(\Sigma^*\) is the set of words on \(\Sigma\) with the monoid operation \#.

It is worth noting that the order and the multiplicity are important in a word \(w = x_1x_2\ldots x_n\). Another interesting remark is that, if \(\Omega\) is another alphabet with \(|\Sigma| = |\Omega|\) (they have the same cardinality), then \(\Sigma^* \cong \Omega^*\) (they are isomorphic monoids). The free monoid on \(\Sigma\) also satisfies the so-called universality property.
Theorem 3.1. For each monoid $M$ and each function $f : \Sigma \to M$, there exists a unique homomorphism of monoids $g : \Sigma^* \to M$ with $g \circ i = f$, where $i : \Sigma \to \Sigma^*$ is the standard inclusion of $\Sigma$ into $\Sigma^*$ which maps each element $a \in \Sigma$ into the word $a$.

We can compare multisets with vectors of natural numbers. It is known that, for $k \in \mathbb{N}$, $k \neq 0$, $\mathbb{N}^k$ is an abelian monoid with respect to addition of vectors. Moreover, $\mathbb{N}^k$ is free with respect to the canonical basis $B = \{e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \mid i = 1, \ldots, k\}$. If $\Sigma = \{a_1, \ldots, a_k\}$, then $\mathbb{N}(\Sigma) \cong \mathbb{N}^k$ as $\mathbb{N}$-semimodules and hence as abelian monoids.

We can connect all these views using the universal property of the free monoid $\Sigma^*$. (It can be connected by this property with any monoid, and not only with commutative ones as in the case of $\mathbb{N}(\Sigma)$.) If in the statement of Theorem 3.1, we replace $M$ with $\mathbb{N}(\Sigma)$, and $f : \Sigma \to M$ with $j : \Sigma \to \mathbb{N}(\Sigma)$ where $j$ maps each $a \in \Sigma$ into $\tilde{a}$, we get a function $g : \Sigma^* \to \mathbb{N}(\Sigma)$ such that $g \circ i = j$, where $i : \Sigma \to \Sigma^*$ is the standard inclusion of $\Sigma$ into $\Sigma^*$ which maps each element $a \in \Sigma$ into the word $a$. If $w = x_1x_2 \cdots x_m$, $x_i \in \Sigma$, $i = 1, \ldots, m$, then $g(w) = j(x_1) + j(x_2) + \cdots + j(x_m)$.

If for any alphabet $\{a_1, \ldots, a_k\}$, $k \in \mathbb{N}$, we denote by $|w|_{a_i}$ the number of appearances of the symbol $a_i$ in $w$, $g(w) = \sum_{i=1}^{k} |w|_{a_i} \cdot \tilde{a}_i$ is a surjective morphism, and we get the following result by using the isomorphism theorem for monoids.

Theorem 3.2. $\Sigma^*/\text{Ker } g \cong \mathbb{N}(\Sigma)$.

Remark 3.1. $\text{Ker } g$ is a congruence on $\Sigma^*$. Two words $w$ and $w'$ are in the same equivalence class with respect to $\text{Ker } g$ if and only if $g(w) = g(w')$; this is equivalent to $|w|_{a_i} = |w'|_{a_i}$ for all $i = 1, \ldots, k$. Moreover, for a multiset $f = \sum_{i=1}^{k} f(a_i) \cdot \tilde{a}_i$, its inverse image under $g$, namely $g^{-1}(f) = \{w \in \Sigma^* \mid |w|_{a_i} = f(a_i), i = 1, \ldots, k\}$ is the language consisting of words in which the number of appearance of the letter $a_i$ equals $f(a_i)$.

If $\Sigma = \{a_1, \ldots, a_k\}$, we define the Parikh image [115] $\varphi_{\Sigma} : \Sigma^* \to \mathbb{N}^k$ in the following way: if $w = x_1x_2 \cdots x_n$ then $\varphi_{\Sigma}(w)$ is the vector in $\mathbb{N}^k$ whose $i$-component is $\sum_{\substack{x_j = a_i \\ j = 1, \ldots, n}} 1$ for each $i = 1, \ldots, k$; if there is no $j$ such that $x_j = a_i$ the $i$-component of the vector is defined to be 0. Informally $\varphi_{\Sigma}(w)$ calculates the number of “occurrences” of each element from $\Sigma$ in $w$.

If in the statement of Proposition 3.2, we replace $M$ with $\mathbb{N}^k$ and $f : \Sigma \to M$ with the function $\varphi_{\Sigma} \circ i$ where $i : \Sigma \to \Sigma^*$ is the standard inclusion of $\Sigma$ into $\Sigma^*$ which maps each element $a_i \in \Sigma$ into the word $a_i$, then there is a unique homomorphism of abelian monoids $\psi_{\Sigma} : \mathbb{N}(\Sigma) \to \mathbb{N}^k$ with $\psi_{\Sigma} \circ j = \varphi_{\Sigma} \circ i$, that is, $\psi_{\Sigma}(\tilde{a}_i) = \varphi_{\Sigma}(a_i) = (0, \ldots, 0, 1, 0, \ldots, 0) = e_i$ for all $a_i \in \Sigma$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the vector in $\mathbb{N}^k$ all of whose components are 0 except the $i$-component which is 1.

Now, because $\psi_{\Sigma}$ maps each element one-to-one from a finite basis of $\mathbb{N}(\Sigma)$ into an element from a finite basis of $\mathbb{N}^k$, and $\mathbb{N}(\Sigma)$ and $\mathbb{N}^k$ have the same rank, we have that $\psi_{\Sigma} : \mathbb{N}(\Sigma) \to \mathbb{N}^k$ is an isomorphism, and
\[\psi_{\Sigma}(\sum_{i=1}^{k} f(a_i) \cdot \bar{a}_i) = (f(a_1), \ldots, f(a_k))\]
for each \(f \in \mathbb{N}(\Sigma)\).

Moreover, the properties of commutative diagrams show us that \(\psi_{\Sigma} \circ g = \varphi_{\Sigma}\), where \(g : \Sigma^* \rightarrow \mathbb{N}(\Sigma)\) is the homomorphism built before such that \(g \circ i = f\).

<table>
<thead>
<tr>
<th>(\mathbb{N}(\Sigma))</th>
<th>(\mathbb{N}^k)</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiset addition</td>
<td>vector addition</td>
</tr>
<tr>
<td>scalar product</td>
<td>scalar product</td>
</tr>
</tbody>
</table>

Several orders can be defined on the set \(\mathbb{N}(\Sigma)\). The most common is the order obtained from the definition of the subset relation on multisets.

**Definition 3.3.** A multiset \(f : \Sigma \rightarrow \mathbb{N}\) is a *subset* of a multiset \(g : \Sigma \rightarrow \mathbb{N}\) (denoted by \(f \subseteq g\)) if and only if \(f(x) \leq g(x)\) for all \(x \in \Sigma\).

Clearly, \((\mathbb{N}(\Sigma), \leq)\) is a partially ordered set. Another multiset order is the Dershowitz and Manna order [60] which is a main tool of many orders used to prove the finite termination of programs and also of term rewriting systems [59].

**Definition 3.4.** Let us suppose there exists a strict order \(<\) on \(\Sigma\). We define the *Dershowitz and Manna (DM) strict order* \(\ll_{DM}\) on \(\mathbb{N}(\Sigma)\) by \(f \ll_{DM} g\) if and only if there exist \(h, k \in \mathbb{N}(\Sigma)\) with the following properties:

1. \(\theta \neq h \subseteq g\)
2. \(f = (g - h) + k\)
3. for all \(y \in \Sigma\) with \(k(y) > 0\), there exists \(x \in \Sigma\) with \(h(x) > 0\) and \(y < x\).

The DM definition is difficult to use in order to prove that two multisets are not related by an inclusion. An equivalent definition is presented in [93].

**Definition 3.5.** Let us suppose there exists a strict order \(<\) on \(\Sigma\). We define the *Huet and Oppen (HO) strict order* \(\ll_{HO}\) on \(\mathbb{N}(\Sigma)\) by \(f \ll_{HO} g\) if and only if the following properties are satisfied:

1. \(f \neq g\)
2. for all \(y \in \Sigma\) with \(f(y) > g(y)\), there exists \(x \in \Sigma\) with \(y < x\) and \(f(x) < g(x)\).

**Theorem 3.3.** The orderings \(\ll_{DM}\) and \(\ll_{HO}\) are equivalent.

**Proof.** Suppose \(f \ll_{DM} g\). Since \(\theta \neq h\), we obtain \(f \neq g\). Indeed, if \(f = g\), we obtain \(h = k\), and since \(\exists y \in \Sigma. k(y) = h(y) > 0\), we obtain \(x \in \Sigma\) with \(k(x) = h(x) > 0\) and \(y < x\). By repeatedly applying Definition 3.4(3), we obtain an infinite chain \(y < x < z < \ldots\) in \(\Sigma\) which contradicts the finiteness of \(\Sigma\). Let \(y \in \Sigma\) such that \(f(y) > g(y)\). Then \(k(y) > 0\). According to Definition 3.4(3), there exists \(x \in \Sigma\) with \(h(x) > 0\) and \(y < x\). If \(f(x) < g(x)\) we are finished. If \(f(x) \geq g(x)\), since \(h(x) > 0\), we obtain \(k(x) > 0\) and we again apply Definition 3.4(3). Since we cannot have an
infinite chain in $\Sigma$ (which would be obtained if we were able to repeatedly apply Definition 3.4(3)), we find an element $z \in \Sigma$ with $y \prec z$ and $f(z) < g(z)$.

Conversely, suppose $f \ll_{HO} g$. Let us define $h(x) = \max\{g(x) - f(x), 0\}$ for all $x \in \Sigma$, and $k(x) = \max\{f(x) - g(x), 0\}$ for all $x \in \Sigma$. Items 2 and 3 from Definition 3.4 follow directly. Let us prove that $\theta \neq h \subseteq g$. According to the definition of $h$, we have $h \subseteq g$. Since $f \neq g$, there exists $y \in \Sigma$ with $f(y) \neq g(y)$. If $f(y) < g(y)$ we have $h(y) > 0$. If $f(y) > g(y)$, there exists $x \in \Sigma$ with $y \prec x$ and $f(x) < g(x)$. Therefore, $h(x) > 0$. In both cases $\theta \neq h$. $\square$

Since $\ll_{DM}$ and $\ll_{HO}$ are equivalent, we denote these order relations by $\ll$.

### 3.1.2 Multisets over Infinite Alphabets

We now formalize the concept of multisets in FSM. According to Example 2.1(4), we already know that $\mathbb{N}$ is an $S_A$-set with the $S_A$-action $\cdot : S_A \times \mathbb{N} \to \mathbb{N}$ defined by $\pi \cdot x := x$ for all $\pi \in S_A$ and $x \in \mathbb{N}$. Also $\mathbb{N}$ is an invariant set because for each $x \in \mathbb{N}$ we have that $\emptyset$ supports $x$. Moreover, $\text{supp}(x) = \emptyset$ for each $x \in \mathbb{N}$.

**Proposition 3.3.** Let $(\Sigma, \cdot)$ be an invariant set (possible infinite), and $f : \Sigma \to \mathbb{N}$ a function such that its algebraic support $S_f \triangleq \{x \in \Sigma \mid f(x) \neq 0\}$ is finite. Then $f$ is finitely supported and $\text{supp}(f) = \text{supp}(S_f)$.

**Proof.** A function $f : \Sigma \to \mathbb{N}$ is finitely supported in the sense of Definition 2.7 if and only if it is finitely supported with respect to the permutation action $\ast$ in the sense of Definition 2.3. However, on $\mathbb{N}$ we have defined the trivial action $(\pi, x) \mapsto x$, and hence the $S_A$-action $\ast$ on $\mathbb{N}^\Sigma$ is given by $(\pi \ast f)(x) = f(\pi^{-1} \cdot x)$ for all $\pi \in S_A$, $f \in \mathbb{N}^\Sigma$ and $x \in \Sigma$. Let $f : \Sigma \to \mathbb{N}$ be an algebraically finitely supported function. Let $S_f = \{a_1, \ldots, a_k\}$, and $S = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k)$. We have to prove that $S$ supports $f$. Let $\pi \in \text{Fix}(S)$. We have that $\pi \in \text{Fix}(\text{supp}(a_i))$ for each $i \in \{1, \ldots, k\}$. Therefore, $\pi \cdot a_i = a_i$ for each $i \in \{1, \ldots, k\}$ because $\text{supp}(a_i)$ supports $a_i$ for each $i \in \{1, \ldots, k\}$. However, $f = \sum f(a) \cdot \tilde{a} = \sum_{a \in S_f} f(a) \cdot \tilde{a}$. A simple calculation show us that $\pi \ast f = \sum_{a \in S_f} f(a) \cdot (\pi \cdot \tilde{a})$. Therefore, $\pi \ast f = f$ for each $\pi \in \text{Fix}(S)$. Thus, $f$ is finitely supported and $\text{supp}(f) \subseteq S$. However, according to Proposition 2.2, we have $S = \text{supp}(S_f)$. It remains to prove that $\text{supp}(S_f) \subseteq \text{supp}(f)$.

We prove that $\text{supp}(f)$ supports $S_f$. Let $\pi \in \text{Fix}(\text{supp}(f))$. According to Proposition 2.4, we have that $f(\pi \cdot x) = f(x), \forall x \in \Sigma$. Thus, for each $x \in S_f$ and each $\pi \in \text{Fix}(\text{supp}(f))$ we have $\pi \cdot x \in S_f$. Therefore, $\pi \ast S_f \subseteq S_f$ for each $\pi \in \text{Fix}(\text{supp}(f))$, where $\ast$ is the $S_A$-action on $\varphi(\Sigma)$ defined as in Subsection 2.4.1. We remark that $\pi \in \text{Fix}(\text{supp}(f))$ iff $\pi^{-1} \in \text{Fix}(\text{supp}(f))$. Thus, for $\pi \in \text{Fix}(\text{supp}(f))$, we also have $\pi^{-1} \ast S_f \subseteq S_f$, which means $\pi \ast (\pi^{-1} \ast S_f) \subseteq \pi \ast S_f$, and $S_f \subseteq \pi \ast S_f$. Therefore, $\pi \ast S_f = S_f$ for each $\pi \in \text{Fix}(\text{supp}(f))$. According to Definition 2.6, we have that $\text{supp}(f)$ supports $S_f$. Since the support of $S_f$ is the least finite set supporting $S_f$, we obtain that $\text{supp}(S_f) \subseteq \text{supp}(f)$. $\square$
Corollary 3.1. If \( f : A \to \mathbb{N} \) is a function such that \( S_f \) is finite, then \( S_f = \text{supp}(f) \).

Proof. The result follows because \( S_f \) is a finite subset of \( A \), and so \( S_f = \text{supp}(S_f) \).

According to Proposition 3.3, the notion of algebraic support of a multiset represents an extension of the notion of support from the framework of invariant sets. In FSM, multisets over finite alphabets can be replaced by algebraically finitely supported multisets over possibly infinite alphabets.

Definition 3.6. Given an invariant set \((\Sigma, \cdot)\) (possible infinite), any function \( f : \Sigma \to \mathbb{N} \) with the property that \( S_f \) is finite is called an extended multiset over \( \Sigma \). The set of all extended multisets over \( \Sigma \) is denoted by \( \mathbb{N}_{\text{ext}}(\Sigma) \).

We remark that each function \( f \in \mathbb{N}_{\text{ext}}(\Sigma) \) can be expressed as \( f = \sum_{a \in \Sigma} f(a) \cdot \tilde{a} \).

Since \( S_f \) is finite, the previous sum is finite. Therefore, \( \mathbb{N}_{\text{ext}}(\Sigma) \) is a free abelian monoid with basis \( \Sigma \). Whenever \( \Sigma \) is finite, \( \mathbb{N}_{\text{ext}}(\Sigma) = \mathbb{N}(\Sigma) \).

Definition 3.7. An invariant monoid is a triple \((M, +, \cdot)\) such that the following conditions are satisfied:

- \((M, +, 0)\) is a monoid.
- \((M, \cdot)\) is an invariant set.
- for each \( \pi \in S_A \) and each \( x, y \in M \) we have \( \pi \cdot (x + y) = \pi \cdot x + \pi \cdot y \) and \( \pi \cdot 0 = 0 \).

The relation required in the third part of Definition 3.7 is justified by the fact that in FSM the internal operation in \( M \) has to be equivariant, that is, the internal operation in \( M \) has itself to be an invariant set if we see it as a subset of \((M \times M) \times M\). Hence the function \( f : M \times M \to M \) defined by \( f(m_1, m_2) = m_1 + m_2 \) must be equivariant (the \( S_A \)-action on \( M \times M \) is defined as in Subsection 2.4.2). According to Corollary 2.3, the equivariance of \( f \) is equivalent to \( f(\pi \cdot (m_1, m_2)) = \pi \cdot f(m_1, m_2) \) for all \( \pi \in S_A \) and \((m_1, m_2) \in M \times M \).

Remark 3.2. If \((M, +, \cdot)\) is an invariant monoid we can easily remark that \( \pi \cdot (k \cdot x) = k \cdot (\pi \cdot x) \) for each \( \pi \in S_A, x \in M \) and \( k \in \mathbb{N} \). There is no confusion if we denote by \( \cdot \) both scalar multiplication on \( M \) and the \( S_A \)-action on \( M \). Scalar multiplication on \( M \) is a function whose domain is \( \mathbb{N} \times M \), whilst the \( S_A \)-action on \( M \) is a function whose domain is \( S_A \times M \).

According to Proposition 3.1, we know that \((\mathbb{N}(\Sigma), +)\) is a free abelian monoid if we work in standard ZF set theory. Analogously, \((\mathbb{N}_{\text{ext}}(\Sigma), +)\) is a free abelian monoid.

In FSM we have the following result.

Theorem 3.4. \( \mathbb{N}_{\text{ext}}(\Sigma) \) is a free abelian invariant monoid whenever \((\Sigma, \cdot)\) is an invariant set.
\textbf{Proof.} We already know that \((N_{\text{ext}}(\Sigma), +)\) is an abelian monoid, where \(f + g: \Sigma \rightarrow \mathbb{N}\) is defined pointwise by \((f + g)(a) = f(a) + g(a)\) for all \(a \in \Sigma\). Also, \(\pi \cdot f \in N_{\text{ext}}(\Sigma)\) for all \(f \in N_{\text{ext}}(\Sigma)\), where \(\cdot\) is the standard \(S_A\)-action on \(\mathbb{N}^2\). According to Proposition 3.3, we have that \((N_{\text{ext}}(\Sigma), \cdot)\) is an invariant set with the \(S_A\)-action \(\cdot: S_A \times N_{\text{ext}}(\Sigma) \rightarrow N_{\text{ext}}(\Sigma)\) defined by \((\pi \cdot f)(x) = f(\pi^{-1} \cdot x)\) for all \(\pi \in S_A, f \in N_{\text{ext}}(\Sigma)\) and \(x \in \Sigma\). Let \(f, g \in N_{\text{ext}}(\Sigma)\). For each \(x \in \Sigma\) we have \((\pi \cdot f + \pi \cdot g)(x) = (f + g)(\pi^{-1} \cdot x) = f(\pi^{-1} \cdot x) + g(\pi^{-1} \cdot x) = (\pi \cdot f)(x) + (\pi \cdot g)(x) = ((\pi \cdot f)(x) + (\pi \cdot g)(x))\). Hence \(\pi \cdot (f + g) = \pi \cdot f + \pi \cdot g\).

As in the proof of Proposition 3.1, every extended multiset \(f \in N_{\text{ext}}(\Sigma)\) can be expressed as \(f = \sum_{a \in S_f}^{\Sigma} f(a) \cdot \tilde{a}\), where for each \(a \in \Sigma\) the multiset \(\tilde{a}: \Sigma \rightarrow \mathbb{N}\) is defined as in the proof of Proposition 3.1. According to Proposition 3.3, we know that \(\tilde{a}\) is finitely supported for each \(a \in \Sigma\). Therefore, \(f = \sum_{a \in \Sigma}^{\Sigma} f(a) \cdot \tilde{a} = \sum_{a \in S_f}^{\Sigma} f(a) \cdot \tilde{a}\) is well formed in FSM, and \(N_{\text{ext}}(\Sigma)\) is a free abelian invariant monoid. \hfill \Box

For invariant monoids we also have a universality property which corresponds to Proposition 3.2 in FSM.

\textbf{Theorem 3.5.} Let \((\Sigma, \cdot)\) be an invariant set. Let \(j: \Sigma \rightarrow N_{\text{ext}}(\Sigma)\) be the function which maps each \(a \in \Sigma\) into \(\tilde{a} \in \tilde{S}\). If \((M, +, \cdot)\) is an arbitrary abelian invariant monoid and \(\varphi: \Sigma \rightarrow M\) is an arbitrary finitely supported function, then there exists a unique finitely supported homomorphism of abelian monoids \(\psi: N_{\text{ext}}(\Sigma) \rightarrow M\) with \(\psi \circ j = \varphi\), i.e. \(\psi(\tilde{a}) = \varphi(a)\) for all \(a \in \Sigma\). Moreover, if a finite set \(S\) supports \(\varphi\), then the same set \(S\) supports \(\psi\). Therefore, if \(\varphi\) is equivariant, then \(\psi\) is also equivariant.

\textbf{Proof.} First we show that the statement of the theorem is well formed in FSM. We know that in FSM only objects with finite support are allowed. For this, we have to prove that \(j\) is finitely supported.

According to Proposition 2.3, we know that \(N_{\text{ext}}(\Sigma)^S\) is an \(S_A\)-set with the \(S_A\)-action \(\triangleright: S_A \times N_{\text{ext}}(\Sigma)^S \rightarrow N_{\text{ext}}(\Sigma)^S\) defined by \((\pi \triangleright f)(x) = \pi \cdot f(\pi^{-1} \cdot x)\) for all \(\pi \in S_A, f \in N_{\text{ext}}(\Sigma)^S\) and \(x \in \Sigma\) (the \(S_A\)-action on \(N_{\text{ext}}(\Sigma)\) is denoted by \(\cdot\)). A function \(f: \Sigma \rightarrow N_{\text{ext}}(\Sigma)\) is finitely supported in the sense of Definition 2.7 if and only if it is finitely supported with respect to the permutation action \(\triangleright\). We prove that \(j\) is equivariant. In the view of Corollary 2.3 we must prove that \(j(\pi \cdot x) = \pi \cdot j(x)\) for each \(\pi \in S_A\) and each \(x \in \Sigma\). Let \(\pi \in S_A\) and \(x \in \Sigma\) be arbitrary elements. For each \(y \in \Sigma\) we have (by the definition of \(j\)) that

\[(j(\pi \cdot x))(y) = \begin{cases} 1, & \text{for } \pi \cdot x = y; \\ 0, & \text{for } \pi \cdot x \neq y. \end{cases}\]

Also

\[(\pi \cdot j(x))(y) = j(x)(\pi^{-1} \cdot y) = \begin{cases} 1, & \text{for } x = \pi^{-1} \cdot y; \\ 0, & \text{for } x \neq \pi^{-1} \cdot y. \end{cases} = \begin{cases} 1, & \text{for } \pi \cdot x = y; \\ 0, & \text{for } \pi \cdot x \neq y. \end{cases}\]

Hence \(j(\pi \cdot x) = \pi \cdot j(x)\) for each \(\pi \in S_A\) and each \(x \in \Sigma\), which means that \(j\) has empty support.
The homomorphism $\psi$ will be defined in the same way as the homomorphism $g$ in Proposition 3.2. As in the standard theory of abelian monoids (or free $\mathbb{N}$-semimodules) the homomorphism $\psi$ is defined by $\psi(f) = \sum_{a \in S_f} f(a) \cdot \varphi(a)$ whenever $f = \sum_{a \in S_f} f(a) \cdot \tilde{a}$. We must prove only that $\psi$ is finitely supported because the other properties of $\psi$ required in the statement of the theorem have standard proofs as in the classical theory of monoids (see Proposition 3.2 or the proof of Proposition 2.34 in [134]). According to Proposition 2.3, we know that the classical theory of monoids (see Proposition 3.2 or the proof of Proposition 2.3) requires $\psi$ is equivariant and $\psi$ is a monoid homomorphism, we obtain $\psi(\pi * f) = \psi(\sum_{a \in S_f} f(a) \cdot (\pi * \tilde{a})) = \psi(\sum_{a \in S_f} f(a) \cdot (\tilde{\pi} * a)) = \sum_{a \in S_f} f(a) \cdot \psi(\tilde{\pi} * a) = \sum_{a \in S_f} f(a) \cdot \varphi(\tilde{\pi} \cdot a)$. Also $\pi \circ \psi(f) = \pi \circ (\sum_{a \in S_f} f(a) \cdot \varphi(a)) = \sum_{a \in S_f} f(a) \cdot (\pi \circ \varphi(a)) = \sum_{a \in S_f} f(a) \cdot (\pi \cdot a)$; the second equality follows because $(M, +, \circ)$ is an invariant monoid and the third because $\pi$ fixes $supp(\varphi)$ pointwise. Therefore, $S$ supports $\psi$.

In the previous subsection we established a connection between $\mathbb{N}(\Sigma)$ and the free monoid on $\Sigma$ denoted by $\Sigma^*$. Our aim is to prove that the results obtained in the previous subsection in the usual ZF framework can be translated into FSM.

**Theorem 3.6.** $\Sigma^*$ is an invariant monoid whenever $(\Sigma, \cdot)$ is invariant set.

**Proof.** From the definition of $\Sigma^*$, we know that $(\Sigma^*, \#)$ is a monoid.

We also claim that $(\Sigma^*, \hat{\cdot})$ is an invariant set with the $S_A$-action $\hat{\cdot} : S_A \times \Sigma^* \to \Sigma^*$ defined by $\pi \hat{\cdot} x_1 x_2 \ldots x_l = (\pi \cdot x_1) \ldots (\pi \cdot x_l)$ for all $\pi \in S_A$ and $x_1 x_2 \ldots x_l \in \Sigma^* \setminus \{1\}$, and $\pi \hat{\cdot} 1 = 1$ for all $\pi \in S_A$. We have that $\hat{\cdot} : S_A \times \Sigma^* \to \Sigma^*$ is a group action of $S_A$ on $\Sigma^*$ in the sense of Definition 2.2 because $\hat{\cdot} : S_A \times \Sigma \to \Sigma$ is an $S_A$-action on $\Sigma$ and it satisfies the axioms of a group action on $\Sigma$ presented in Definition 2.2.

We prove that each element $x_1 x_2 \ldots x_n$ in $\Sigma^*$ is finitely supported. Let $x = x_1 x_2 \ldots x_n$ be an arbitrary element from $\Sigma^*$ and $U_x = supp(x_1) \cup \ldots \cup supp(x_n)$. Let $\pi \in Fix(U_x)$. We have $\pi \hat{\cdot} x_1 x_2 \ldots x_n = (\pi \cdot x_1) \ldots (\pi \cdot x_n)$. However, $\pi$ fixes pointwise the support of each $x_i$, $i = 1, \ldots, n$, and hence $\pi \cdot x_i = x_i$, $\forall i \in \{1, \ldots, n\}$. Thus, $\pi \hat{\cdot} x_1 x_2 \ldots x_n = x_1 x_2 \ldots x_n$ for each $\pi \in Fix(U_x)$, and so $U_x$ supports $x$. By direct calculation, we can also prove that $\Sigma^*$ satisfies the axioms of an invariant monoid. \qed

Theorem 3.1 which represents the universality property for $\Sigma^*$ in the ZF framework has a corresponding result in FSM.

**Theorem 3.7.** Let $(\Sigma, \circ_\Sigma)$ be an invariant set. Let $i : \Sigma \to \Sigma^*$ be the standard inclusion of $\Sigma$ into $\Sigma^*$ which maps each element $a \in \Sigma$ into the word $a$. If $(M, \cdot, \circ_M)$ is an arbitrary invariant monoid and $\varphi : \Sigma \to M$ is an arbitrary finitely supported
function, then there exists a unique finitely supported homomorphism of monoids \( \psi : \Sigma^* \to M \) with \( \psi \circ i = \varphi \). Moreover, if a finite set \( S \) supports \( \varphi \), then the same set \( S \) supports \( \psi \). Therefore, if \( \varphi \) is equivariant, then \( \psi \) is also equivariant.

Proof. First we show that the statement of the theorem is well formed in FSM. For this, we have to prove that \( i \) is finitely supported. According to Proposition 2.3, we know that \((\Sigma^*)^2\) is an \( S_A \)-set with the \( S_A \)-action \( \triangleright : S_A \times (\Sigma^*)^2 \to (\Sigma^*)^2 \) defined by \((\pi \triangleright f)(x) = \pi \tilde{x}(f(\pi^{-1} \circ \Sigma \cdot x))\) for all \( \pi \in S_A \), \( f \in (\Sigma^*)^2 \) and \( x \in \Sigma \). A function \( f : \Sigma \to \Sigma^* \) is finitely supported in the sense of Definition 2.7 if and only if it is finitely supported with respect to the permutation action \( \triangleright \). We prove that \( i \) is equivariant.

In the view of Corollary 2.3 we must prove that \( i(\pi \circ \Sigma x) = \pi \tilde{x}(i(x)) \) for each \( \pi \in S_A \) and each \( x \in \Sigma \). Let \( \pi \in S_A \) and \( x \in \Sigma \) be arbitrary elements. From the definition of \( i \), we know that \( i(\pi \circ \Sigma x) = \pi \circ \Sigma x \). From the definition of \( \tilde{x} \), we know that \( \pi \tilde{x}(i(x)) = \pi \tilde{x}x = \pi \circ \Sigma x \). Hence \( \pi \triangleright i = i \) for all \( \pi \in S_A \), which means \( i \) is equivariant and hence finitely supported.

If \((M, \cdot, \circ_M)\) is an invariant monoid, then, clearly, \((M, \cdot)\) is a monoid and from the general theory of monoids we can define a unique homomorphism of monoids \( \psi : \Sigma^* \to M \) with \( \psi \circ i = \varphi \). It remains to prove that \( \psi \) is indeed finitely supported.

Let us consider \( S = supp(\varphi) \). Thus, by Proposition 2.4, we have \( \varphi(\pi \circ \Sigma x) = \pi \circ_M \varphi(x) \) for all \( x \in \Sigma \) and \( \pi \in Fix(S) \). We have to prove that \( S \) supports \( \psi \). Let \( \pi \in Fix(S) \). According to Proposition 2.4, it is sufficient to prove that \( \psi((\pi \tilde{x}x_1x_2\ldots x_n) = \pi \circ_M \psi(x_1x_2\ldots x_n) = \pi \circ_M \varphi(x_1) \cdot \varphi(x_2) \cdot \ldots \cdot \varphi(x_n) \). Since \((M, \cdot, \circ_M)\) is an invariant monoid, we have \( \pi \circ_M \psi(x_1x_2\ldots x_n) = \pi \circ_M (\varphi(x_1) \cdot \varphi(x_2) \cdot \ldots \cdot \varphi(x_n)) = \pi \circ_M \psi(\pi \circ_M \varphi(x_1)) \cdots \pi \circ_M \psi(\varphi(x_n)) = \pi \circ_M \psi(\pi \circ_M \varphi(x_1) \cdot \pi \circ_M \varphi(x_2) \cdot \ldots \cdot \pi \circ_M \varphi(x_n)). Hence, we have \( \psi((\pi \tilde{x}x_1x_2\ldots x_n) = \psi((\pi \circ_M \varphi(x_1)) \cdots \pi \circ_M \varphi(x_n)).\) Since \( \psi(\pi \tilde{x}x_1x_2\ldots x_n) = \psi((\pi \circ_M \varphi(x_1)) \cdots \pi \circ_M \varphi(x_n)) = \psi((\pi \circ_M \varphi(x_1)) \cdots \pi \circ_M \varphi(x_n)) = \psi((\pi \circ_M \varphi(x_1)) \cdots \pi \circ_M \varphi(x_n)).\) Hence \( \psi((\pi \tilde{x}x_1x_2\ldots x_n) = \pi \circ_M \psi(x_1x_2\ldots x_n) \) for each \( \pi \in Fix(S) \), which means \( S \) supports \( \psi \).

Several results obtained in the previous subsection (in the ZF framework) can be translated into FSM. If in the statement of Theorem 3.7, we replace \( M \) with \( N_{ext}(\Sigma) \) and \( \varphi \) with \( \psi \), we get an equivariant monoid homomorphism \( \psi : \Sigma^* \to N_{ext}(\Sigma) \) such that \( \psi \circ j = j \), where \( j : \Sigma \to \Sigma^* \) is the standard inclusion of \( \Sigma \) into \( \Sigma^* \) which maps each element \( a \in \Sigma \) into the word \( a \). Now if \( w = x_1x_2\ldots x_n \) then we obtain that \( \psi(w) = j(x_1) + j(x_2) + \ldots + j(x_n) \). Now, clearly, \( \psi \) is surjective, and from the first isomorphism theorem for monoids we have \( \Sigma^*/Ker \psi \cong N_{ext}(\Sigma) \). Moreover, in FSM we have the following result.

**Proposition 3.4.** \( \Sigma^*/Ker \psi \) is an invariant monoid, and the isomorphism \( \Theta \) between the monoids \( \Sigma^*/Ker \psi \) and \( N_{ext}(\Sigma) \), defined by \( \Theta([w]) = \psi(w) \) for each \( w \in \Sigma^* \) (where \([w]\) is the equivalence class of \( w \) modulo the equivalence relation Ker \( \psi \)) is equivariant.

**Proof.** We remark that \( \Theta \) is defined as in the standard proof of the first isomorphism theorem for monoids. First we prove that we can define an invariant structure on
We know that $(\Sigma^*, \tilde{\kappa})$ is an invariant set (Theorem 3.6). We define $\odot : S_A \times \Sigma^*/\text{Ker} \psi \to \Sigma^*/\text{Ker} \psi$ by $\pi \odot [w] = [\pi \kappa w]$ for each $w \in \Sigma^*$ and each $\pi \in S_A$. First we show that $\odot$ is a well-defined function. Let $w = x_1 x_2 \ldots x_n$ and $v = y_1 y_2 \ldots y_m$ be two elements in $\Sigma^*$ such that $[w] = [v]$. This means $\psi(w) = \psi(v)$ which by the definition of $\psi$ is the same as $j(x_1) + j(x_2) + \ldots + j(x_n) = j(y_1) + j(y_2) + \ldots + j(y_m)$. Now we have $\pi j(x_1) + j(x_2) + \ldots + j(x_n)) = \pi j(y_1) + j(y_2) + \ldots + j(y_m))$ for each $\pi \in S_A$ where $\pi$ represents the $S_A$-action on $\mathbb{N}(\Sigma)$. Since $\mathbb{N}(\Sigma)$ is an invariant monoid and because $j$ is equivariant (see the proof of Theorem 3.5), in the view of Corollary 2.3 we have $j(\pi x_1) + j(\pi x_2) + \ldots + j(\pi x_n) = j(\pi y_1) + j(\pi y_2) + \ldots + j(\pi y_m)$, which means $\psi(\pi \kappa w) = \psi(\pi \kappa v)$ for each $\pi \in S_A$. Therefore, $[\pi \kappa w] = [\pi \kappa v]$ for each $\pi \in S_A$ which means that $\odot$ is well defined. Since $\tilde{\kappa}$ is an $S_A$-action on $\Sigma^*$, an easy calculation shows us that $\odot$ is an $S_A$-action on $\Sigma^*/\text{Ker} \psi$. Moreover, each element in $\Sigma^*/\text{Ker} \psi$ is finitely supported by the support of its representative. Therefore, $(\Sigma^*/\text{Ker} \psi, \odot)$ is an invariant set. Since $(\Sigma^*, \#)$ is an invariant monoid (the conditions in Definition 3.7 are satisfied), it is trivial to check that $(\Sigma^*/\text{Ker} \psi, \#)$ is also an invariant monoid (we also denote by $\#$ the internal law on the factor monoid $\Sigma^*/\text{Ker} \psi$); the proof is an easy calculation which uses only the definition of $\odot$ and the distributivity property of $\tilde{\kappa}$ over $\#$.

If $\Sigma = \{a_1, \ldots, a_k\}$, the Parikh image $\varphi_\Sigma : \Sigma^* \to \mathbb{N}^k$ is finitely supported. Indeed, $\mathbb{N}^k$ is an $S_A$-set with the $S_A$-action $x : S_A \times \mathbb{N}^k \to \mathbb{N}^k$ defined by $\pi x := x$ for all $\pi \in S_A$ and $x \in \mathbb{N}^k$. From Subsection 2.4.2, we know how an $S_A$-action on the Cartesian product of two invariant sets looks like. Thus, $\mathbb{N}^k$ is endowed with a trivial $S_A$-action defined by $\pi x := x$ for all $\pi \in S_A$ and $x \in \mathbb{N}^k$. Also $\mathbb{N}^k$ is an invariant set since for each $x \in \mathbb{N}^k$ we have that $\Theta$ supports $x$. We prove that $U = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k)$ supports $\varphi_\Sigma$. In the view of Proposition 2.4 we must prove that we have $\varphi_\Sigma(x_1 x_2 \ldots x_n) = \pi \varphi_\Sigma(x_1 x_2 \ldots x_n) = \varphi_\Sigma(x_1 x_2 \ldots x_n)$ (since the $S_A$-action on $\mathbb{N}^k$ is trivial) for each $\pi \in \text{Fix}(U)$ and each $x_1 x_2 \ldots x_n \in \Sigma^*$. Indeed, if $\pi \in \text{Fix}(U)$ we have $\pi x_1 x_2 \ldots x_n = x_1 x_2 \ldots x_n$ (Theorem 3.6) and hence we obtain the required relation.

In the statement of Theorem, we replace $M$ with $\mathbb{N}^k$ and $\varphi : \Sigma \to M$ with the function $\varphi_\Sigma \circ i$ where $i : \Sigma \to \Sigma^*$ is the standard inclusion of $\Sigma$ into $\Sigma^*$, then there is a unique fintely supported homomorphism of abelian monoids $\psi_\Sigma : \mathbb{N}(\Sigma) \to \mathbb{N}^k$ with $\psi_\Sigma \circ j = \varphi_\Sigma \circ i$.

According to Definition 3.21, an invariant partially ordered set $(E, \sqsubseteq)$ is an invariant set $E$ together with a partial order relation $\sqsubseteq$ which is equivariant as a subset of $E \times E$ in the sense of Definition 2.6. Similarly, an invariant strictly ordered set $(E, <)$ is an invariant set $E$ together with a strict (partial or total) order relation $<$ which is equivariant as a subset of $E \times E$ in the sense of Definition 2.6.

**Proposition 3.5.** If $(\Sigma, <)$ is an invariant set, then $(\mathbb{N}_{ext}(\Sigma), *, \sqsubseteq)$ is an invariant partially ordered set.
Proof. According to Proposition 3.3, we have that $(N_{\text{ext}}(\Sigma), \star)$ is an invariant set with the $S_A$-action $\star : S_A \times N_{\text{ext}}(\Sigma) \to N_{\text{ext}}(\Sigma)$ defined by $(\pi \star f)(x) = f(\pi^{-1} \cdot x)$ for all $\pi \in S_A$, $f \in N_{\text{ext}}(\Sigma)$, and $x \in \Sigma$. Let $f, g \in N_{\text{ext}}(\Sigma)$ such that $f \subseteq g$. This means $f(x) \leq g(x)$ for all $x \in \Sigma$. We must prove that $\pi \star f \subseteq \pi \star g$. Let $x \in \Sigma$. We have $(\pi \star f)(x) = f(\pi^{-1} \cdot x) \leq g(\pi^{-1} \cdot x) = (\pi \star g)(x)$. Therefore, $\subseteq$ is equivariant. \qed

3.1.3 An Extension of the Framework

Since a finite invariant set necessarily has a trivial permutation action (see Corollary 2.2), the restriction of the results in Section 3.1.2 for $N(\Sigma)$ becomes trivial\textsuperscript{1}. This is the reason why we do not discuss the results in Section 3.1.2 (which are valid in the general case when $\Sigma$ is an infinite invariant set) in the particular case when $\Sigma$ is a finite alphabet. The triviality of the properties of $N(\Sigma)$ could be avoided if we were to replace “finite invariant set” by “finite set in the Fraenkel-Mostowski cumulative hierarchy $FM(A)$”. An FM set is a finitely supported element in the invariant set $FM(A)$; additionally an FM set has the recursive property that all its elements are also FM sets. We generalize the results in the previous section in order to be closer to the framework of FM sets. However, we preserve the terminology of invariant sets in order to present the following results. In order to make our point we use Definition 2.8 and Proposition 2.5.

According to Proposition 2.5, we conclude that, if $X$ and $Y$ are invariant sets and $Z$ is a finitely supported subset of $X$, then the set of all finitely supported functions from $Z$ to $Y$ is a finitely supported subset of the invariant set $X \times Y$. Moreover, if $f : Z \to Y$ is a finitely supported function, then we can define the function $g : X \to Y$ by considering $g(x) = f(x)$, $\forall x \in Z$ and $g(x) = y_0$, $\forall x \in X \setminus Z$ for some fixed $y_0 \in Y$. Obviously, $g$ is supported by $\text{supp}(f) \cup \text{supp}(y_0)$. Therefore, we can extend each finitely supported function $f : Z \to Y$ to a finitely supported function $g : X \to Y$. Informally, we agree to say that the set of all finitely supported functions from $Z$ to $Y$ is a finitely supported subset of the invariant set formed by the collection of all finitely supported functions from $X$ to $Y$.

According to Proposition 2.5, the results in Section 3.1.2 can be generalized in terms of “finitely supported subsets of invariant sets”. We present only their statements because their proofs are analogous to the original proofs presented in Section 3.1.2 (just note that instead of Proposition 2.4 we have to use Proposition 2.5).

Proposition 3.6. Let $(\Sigma, \cdot)$ be an invariant set (possible infinite), $(\Sigma_0, \cdot)$ a finitely supported subset of $\Sigma$, and $f : \Sigma_0 \to N$ a function such that its algebraic support $S_f \overset{\text{def}}{=} \{ x \in \Sigma_0 \mid f(x) \neq 0 \}$ is finite. Then $f$ is finitely supported and $\text{supp}(f) \subseteq \text{supp}(S_f) \cup \text{supp}(\Sigma_0)$.

Corollary 3.2. Let $\Sigma_0 = \{ a_1, \ldots, a_k \}$ be a finite subset of an invariant set $(\Sigma, \cdot)$. Then each function $f : \Sigma_0 \to N$ is supported by the set $S = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k)$.

\textsuperscript{1} In the particular case when $\Sigma$ is a finite alphabet we have that $N_{\text{ext}}(\Sigma)$ coincides with $N(\Sigma)$. 

3.1 Multisets in Finitely Supported Mathematics 61

Definition 3.8. Given an invariant set \((\Sigma, \cdot)\) (possible infinite) and \((\Sigma_0, \cdot)\) a finitely supported subset of \(\Sigma\), any function \(f : \Sigma_0 \to \mathbb{N}\) with the property that \(S_f\) is finite is called an extended multiset over \(\Sigma_0\) of rank 1. The set of all extended multisets over \(\Sigma_0\) of rank 1 is denoted by \(\mathbb{N}^1_{\text{ext}}(\Sigma_0)\).

If \(f : \Sigma_0 \to \mathbb{N}\) is an extended multiset over \(\Sigma_0\) of rank 1, then we can define the function \(g : \Sigma \to \mathbb{N}\) by considering \(g(x) = f(x), \forall x \in \Sigma_0\) and \(g(x) = 0, \forall x \in \Sigma \setminus \Sigma_0\). Obviously, \(g\) is an extended multiset over \(\Sigma\) which is supported by \(\text{supp}(f)\).

Definition 3.9. A finitely supported monoid is a triple \((M, +, \cdot)\) such that the following conditions are satisfied:

- \((M, +, 0)\) is a monoid;
- \((M, \cdot)\) is a finitely supported subset of an invariant set;
- for each \(\pi \in \text{Fix}(\text{supp}(M))\) and each \(x, y \in M\) we have \(\pi \cdot (x + y) = \pi \cdot x + \pi \cdot y\) and \(\pi \cdot 0 = 0\).

Theorem 3.8. Let \((\Sigma, \cdot)\) be an invariant set and \((\Sigma_0, \cdot)\) be a finitely supported subset of \(\Sigma\). The set \(\mathbb{N}^1_{\text{ext}}(\Sigma_0)\) is a free abelian finitely supported monoid.

Theorem 3.9. Let \((\Sigma, \cdot)\) be an invariant set and \((\Sigma_0, \cdot)\) a finitely supported subset of \(\Sigma\). Let \(j : \Sigma_0 \to \mathbb{N}^1_{\text{ext}}(\Sigma_0)\) be the function which maps each \(a \in \Sigma_0\) into \(\bar{a} \in \widetilde{\Sigma}_0\). Then \(j\) is supported by \(\text{supp}(\Sigma_0)\). If \((M, +, \cdot)\) is an arbitrary abelian finitely supported monoid and \(\varphi : \Sigma_0 \to M\) is an arbitrary finitely supported function, then there exists a unique finitely supported homomorphism of abelian monoids \(\psi : \mathbb{N}^1_{\text{ext}}(\Sigma_0) \to M\) with \(\psi \circ j = \varphi\), i.e. \(\psi(\bar{a}) = \varphi(a)\) for all \(a \in \Sigma_0\). Moreover, if a finite set \(S\) supports \(\varphi\), then the set \(S \cup \text{supp}(M) \cup \text{supp}(\Sigma_0)\) supports \(\psi\).

Theorem 3.10. Let \((\Sigma, \cdot)\) be an invariant set and \((\Sigma_0, \cdot)\) a finitely supported subset of \(\Sigma\). \(\Sigma_0^*\) is a finitely supported monoid. Moreover, each element of the form \(x_1 x_2 \ldots x_n\) from \(\Sigma_0^*\) is supported by the set \(U = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k)\) when \(\Sigma_0\) is a finite subset \(\{a_1, \ldots, a_k\}\) of \(\Sigma\).

Clearly, \(\Sigma_0^*\) is a finitely supported subset (supported by \(\text{supp}(\Sigma_0)\)) of \(\Sigma^*\).

Theorem 3.11. Let \((\Sigma, \cdot)\) be an invariant set and \((\Sigma_0, \cdot)\) a finitely supported subset of \(\Sigma\). Let \(i : \Sigma_0 \to \Sigma_0^*\) be the standard inclusion of \(\Sigma_0\) into \(\Sigma_0^*\) which maps each element \(a \in \Sigma_0\) into the word \(a\). Then \(i\) is supported by \(\text{supp}(\Sigma_0)\). If \((M, \cdot, \varnothing)\) is an arbitrary finitely supported monoid and \(\varphi : \Sigma_0 \to M\) is an arbitrary finitely supported function, then there exists a unique finitely supported homomorphism of monoids \(\psi : \Sigma_0^* \to M\) with \(\psi \circ i = \varphi\). Moreover, if a finite set \(S\) supports \(\varphi\), then the set \(S \cup \text{supp}(M) \cup \text{supp}(\Sigma_0)\) supports \(\psi\).

Proposition 3.7. Let \((\Sigma, \cdot)\) be an invariant set and \((\Sigma_0, \cdot)\) be a finitely supported subset of \(\Sigma\). The sub-multiset order \(\subseteq\) on \(\mathbb{N}^1_{\text{ext}}(\Sigma_0)\) is supported (as a subset of \(\Sigma \times \Sigma\)) by \(\text{supp}(\Sigma_0)\).
**Theorem 3.12.** Let \((\Sigma, \cdot)\) be an invariant set and \((\Sigma_0, \cdot)\) be a finite subset of \(\Sigma\). Let \(\prec\) be a strict order relation on \(\Sigma_0\). The Dershowitz and Manna order \(\preceq\) on \(\mathbb{N}_{\text{ext}}^1(\Sigma_0)\) induced by \(\prec\) is supported (as a subset of \(\Sigma \times \Sigma\)) by \(\text{supp}(\Sigma_0) \cup \text{supp}(\prec)\).

**Proof.** We know that \(\prec\) is a strict order relation on \(\Sigma_0\). Since \(\prec\) is a finite subset of \(\Sigma_0 \times \Sigma_0\), it follows that \(\prec\) is finitely supported. Let \(\pi \in \text{Fix}(\text{supp}(\Sigma_0) \cup \text{supp}(\prec))\). Since \(\Sigma_0\) is finite, we use the HO definition of \(\preceq\) (see Definition 3.5). Let \(f, g \in \mathbb{N}_{\text{ext}}^1(\Sigma_0)\) such that \(f \preceq g\), and \(\pi \in S_A\). Since \(f \neq g\), there exists \(x \in \Sigma_0\) such that \(f(x) \neq g(x)\). Therefore, \(f(x) = (\pi \star f)(\pi \cdot x) \neq (\pi \star g)(\pi \cdot x) = g(x)\). Since \(\pi \cdot x \in \Sigma_0\), we have \(\pi \star f \neq \pi \star g\). Let \(y \in \Sigma_0\) such that \((\pi \star f)(y) > (\pi \star g)(y)\). Then \(f(\pi^{-1} \cdot y) > g(\pi^{-1} \cdot y)\). According to Definition 3.5, there exists \(x \in \Sigma_0\) with \(\pi^{-1} \cdot y \prec x\) and \(f(x) < g(x)\). Since \(\pi \in \text{Fix}(\text{supp}(\prec))\), we have \(y \prec \pi \cdot x\). Since \(f(x) < g(x)\), we obtain \((\pi \star f)(\pi \cdot x) < (\pi \star g)(\pi \cdot x)\). Thus, \(\pi \star f \preceq \pi \star g\). \(\square\)

Note that none of the results in this section leads to a trivial corollary when we require \(\Sigma_0\) to be finite. Therefore, the properties of \(\mathbb{N}_{\text{ext}}^1(\Sigma_0) = \mathbb{N}(\Sigma_0)\) are non-trivial even when \(\Sigma_0\) is a finite subset of an invariant set.

### 3.2 Generalized Multisets in Finitely Supported Mathematics

Generalized multisets extend the usual multisets by allowing negative multiplicities as well. In a generalized multiset, the multiplicity of an element can be either a positive number, zero, or a negative number. Since generalized multisets are characterized by the multiplicity of each element, they can also be defined as functions from \(\Sigma\) (the universe of elements) to \(\mathbb{Z}\), where \(\mathbb{Z}\) is the set of all integers. A first study of generalized multisets is due to Blizard [38]. Loeb also investigated generalized multisets (see [107]) by using the alternative notion of hybrid set for what we call a generalized multiset. However, the first application of the concept of “generalized multiset” is due to Reisig [129]; it uses generalized multisets and generalized multirelations (which are in fact generalized multisets over the Cartesian product \(D \times D\) of a set of sorts \(D\)) to define relation nets. In [32] generalized multisets are interpreted in a chemical programming framework. In mathematics, an example of the theory of generalized multisets is represented by surreal numbers [56]. Generalized multisets could also be used in order to characterize P systems with anti-matter described in [26]. An algebraic study on generalized multisets in the classical Zermelo-Fraenkel (ZF) framework and in Reverse Mathematics can be found in [10]. The formalization of generalized multisets in FSM belongs to the authors [19].

In this section we apply a similar algorithm to that presented in Section 3.1, and we define and study generalized multisets in FSM. The FSM properties are also compared with the related ZF properties.
3.2 Generalized Multisets in Finitely Supported Mathematics

3.2.1 Algebraic Properties of Generalized Multisets

3.2.1.1 Generalized Multisets as Groups

**Definition 3.10.** Given a finite alphabet $\Sigma$, any function $f : \Sigma \to \mathbb{Z}$ is called a generalized multiset over $\Sigma$. The value of $f(a)$ is said to be the multiplicity of $a$. The set of all generalized multisets over $\Sigma$ is denoted by $Z(\Sigma)$.

The additive structure of $\mathbb{Z}$ induces an additive operation (sum) on generalized multisets in the same way as the additive structure of $\mathbb{N}$ induces an additive operation (sum) on multisets. On $Z(\Sigma)$ we define an additive law by:

$$+ : Z(\Sigma) \times Z(\Sigma) \to Z(\Sigma),$$

$$(f, g) \mapsto f + g$$

where $f + g : \Sigma \to \mathbb{Z}$ is defined pointwise by $(f + g)(a) = f(a) + g(a)$ for all $a \in \Sigma$. Since $Z(\Sigma)$ is formed by all functions from $\Sigma$ to $\mathbb{Z}$, it is clear that $(Z(\Sigma), +)$ is an abelian group, the identity being the empty generalized multiset $\theta : \Sigma \to \mathbb{Z}$, $\theta(a) = 0$ for all $a \in \Sigma$, and the inverse of an element $f : \Sigma \to \mathbb{Z}$ is the element $-f : \Sigma \to \mathbb{Z}$ defined by $(-f)(a) = -(f(a))$ for all $a \in \Sigma$. Since $(Z(\Sigma), +)$ is an abelian group, it follows that $(Z(\Sigma), +)$ is a $\mathbb{Z}$-module with the scalar multiplication from $\mathbb{Z}$ defined by:

$$\cdot : \mathbb{Z} \times Z(\Sigma) \to Z(\Sigma),$$

$$(k, f) \mapsto k \cdot f$$

where $k \cdot f : \Sigma \to \mathbb{Z}$ is defined pointwise by $(k \cdot f)(a) = k \cdot f(a)$, for all $a \in \Sigma$ and $k \in \mathbb{Z}$.

**Proposition 3.8.** $(Z(\Sigma), +)$ is a free abelian group.

**Proof.** If $a \in \Sigma$, we consider the generalized multiset $\tilde{a} : \Sigma \to \mathbb{Z}$ defined by

$$\tilde{a}(b) = \begin{cases} 1, & \text{for } b = a; \\ 0, & \text{for } b \in \Sigma \setminus \{a\}. \end{cases}$$

It is easy to check that every generalized multiset $f \in Z(\Sigma)$ can be expressed as

$$f = \sum_{a \in \Sigma} f(a) \cdot \tilde{a}.$$

Since $\Sigma$ is finite, the sum is finite. In fact, the set of generalized multisets $\{\tilde{a} \mid a \in \Sigma\}$ is a basis for the $\mathbb{Z}$-module $Z(\Sigma)$ since $\{\tilde{a} \mid a \in \Sigma\}$ is also linearly independent. $\square$

According to Proposition 2.37 in [134], two free $R$-modules are isomorphic iff there are bases of each having the same cardinality, whenever $R$ is a commutative ring. If we denote the basis of $Z(\Sigma)$ by $\tilde{\Sigma} = \{\tilde{a} \mid a \in \Sigma\}$, it is clear that there is a bijection from $\Sigma$ onto $\tilde{\Sigma}$ given by $a \mapsto \tilde{a}$. It follows that $|\Sigma| = |\tilde{\Sigma}|$ and so, $Z(\Sigma) \cong FA(\Sigma)$.
where $FA(\Sigma)$ represents the free $\mathbb{Z}$-module with basis $\Sigma$. $\mathbb{Z}(\Sigma)$ and $FA(\Sigma)$ can be identified (up to an isomorphism).

Since $\mathbb{Z}(\Sigma)$ is the free $\mathbb{Z}$-module with basis $\tilde{\Sigma}$, it satisfies the universality property described in Proposition 3.9(1). We denote by $j : \Sigma \to \mathbb{Z}(\Sigma)$ the function which maps each $a \in \Sigma$ into $\tilde{a} \in \tilde{\Sigma}$. It is clear that $j$ is the composition of the standard inclusion $i : \tilde{\Sigma} \to \mathbb{Z}(\Sigma)$, $i(\tilde{a}) = \tilde{a}$ for all $\tilde{a} \in \tilde{\Sigma}$ with the bijection of $\Sigma$ onto $\tilde{\Sigma}$ defined by $a \mapsto \tilde{a}$. So, the universality property for $FA(\Sigma)$ can be extended to $\mathbb{Z}(\Sigma)$ by replacing the standard inclusion of $\Sigma$ into $FA(\Sigma)$ with $j$; this result is presented as Proposition 3.9(2).

**Proposition 3.9.**
1. If $G$ is any abelian group and $f : \tilde{\Sigma} \to G$ an arbitrary function, then there is a unique homomorphism of abelian groups $g : \mathbb{Z}(\Sigma) \to G$ with $g \circ i = f$, i.e. $g(\tilde{a}) = f(\tilde{a})$ for all $\tilde{a} \in \tilde{\Sigma}$.
2. If $G$ is any abelian group and $f : \Sigma \to G$ an arbitrary function, then there is a unique homomorphism of abelian groups $g : \mathbb{Z}(\Sigma) \to G$ with $g \circ j = f$, i.e. $g(a) = f(a)$ for all $a \in \Sigma$.

**Proof.** This property can be obtained as a particular case of Proposition 2.34 in [134] proving the universality property for free (left-)modules.

Some properties of $\mathbb{Z}(\Sigma)$ also follow from the general theory of free modules.

**Proposition 3.10.** Let $p : G \to H$ be any surjective homomorphism of abelian groups. For every homomorphism $h : \mathbb{Z}(\Sigma) \to H$ there is a homomorphism of abelian groups $g : \mathbb{Z}(\Sigma) \to G$ such that $p \circ g = h$.

**Proof.** This result can be obtained as a particular case of Theorem 3.1 from [134] proving that every free (left-)module is projective. The projectivity of $\mathbb{Z}(\Sigma)$ is mathematically expressed in the statement of Proposition 3.10 in the same way as in the general theory (see [134]).

Using some basic notions of homological algebra presented in [134] we can give the following result.

**Corollary 3.3.** The functor $\text{Hom}_\mathbb{Z}(\mathbb{Z}(\Sigma), -)$ is an exact functor, which means it keeps the exactness of exact sequences.

**Proof.** The projectivity of a (left-)R-module $A$ is equivalent to the exactness of the functor $\text{Hom}_R(A, -)$ (see Proposition 3.2 in [134]). Now, by Proposition 3.10, $\mathbb{Z}(\Sigma)$ is a projective $\mathbb{Z}$-module, and that means the functor $\text{Hom}_\mathbb{Z}(\mathbb{Z}(\Sigma), -)$ is an exact functor.

**Theorem 3.13.** If $G \leq \mathbb{Z}(\Sigma)$ is a subgroup of the abelian group $\mathbb{Z}(\Sigma)$ then $G$ is a free abelian group and has a basis of cardinality equal to at most $|\Sigma|$ elements.

**Proof.** In Theorem 4.13 and Corollary 4.15 in [134] it was proved that, if $R$ is a domain all of whose ideals are principal (i.e. cyclic, generated by one element), then every submodule $A$ of a free $R$-module $F$ is also free with $\text{rank}(A) \leq \text{rank}(F)$. Our proof is complete because all the ideals of $\mathbb{Z}$ are of form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, and so $\mathbb{Z}$ is a principal ideal domain (PID).
Another important theorem which is valid for finitely generated modules over a PID is the theorem of invariant factors. We give its form only for abelian groups. For proof we recommend [133]. The direct sums of modules (abelian groups) are denoted by \( \oplus \) and the order of an element \( x \) in a group is denoted by \( \text{ord}(x) \).

**Theorem 3.14.** There are \( m,n \in \mathbb{N} \), \( m \leq n \) and \( x_1,x_2,\ldots,x_n \in \mathbb{Z}(\Sigma) \) such that \( \mathbb{Z}(\Sigma) = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_m \oplus \mathbb{Z}x_{m+1} \oplus \cdots \oplus \mathbb{Z}x_n \) and \( \text{ord}(x_i) = d_i \in \mathbb{N}^* \), \( i = 1,\ldots,n \) satisfy the conditions \( 1 < d_i \), \( i = 1,\ldots,m \) and \( d_i|d_j \), \( j = 1,\ldots,m \) and \( d_m+1 = \cdots = d_n = \infty \). Moreover, the elements \( m,n \in \mathbb{N} \) and \( \text{ord}(x_i) = d_i \in \mathbb{N}^* \) are uniquely determined in the sense that: whenever we have \( m',n' \in \mathbb{N} \), \( m' \leq n' \) and \( y_1,y_2,\ldots,y_{n'} \in \mathbb{Z}(\Sigma) \) such that \( \mathbb{Z}(\Sigma) = \mathbb{Z}y_1 \oplus \mathbb{Z}y_2 \oplus \cdots \oplus \mathbb{Z}y_{m'} \oplus \mathbb{Z}y_{m'+1} \oplus \cdots \oplus \mathbb{Z}y_{n'} \), and \( \text{ord}(y_i) = e_i \in \mathbb{N}^* \), \( i = 1,\ldots,n' \) satisfy the conditions \( 1 < e_i \), \( i = 1,\ldots,m' \) and \( e_1|e_2|\cdots|e_{m'} \) and \( e_{m'+1} = \cdots = e_{n'} = \infty \), then we must have \( m = m' \), \( n = n' \) and \( d_i = e_i \), \( \forall i \in \{1,\ldots,n\} \).

A similar theorem for decomposing \( \mathbb{Z}(\Sigma) \) into indecomposable subgroups (i.e. into cyclic subgroups of infinite order or of order \( p^k \) where \( p \) is a prime and \( k \in \mathbb{N}^* \)) can be presented. The proof uses the property that \( \mathbb{Z}(\Sigma) \) is finitely generated, and can be found in [133].

**Theorem 3.15.** \( \mathbb{Z}(\Sigma) \) can be decomposed into a direct sum of indecomposable subgroups. Moreover, that decomposition is unique in the sense that if \( \mathbb{Z}(\Sigma) = A_1 \oplus A_2 \oplus \cdots \oplus A_n = B_1 \oplus B_2 \oplus \cdots \oplus B_m \) are two decompositions of \( \mathbb{Z}(\Sigma) \) into indecomposable subgroups, then \( m = n \) and there is a permutation \( \sigma \in S_n \) such that \( A_i \cong B_{\sigma(i)} \), \( 1 \leq i \leq n \).

**Definition 3.11.** 1. Adjoin one element to \( \Sigma \) and denote it by \( 1 \). A word on \( \Sigma \) is either the element 1 or a formal expression \( x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n} \) where \( n \in \mathbb{N} \), \( x_i \in \Sigma \) and \( e_i \in \{\pm 1\} \).

- Two words are called equivalent if one can be obtained from another by repeatedly cancelling or inserting terms of the form \( x^{-1}x \) or \( xx^{-1} \) for \( x \in \Sigma \). A word in which all occurring terms can be cancelled is defined to be equivalent to the “empty word”. The equivalence class of an word \( w \) is denoted by [\( w \)].

- The juxtaposition of words \( w = x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n} \) and \( w' = y_1^{\delta_1}y_2^{\delta_2}\cdots y_m^{\delta_m} \) is the word \( w\#w' := x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}y_1^{\delta_1}y_2^{\delta_2}\cdots y_m^{\delta_m} \). Moreover, we define \( w\#1 = 1\#w = w \) for all words \( w \).

2. The free group \( F(\Sigma) \) is the set of all equivalence classes of words on \( \Sigma \) with the group operation \( [w][w'] := [w\#w'] \).

It is easy to check that \( \tau \) is well defined, independent of the chosen representatives, and verifies the axioms of a group law over \( F(\Sigma) \).

**Example 3.1.** According to Definition 3.11, words of the form \( aa^{-1}bc^{-1}c \) (for example), \( d^{-1}db \) and \( b \) are identified (they are in the same equivalence class).

It is worth noting that the order and the multiplicity are important in a word \( w = x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n} \). Another interesting remark is that, if \( \Omega \) is another alphabet with \( |\Sigma| = |\Omega| \) (they have the same cardinality), then \( F(\Sigma) \cong F(\Omega) \). The free group on \( \Sigma \) also satisfies the so-called universality property (see Proposition 25.3 in [149]).
Theorem 3.16. For each group $G$ and each function $f : \Sigma \rightarrow G$, there is a unique homomorphism of groups $g : F(\Sigma) \rightarrow G$ with $g \circ i = f$, where $i : \Sigma \rightarrow F(\Sigma)$ is the standard inclusion of $\Sigma$ into $F(\Sigma)$ which maps each element $a \in \Sigma$ into the word $[a]$.

Remark 3.3. The properties of the function $g$ found in Theorem 3.16 allow us to say that $g(1) = e$ and $g([x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}]) = g([x_1]^{e_1} \circ g([x_2]^{e_2} \circ \ldots \circ g([x_n]^{e_n}) = f([x_1]^{e_1} \circ f([x_2]^{e_2} \circ \ldots \circ f([x_n]^{e_n})$ for each word $[x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}]$; $e$ represents the identity element in $G$ and $\circ$ represents the internal law of $G$.

We can compare generalized multisets with vectors of integer numbers. It is known that, for $k \in \mathbb{N}$, $k \neq 0$, $\mathbb{Z}^k$ is an abelian group with respect to addition of vectors. Moreover, $\mathbb{Z}^k$ is free with the canonical basis $B = \{e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \mid i = 1, \ldots, k\}$. If $\Sigma = \{a_1, \ldots, a_k\}$, then $\mathbb{Z}(\Sigma) \cong \mathbb{Z}^k$ as $\mathbb{Z}$-modules and hence as abelian groups.

We can connect all these views using the universal property of the free group $F(\Sigma)$ (it can be connected by this property with any group, and not only with commutative ones as in the case of $\mathbb{Z}(\Sigma)$). If in the statement of Theorem 3.16, we replace $G$ with $\mathbb{Z}(\Sigma)$, and $f : \Sigma \rightarrow G$ with $j : \Sigma \rightarrow \mathbb{Z}(\Sigma)$ where $j$ maps each $a$ into $\tilde{a}$, we get a function $g : F(\Sigma) \rightarrow \mathbb{Z}(\Sigma)$ such that $g \circ i = j$, where $i : \Sigma \rightarrow F(\Sigma)$ is the standard inclusion of $\Sigma$ into $F(\Sigma)$ which maps each element $a \in \Sigma$ into the word $[a]$. Now if $w = [x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}]$, then, by Remark 3.3, we obtain that $g(w) = e_1 j(x_1) + e_2 j(x_2) + \ldots + e_n j(x_n)$. Now, clearly, $g$ is surjective, and from the first isomorphism theorem for groups we have $F(\Sigma)/\text{Ker } g \cong \mathbb{Z}(\Sigma)$.

The Parikh image for multisets has a corresponding result for generalized multisets. The generalization is natural. If $\Sigma = \{a_1, \ldots, a_k\}$, we define the Parikh image $\varphi(\Sigma) : F(\Sigma) \rightarrow \mathbb{Z}^k$ in the following way: if $w = [x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}]$ then $\varphi(\Sigma)(w)$ is the vector in $\mathbb{Z}^k$ whose $i$-component is $\sum_{x_i = a_j} x_j = a_j$ for each $i = 1, \ldots, k$; if there is no $j$ such that $x_j = a_i$ the $i$-component of the vector is defined to be $0$. Informally, $\varphi(\Sigma)(w)$ calculates the number of “occurrences” (even the “negative” ones) of each element from $\Sigma$ in $w$. For example if $\Sigma = \{a, b, c, d, e\}$ and $w = [aa^{-1}bc^{-1}c^{-1}]$, that is, $x_1 = a$, $x_2 = a^{-1}$, $x_3 = b$, $x_4 = c^{-1}$, $x_5 = c^{-1}$, $x_6 = c$, then $\varphi(\Sigma)(w) = (1 + (-1), 1, (-1) + (-1) + 1, 0, 0) = (0, 1, -1, 0, 0)$.

If in the statement of Proposition 3.9, we replace $G$ with $\mathbb{Z}^k$ and $f : \Sigma \rightarrow G$ with the function $\varphi(\Sigma) \circ i$ where $i : \Sigma \rightarrow F(\Sigma)$ is the standard inclusion of $\Sigma$ into $F(\Sigma)$ which maps each element $a_u \in \Sigma$ into the word $[a_u]$, then there is a unique homomorphism of abelian groups $\psi(\Sigma) : \mathbb{Z}(\Sigma) \rightarrow \mathbb{Z}^k$ with $\psi(\Sigma) \circ j = \varphi(\Sigma) \circ i$, that is, $\psi(\Sigma)(\tilde{a}_u) = \varphi(\Sigma)(a_u) = (0, 0, 0, 0, 0) = e_u$ for all $a_u \in \Sigma$, where $e_u = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the vector in $\mathbb{Z}^k$ all of whose components are $0$ except the $u$ component that is $1$.

Now, because $\psi(\Sigma)$ maps each element one-to-one from a finite basis of $\mathbb{Z}(\Sigma)$ into an element from a finite basis of $\mathbb{Z}^k$, and $\mathbb{Z}(\Sigma)$ and $\mathbb{Z}^k$ have the same rank, we have that $\psi(\Sigma) : \mathbb{Z}(\Sigma) \rightarrow \mathbb{Z}^k$ is an isomorphism, and

$$\psi(\Sigma) \left( \sum_{i=1}^{k} f(a_i) \cdot \tilde{a}_i \right) = (f(a_1), \ldots, f(a_k))$$

for each $f \in \mathbb{Z}(\Sigma)$. 


Moreover, the properties of commutative diagrams show us that $\psi_\Sigma \circ g = \varphi_\Sigma$ where $g : F(\Sigma) \to \mathbb{Z}(\Sigma)$ is the homomorphism built before such that $g \circ i = j$.

$$\psi_\Sigma \circ g = \varphi_\Sigma$$

Moreover, the properties of commutative diagrams show us that $\psi_\Sigma \circ g = \varphi_\Sigma$ where $g : F(\Sigma) \to \mathbb{Z}(\Sigma)$ is the homomorphism built before such that $g \circ i = j$.

Another property of $\mathbb{Z}(\Sigma)$ follow from the construction of $FA(\Sigma)$ presented by Spindler in [149]. We obtain $\mathbb{Z}(\Sigma) \cong FA(\Sigma) = F(\Sigma)/D(F(\Sigma))$ where, for a group $(H, \cdot)$, $D(H)$ is the commutator subgroup of $H$, i.e. the subgroup of $H$ generated by all commutators $[x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1}$ with $x, y \in H$.

### 3.2.1.2 Orders on Generalized Multisets

The set $\mathbb{Z}(\Sigma)$ can be partially ordered. Some orders on $\mathbb{Z}(\Sigma)$ are induced by our intuition and some of them are purely abstract. The best known order on generalized multisets is Loeb’s order presented in [107]. This order is obtained from the definition of the subset property in the case of generalized multisets.

**Definition 3.12 (Loeb).** Let $f$ and $g$ be generalized multisets. We say that $f$ is a subset of $g$ and we write $f \subseteq g$ if either $f(u) \ll g(u)$ for all $u \in \Sigma$ or $g(u) - f(u) \ll g(u)$ for all $u \in \Sigma$, where $\ll$ is the partial ordering of integers defined as follows: $i \ll j$ iff $i \leq j$ and both of $i$ and $j$ are either greater or equal to 0 or smaller than 0.

Loeb proved that $\subseteq$ is a partial order relation on $\mathbb{Z}(\Sigma)$. Unfortunately, $\subseteq$ is not compatible with the group law on $\mathbb{Z}(\Sigma)$. This means there may exist $f, g, h \in \mathbb{Z}(\Sigma)$ such that $f \subseteq g$ and $f + h \not\subseteq g + h$. Although $\subseteq$ helps us to obtain some important combinatorial properties of $\mathbb{Z}(\Sigma)$, it does not help us to obtain new algebraic properties of $\mathbb{Z}(\Sigma)$.

The following question arises: “Can we find an order relation on the set of generalized multisets which is compatible with the group law on $\mathbb{Z}(\Sigma)$?” The answer comes quickly if we look to the classical definition of sub-multisets. We can naturally extend that definition to generalized multisets, and so we say that a generalized multiset $f$ is a subset of the generalized multiset $g$ (and we denote this by $f \preceq g$) iff $f(u) \leq g(u)$ for all $u \in \Sigma$. This new definition of the subset property contradicts Loeb’s viewpoint.

Informally, Loeb [107] builds step by step the subsets of a given generalized multiset $g$. A subset $f$ of $g$ is obtained by removing some elements in $g$. The generalized multiset obtained after $f$ has been removed is also a subset of $g$. Nothing special until now. However, Loeb introduces a law of removing which says that we cannot remove from $g$ an element which is not a member of $g$. Intuitively, this is correct if we identify the generalized multiset with its algebraic support. In Loeb’s approach the members of a generalized multiset $g$ over $\Sigma$ are only those $u \in \Sigma$ for which
g(u) \neq 0. So, even Loeb also defines the generalized multisets over \( \Sigma \) as functions from \( \Sigma \) to \( \mathbb{Z} \) (Definition 2.1 in [107]), he actually works with the generalized multisets over \( \Sigma \) as partial functions from \( \Sigma \) to \( \mathbb{Z}^+ \). This viewpoint has combinatorial benefits (see [107]). However we have a slightly different perspective.

We do not define a membership relation on a given generalized multiset in the sense that Loeb did. We say that each element of \( \Sigma \) belongs to the generalized multiset \( g : \Sigma \rightarrow \mathbb{Z} \) with a certain multiplicity. Let \( u \in \Sigma \). If \( g(u) > 0 \) we say that \( u \) belongs to the generalized multiset \( g : \Sigma \rightarrow \mathbb{Z} \) with a positive multiplicity, if \( g(u) < 0 \) we say that \( u \) belongs to the generalized multiset \( g : \Sigma \rightarrow \mathbb{Z} \) with a negative multiplicity, and if \( g(u) = 0 \) we say that \( u \) belongs to the generalized multiset \( g : \Sigma \rightarrow \mathbb{Z} \) with null multiplicity. Sure, intuitively we cannot say that something appears in a set zero times. This contradicts the ZF axioms of set theory. However, the entire theory of multisets and generalized multisets is in contradiction with ZF axiomatic set theory if we see them like sets. In fact generalized multisets are not sets in the sense of the ZF axioms. They are functions. So, the notion of ‘membership of an element’ in the ordinary set theory can be replaced with the notion of ‘multiplicity of that element’ in a generalized multiset. If we allow the presence of elements with negative multiplicities in a generalized multiset, we can also allow the presence of elements with null multiplicities in that generalized multiset. Moreover, precisely, we can see the elements with negative multiplicities as ‘anti-matter objects’ that annihilate the objects with positive multiplicities.

We give now a new definition of subsets of generalized multisets.

**Definition 3.13.** Let \( f \) and \( g \) be two generalized multisets over \( \Sigma \). We say that \( f \) is a subset of the generalized multiset \( g \) (and we denote this by \( f \preceq g \)) iff \( f(u) \leq g(u) \) for all \( u \in \Sigma \).

It is clear that \((\mathbb{Z}(\Sigma), \preceq)\) is a partially ordered set. Moreover, \((\mathbb{Z}(\Sigma), \preceq)\) is a lattice because, for each \( f, g : \Sigma \rightarrow \mathbb{Z} \), there are \( h, k : \Sigma \rightarrow \mathbb{Z} \) defined by \( h(u) = \min(f(u), g(u)) \) for all \( u \in \Sigma \), \( k(u) = \max(f(u), g(u)) \) for all \( u \in \Sigma \), such that \( h = \inf(f, g) \) and \( k = \sup(f, g) \) with respect to the partial order \( \preceq \) on \( \mathbb{Z}(\Sigma) \).

From the general theory of lattices, we know that we can define two binary operations

- \( \land : \mathbb{Z}(\Sigma) \times \mathbb{Z}(\Sigma) \rightarrow \mathbb{Z}(\Sigma) \), \( (f, g) \mapsto h \), where \( h : \Sigma \rightarrow \mathbb{Z} \) is defined by \( h(u) = \min(f(u), g(u)) \) for all \( u \in \Sigma \);
- \( \lor : \mathbb{Z}(\Sigma) \times \mathbb{Z}(\Sigma) \rightarrow \mathbb{Z}(\Sigma) \), \( (f, g) \mapsto k \), where \( k : \Sigma \rightarrow \mathbb{Z} \) is defined by \( k(u) = \max(f(u), g(u)) \) for all \( u \in \Sigma \).

such that \((\mathbb{Z}(\Sigma), \land, \lor)\) is a lattice (this means \( \land \) and \( \lor \) satisfy the properties of commutativity, associativity and absorption).

Also \( \preceq \) is compatible with the group law on \( \mathbb{Z}(\Sigma) \). We can easily check that for all \( f, g, h \in \mathbb{Z}(\Sigma) \) such that \( f \preceq g \) we have \( f + h \preceq g + h \).

**Definition 3.14.** A group \((G, +)\) endowed with a partial order \( \preceq \) is a partially ordered group (po-group) if for all \( g, h, x, y \in G \) we have that \( g \preceq h \) implies that \( x + g + y \leq x + h + y \).
• If \((G, +)\) is a po-group and the partial order \(\leq\) is a lattice order, then \((G, +)\) is called a lattice-ordered group \((l\text{-group})\).

• If \((G, +)\) is a po-group and the partial order \(\leq\) is a total order, then \((G, +)\) is called a totally-ordered group \((o\text{-group})\).

It is clear now that \((\mathbb{Z}(\Sigma), +, \preceq)\) is a lattice-ordered group. From the general theory of \(l\)-groups, it follows quickly that \((\mathbb{Z}(\Sigma), \wedge, \vee)\) is a distributive lattice.

The definition of (partially-)ordered groups can be extended to other algebraic structures. For example we give a definition which will be used in the statement of Theorem 3.23.

**Definition 3.15.** A field \((F, +, \cdot, 0, 1)\) together with a total order \(\leq\) on \(F\) is a totally ordered field if the order satisfies the following compatibility properties:

- if \(x \leq y\), then \(x + z \leq y + z\) for all \(x, y, z \in F\).
- if \(0 \leq x\) and \(0 \leq y\), then \(0 \leq x \cdot y\) for all \(x, y \in F\).

There are a lot of papers which study \(l\)-groups. Our goal was to prove that the set of all generalized multisets over \(\Sigma\) is an \(l\)-group. Many results in the general theory can be particularized to \(\mathbb{Z}(\Sigma)\). We present some of them without proof. The proofs can be found in the indicated references.

**Theorem 3.17 (Riesz Decomposition).** Let \(f, g_1, \ldots, g_n \in \mathbb{Z}(\Sigma)\) such that \(\theta \leq g_i, i = 1, \ldots, n\) and \(\theta \leq f \leq g_1 + \ldots + g_n\). Then there exist \(h_1, \ldots, h_n \in \mathbb{Z}(\Sigma)\) such that \(\theta \leq f = h_1 + \ldots + h_n\) and \(\theta \leq h_i \leq g_i, i = 1, \ldots, n\).

**Proof.** See Chapter 9 in [39]. \(\square\)

**Definition 3.16.** A subgroup \(H\) of an \(l\)-group \(G\) is an \(l\)-subgroup of \(G\) if \(H\) is a sublattice of \(G\). An \(l\)-subgroup \(H\) of an \(l\)-group \(G\) is called a convex \(l\)-subgroup if \(0 \leq g \leq h \in H\) and \(g \in G\) implies \(g \in H\). A normal convex \(l\)-subgroup \(H\) of an \(l\)-group \(G\) is called an \(l\)-ideal of \(G\).

**Remark 3.4.** In the theory of lattice-ordered groups \(l\)-ideals play the same role as normal subgroups in the ordinary theory of groups.

**Theorem 3.18.** For a convex \(l\)-subgroup \(G\) of \(\mathbb{Z}(\Sigma)\) the following are equivalent:

1. If \(H, K\) are two convex \(l\)-subgroups of \(\mathbb{Z}(\Sigma)\) such that \(H \cap K \subseteq G\), then either \(H \subseteq G\) or \(K \subseteq G\).
2. If \(H, K\) are two convex \(l\)-subgroups of \(\mathbb{Z}(\Sigma)\) such that \(H \supseteq G\) and \(K \supseteq G\), then \(H \cap K \supseteq G\).
3. The lattice of the cosets of \(G\) with the induced order is totally ordered.
4. The set of convex \(l\)-subgroups of \(\mathbb{Z}(\Sigma)\) which contain \(G\) is a totally ordered set under inclusion.

**Definition 3.17.** 1. A map \(f\) between two \(l\)-groups \(G\) and \(H\) is an \(l\)-homomorphism \((l\text{-isomorphism})\) if \(f\) is a group homomorphism (isomorphism) and \(f(g \wedge g') = f(g) \wedge f(g')\) for all \(g, g' \in G\).
2. A map $f$ between two $o$-groups $G$ and $H$ is an $o$-homomorphism (or-isomorphism) if $f$ is a group homomorphism (isomorphism) and $f(g) \leq f(g')$ for all $g, g' \in G$ with $g \leq g'$.

**Remark 3.5.** If $f$ is an $l$-homomorphism between two $l$-groups $G$ and $H$, we can also prove that $f(g \vee g') = f(g) \vee f(g')$ for all $g, g' \in G$.

The following three theorems justify Remark 3.4.

**Theorem 3.19.** For an $l$-subgroup $G$ of $\mathbb{Z}(\Sigma)$ the following are equivalent:

1. $G$ is an $l$-ideal.
2. $G$ is the kernel of an $l$-homomorphism.

**Theorem 3.20.** Let $G$ and $H$ be two $l$-ideals of $\mathbb{Z}(\Sigma)$ with $H \subseteq G$. Then $G/H$ is an $l$-ideal of $\mathbb{Z}(\Sigma)/H$, and $\mathbb{Z}(\Sigma)/G$ is $l$-isomorphic to $(\mathbb{Z}(\Sigma)/H)/(G/H)$.

**Theorem 3.21.** Let $G$ be an $l$-subgroup of $\mathbb{Z}(\Sigma)$ and $H$ a convex $l$-subgroup of $\mathbb{Z}(\Sigma)$ such that $H$ is normal in the $l$-group generated by $G \cup H$. Then $G \cap H$ is an $l$-ideal in $G$, $G + H$ is an $l$-subgroup of $\mathbb{Z}(\Sigma)$, and $G/(G \cap H)$ is $l$-isomorphic to $(G + H)/H$.

**Definition 3.18.** An ordered permutation group $(G, \Omega)$ is a permutation group $(G, \cdot)$ (i.e. a subgroup of the group of all bijections $f : \Omega \to \Omega$) acting on a totally ordered set $(\Omega, <)$ where for all $a, b \in \Omega$ we have $a < b$ iff $g(a) < g(b)$ for all $g \in G$.

The group $G$ defined before is a po-group with the partial order given by:

$$
\text{for } g, g' \in G \text{ we have } g \leq g' \iff g(a) \leq g'(a) \text{ for all } a \in \Omega.
$$

If this partial order is a lattice order so that $G$ is an $l$-group, then $(G, \Omega)$ is called a lattice-ordered permutation group ($l$-permutation group).

**Example 3.2.** Let $(\Omega, <)$ be a partially ordered set and $\text{Aut}(\Omega, <) \not= \text{A}(\Omega)$ the group of all permutations of $\Omega$ that preserve the order $<$. Thus, a permutation $f : \Omega \to \Omega$ belongs to $\text{A}(\Omega)$ iff $f(a) < f(b)$ whenever $a < b$ in $\Omega$. We define the relation $\leq$ on $\text{A}(\Omega)$ by: $f \leq g$ iff $f(a) \leq g(a)$ for all $a \in \Omega$. It is easy to prove that $(\text{A}(\Omega), \leq)$ is a po-group. Moreover, if $(\Omega, <)$ is a totally ordered set, then $\text{A}(\Omega)$ is an $l$-group.

Every $l$-permutation group $(G, \Omega)$ is an $l$-subgroup of $\text{A}(\Omega)$. Conversely every $l$-subgroup of $\text{A}(\Omega)$ is an $l$-permutation group according to Definition 3.18.

Holland’s theorem is a generalization for $l$-groups of the well-known theorem of Cayley for groups. Cayley’s theorem states that each group $G$ can be embedded in the symmetric group of $G$ [133]. Holland’s theorem (presented in [90]) says that every $l$-group can be $l$-embedded in the $l$-group $\text{A}(\Omega)$ for some totally ordered set $\Omega$. As a particular case of Holland’s theorem, for the $l$-group $\mathbb{Z}(\Sigma)$ we get Theorem 3.22.

**Theorem 3.22.** $\mathbb{Z}(\Sigma)$ is $l$-isomorphic to an $l$-permutation group.
An application of Holland’s theorem is Weinberg’s theorem which says that every \( l \)-group can be \( l \)-embedded in the \( l \)-group \( A(F) \) for some totally ordered field \( F \) (see Definition 3.15). This means that every \( l \)-group is \( l \)-isomorphic to an \( l \)-subgroup of \( A(F) \) for some totally ordered field \( F \) (the construction of \( A(F) \) is presented in Example 3.2 with the set \( \Omega \) instead of the set \( F \)). For the proof of Weinberg’s theorem see for example Theorem 7.B in [79]. Since \( \mathbb{Z}(\Sigma) \) is an \( l \)-group, we get Theorem 3.23.

**Theorem 3.23.** \( \mathbb{Z}(\Sigma) \) is \( l \)-isomorphic to an \( l \)-subgroup of \( A(F) \) for some totally ordered field \( F \).

Theorem 3.23 can also be proved directly from another result belonging to Holland which says that every countable \( l \)-group can be \( l \)-embedded in \( Aut(\mathbb{Q}, \leq) \), and hence in \( Aut(\mathbb{R}, \leq) \). So, \( \mathbb{Z}(\Sigma) \) can be \( l \)-embedded in \( Aut(\mathbb{Q}, \leq) \), and hence in \( Aut(\mathbb{R}, \leq) \) (\( \leq \) is the usual order on \( \mathbb{Q} \) and on \( \mathbb{R} \)).

In [104], Levi proved that an abelian group is an \( o \)-group if and only if it is torsion free. This means we can find a total order on \( \mathbb{Z}(\Sigma) \) such that \( \mathbb{Z}(\Sigma) \) is an \( o \)-group. In this case things are more clear than they seem to be. We recall that \( \mathbb{Z}(\Sigma) \) is the free abelian group with basis \( \tilde{\Sigma} = \{ \tilde{a}_1, \ldots, \tilde{a}_k \} \). If \( |\tilde{\Sigma}| = k \), we denote \( I = \{ 1, \ldots, k \} \). If \( f, g \in \mathbb{Z}(\Sigma) \) and \( f \neq g \), then \( f \) and \( g \) can be uniquely expressed as \( f = \sum_{i \in I} x_i \tilde{a}_i \) and \( g = \sum_{i \in I} y_i \tilde{a}_i \) with \( x_i, y_i \in \mathbb{Z} \); we define \( f < g \) iff \( x_j < y_j \) (as integer numbers) where \( j \) is the greatest \( i \in I \) such that \( x_j \neq y_j \). The relation \( < \) is a total order relation and \( (\mathbb{Z}(\Sigma), <) \) is an \( o \)-group.

We already know (from [149]) that \( \mathbb{Z}(\Sigma) = FA(\tilde{\Sigma}) = F(\tilde{\Sigma})/D(F(\tilde{\Sigma})) \). A general result in the theory of \( l \)-groups says that whenever \( F \) is a free group, for each total order of the free abelian group \( F/D(F) \), there is a total order of \( F \) such that the natural surjection of \( F \) onto \( F/D(F) \) is an \( o \)-homomorphism (see Theorem 3.8 in [150]). A consequence of this fact is the following theorem.

**Theorem 3.24.** For the total order \( < \) on \( \mathbb{Z}(\Sigma) \), there is a total order on \( F(\tilde{\Sigma}) \) such that the natural surjection of \( F(\tilde{\Sigma}) \) onto \( F(\tilde{\Sigma})/D(F(\tilde{\Sigma})) = \mathbb{Z}(\Sigma) \) is an \( o \)-homomorphism.

From general group theory (general module theory), we know that every torsion-free abelian group can be embedded (as a group) in a rational vector space. This means every torsion-free abelian group (particularly \( \mathbb{Z}(\Sigma) \)) can be embedded as a group in a divisible group. For ordered groups there is a stronger result (presented as Corollary 8.6.3 in [79]) which says that each \( l \)-group can be \( l \)-embedded in a divisible \( l \)-group. We can present the following theorem.

**Theorem 3.25.** There is an injective \( l \)-homomorphism between \((\mathbb{Z}(\Sigma), \wedge, \vee)\) and a divisible \( l \)-group.

Of course, some of these properties of the set of all generalized multisets can be proved directly, because \( \mathbb{Z}(\Sigma) \) has a well-known structure. However, we want to emphasize the benefits of the theory of \( l \)-groups on a particular example and to present some results of \( \mathbb{Z}(\Sigma) \) which are not trivial and cannot easily be obtained in
another way. Anyway, since \( \mathbb{Z}(\Sigma) \) is a particularly well-known group, the results presented in this section could be more easily proved than in the general theory. For example, although the general result from which we get Theorem 3.25 has a difficult proof, for \( \mathbb{Z}(\Sigma) \) things are more clear. If we denote by \( \mathbb{Q}(\Sigma) \) the set of all functions \( f : \Sigma \to \mathbb{Q} \) where \( \mathbb{Q} \) is the field of rational numbers, then \((\mathbb{Q}(\Sigma), \preceq)\) is an \( l \)-group (\( \preceq \) is the partial order relation defined by \( f \preceq g \) iff \( f(u) \leq g(u) \) for all \( u \in \Sigma \)). Moreover, \( \mathbb{Q}(\Sigma) \) is divisible, and the standard inclusion \( i : \mathbb{Z}(\Sigma) \to \mathbb{Q}(\Sigma) \) is an injective \( l \)-morphism. However, the direct proofs of the other theorems are not trivial. For them the general theory of \( l \)-groups is useful.

3.2.1.3 Generalized Multisets in Reverse Mathematics

The theory of \( l \)-groups was studied from the perspective of Reverse Mathematics in [86, 132, 147]. Reverse Mathematics [144] is a subfield of logic which tries to discover exactly which set-theoretic axioms are truly necessary to prove a theorem. The usual axioms of set theory, ZFC or ZF, are quite strong. We can make finer distinctions by restricting ourselves to “countable” mathematics and axiom systems which, though weaker, are still able to prove many classical theorems of mathematics. More formally, the setting for Reverse Mathematics is the language of second-order arithmetic \( \mathbb{Z}_2 \). In second-order arithmetic, all objects must be represented as either natural numbers or sets of natural numbers. Reverse Mathematics is useful for studying theorems of either countable or essentially countable mathematics.

The complete set comprehension scheme for \( \mathbb{Z}_2 \) consists of axioms which say that if we have a formula in \( \mathbb{Z}_2 \), the set of numbers which satisfy it exists. Mathematically, this can be expressed as: \( \exists X \forall a (a \in X \leftrightarrow \phi(a)) \) where \( \phi \) is any formula in the language \( \mathbb{Z}_2 \) not mentioning \( X \). This full collection is too strong to be interesting for Reverse Mathematics, but it contains five particular subsystems. Here we mention just two of them. A complete study of these subsystems may be found in [132] or [144].

\( RCA_0 \) is the system whose set comprehension scheme is limited to \( \Delta^0_1 \) formulas (axioms allowing \( \Sigma^0_1 \) induction are also included). Clearly, \( RCA_0 \) contains the ordered semiring axioms for the natural numbers, plus \( \Delta^0_1 \) comprehension, \( \Sigma^0_1 \) formula induction and the set induction axiom: \( \forall X((0 \in X \land \forall n (n \in X \to n + 1 \in X)) \to \forall n (n \in X)) \); the \( \Delta^0_1 \) comprehension scheme consists of all axioms of the form: \( \forall n (\phi(n) \leftrightarrow \psi(n)) \to \exists X \forall n (n \in X \leftrightarrow \phi(n)) \) where \( \phi \) is a \( \Sigma^0_1 \) formula, \( \psi \) is a \( \Pi^0_1 \) formula and \( X \) does not occur free in either \( \phi \) or \( \psi \). The \( \Sigma^0_1 \) formula induction scheme contains the following axiom for each \( \Sigma^0_1 \) formula \( \phi \): \( (\phi(0) \land \forall n (\phi(n) \to \phi(n + 1))) \to \forall n (\phi(n)) \). \( RCA_0 \) essentially corresponds to computable or recursive mathematics. \( RCA_0 \) is strong enough to establish the basic facts about the number systems \( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \) and \( \mathbb{R} \) (as a set of sequences of rational numbers).

Another subsystem is \( WKL_0 \) which consists of all the axioms of \( RCA_0 \) plus the Weak Konig’s Lemma axiom saying “If \( T \) is an infinite subtree of the full binary tree (i.e. of the tree of all finite sequences of 0’s and 1’s), then \( T \) has an infinite path”
3.2 Generalized Multisets in Finitely Supported Mathematics

Many properties of $\mathbb{Z}(\Sigma)$ remain valid if some axioms from Zermelo-Fraenkel with Choice (ZFC) set theory are relaxed. First, $\mathbb{Z}(\Sigma)$ is an $I$-group according to the $\text{RCA}_0$ axioms. Indeed, $\mathbb{Z}(\Sigma)$ is a free abelian group with a finite number of generators, and so $\mathbb{Z}(\Sigma)$ is a set in $\text{RCA}_0$ (see Example 3.3 in [147], or Example 2.5 in [146] - the part where a free abelian group with $\omega$ generators is organized as a group in $\text{RCA}_0$; the proof of this part remains valid even if $\mathbb{Z}(\Sigma)$ has a finite (countable) number of generators). Another possibility of representing $\mathbb{Z}(\Sigma) = \mathbb{Z^\Sigma}$ as a set in second-order arithmetic is to use finite sequences of pairs $(x, z)$ with $x \in \Sigma$ and $z \in \mathbb{Z} \setminus \{0\}$. This was done in Definition 3.4 from [148] which can also be applied to our case since $\Sigma$ is a finite set. Moreover, the binary operations on $\mathbb{Z}(\Sigma)$ satisfy the conditions on Definition 2.6 in [132]. This means that $\mathbb{Z}(\Sigma)$ is an $I$-group in $\text{RCA}_0$.

Now, according to Theorem 2.21 in [132], we can say that Theorem 3.17 is provable in $\text{RCA}_0$. By Theorem 5.3 in [132], it follows that Theorem 3.18 is provable in $\text{RCA}_0$. An important result presented as Corollary 6.5 in [132] shows us that Theorem 3.22 is provable in $\text{WKL}_0$. Since $F(\Sigma)$ (and $F(\tilde{\Sigma})$) is free with a countable (finite) number of generators, we obtain that $F(\Sigma)$ (and $F(\tilde{\Sigma})$) is an $o$-group in $\text{RCA}_0$ (see Corollary 5.2 in [147], or Proposition 5.5 and Corollary 5.3 in [146]). Moreover, in $\text{RCA}_0$ Theorem 3.24 which says that $\mathbb{Z}(\Sigma)$ is the $o$-epimorphic image of a totally ordered free group is also provable (see the proof of Theorem 5.7 in [146]).

We conclude that, even if we replace some axioms of ZFC set theory with weaker ones, many properties of $\mathbb{Z}(\Sigma)$ obtained in the ZFC framework are preserved. Our next goal will be to study the properties of $\mathbb{Z}(\Sigma)$ when ZFC is replaced by FSM.

### 3.2.2 Generalized Multisets over Infinite Alphabets

We now formalize the concept of generalized multisets in FSM. According to Example 2.1(4), we already know that $\mathbb{Z}$ is an $S_A$-set with the $S_A$-action $\cdot : S_A \times \mathbb{Z} \to \mathbb{Z}$ defined by $\pi \cdot x := x$ for all $\pi \in S_A$ and $x \in \mathbb{Z}$. Also $\mathbb{Z}$ is an invariant set because for each $x \in \mathbb{Z}$ we have that $\emptyset$ supports $x$. Moreover, $\text{supp}(x) = \emptyset$ for each $x \in \mathbb{Z}$.

**Definition 3.19.** Given an invariant set $(\Sigma, \cdot)$ (possible infinite), any function $f : \Sigma \to \mathbb{Z}$ with the property that $S_f \overset{\text{def}}{=} \{ x \in \Sigma | f(x) \neq 0 \}$ is finite is called an extended generalized multiset over $\Sigma$. The set of all extended generalized multisets over $\Sigma$ is denoted by $\mathbb{Z}^{\text{ext}}(\Sigma)$.

We remark that each function $f \in \mathbb{Z}^{\text{ext}}(\Sigma)$ can be expressed as $f = \sum_{a \in \Sigma} f(a) \cdot \tilde{a}$. Since $S_f$ is finite, the previous sum is finite. Therefore, $\mathbb{Z}^{\text{ext}}(\Sigma)$ is a free abelian group with basis $\tilde{\Sigma}$. Whenever $\Sigma$ is finite we have $\mathbb{Z}^{\text{ext}}(\Sigma) = \mathbb{Z}(\Sigma)$. As in the previous section (see Proposition 3.3) we can prove the following.
Proposition 3.11. Let $(\Sigma, \cdot)$ be an invariant set. Then each function $f \in \mathcal{Z}_{ext}(\Sigma)$ is finitely supported in the sense of Definition 2.7. Moreover, $\text{supp}(f) = \text{supp}(S_f)$.

Definition 3.20. An invariant group is a triple $(G, \cdot, \circ)$ such that the following conditions are satisfied:

- $(G, \cdot)$ is a group.
- $(G, \circ)$ is a non-trivial invariant set (see Example 2.1(4)).
- for each $\pi \in S_A$ and each $x, y \in G$ we have $\pi \circ (x \cdot y) = (\pi \circ x) \cdot (\pi \circ y)$, which means the internal law on $G$ is equivariant.

Example 3.3. The group $(S_A, \circ)$ is an invariant group, where $\circ$ is the usual composition of permutations and $\cdot$ is the $S_A$-action on $S_A$ defined as in Example 2.1(3). Since the composition law on $S_A$ is associative, one can easily verify that $\pi \cdot (\sigma \circ \tau) = (\pi \cdot \sigma) \circ (\pi \cdot \tau)$ for all $\pi, \sigma, \tau \in S_A$.

According to Proposition 3.8, we know that $(\mathbb{Z}(\Sigma), +)$ is a free abelian group if we work in the ZF framework. Analogously $(\mathcal{Z}_{ext}(\Sigma), +)$ is a free abelian group. As in the case of multisets (Theorem 3.4), in FSM we have the following result.

Theorem 3.26. $\mathcal{Z}_{ext}(\Sigma)$ is a free abelian invariant group whenever $(\Sigma, \cdot)$ is an invariant set.

For invariant groups we also have a universality property which is corresponds to Proposition 3.9 in FSM. Its proof is similar to the proof of Theorem 3.5.

Theorem 3.27. Let $(\Sigma, \cdot)$ be an invariant set. Let $j: \Sigma \to \mathcal{Z}_{ext}(\Sigma)$ be the function which maps each $a \in \Sigma$ into $\tilde{a} \in \tilde{\Sigma}$. If $(G, +, \circ)$ is an arbitrary abelian invariant group and $\varphi: \Sigma \to G$ is an arbitrary finitely supported function, then there exists a unique finitely supported homomorphism of abelian groups $\psi: \mathcal{Z}_{ext}(\Sigma) \to G$ with $\psi \circ j = \varphi$, i.e. $\psi(\tilde{a}) = \varphi(a)$ for all $a \in \Sigma$. Moreover, if a finite set $S$ supports $\varphi$, then the same set $S$ supports $\psi$. Therefore, if $\varphi$ is equivariant, then $\psi$ is also equivariant.

In the previous subsection we established a connection between $\mathbb{Z}(\Sigma)$ and the free group on $\Sigma$ denoted by $F(\Sigma)$. A similar result can be proved in FSM.

Theorem 3.28. $F(\Sigma)$ is an invariant group whenever $(\Sigma, \cdot)$ is an invariant set.

Proof. We claim that $(F(\Sigma), \tilde{x})$ is an invariant set with the $S_A$-action $\tilde{x}: S_A \times F(\Sigma) \to F(\Sigma)$ defined by $\tilde{x}[x_1^{e_1} x_2^{e_2} \ldots x_l^{e_l}] = [(\pi \circ x_1)^{e_1} (\pi \circ x_2)^{e_2} \ldots (\pi \circ x_l)^{e_l}]$ for all $\pi \in S_A$ and $[x_1^{e_1} x_2^{e_2} \ldots x_l^{e_l}] \in F(\Sigma)$. First we remark that the function $\tilde{x}: S_A \times F(\Sigma) \to F(\Sigma)$ is well defined (it does not depend on the chosen representatives for the words in $F(\Sigma)$). Indeed, let $x_1^{e_1} x_2^{e_2} \ldots x_l^{e_l}$ and $y_1^{d_1} y_2^{d_2} \ldots y_m^{d_m}$ be two words in the same equivalence class. This means that $y_1^{d_1} y_2^{d_2} \ldots y_m^{d_m}$ can be obtained from $x_1^{e_1} x_2^{e_2} \ldots x_l^{e_l}$ by repeatedly cancelling or inserting terms of the form $x^{-1}x$ or $xx^{-1}$ for $x \in \Sigma$. When a term of the form $xx^{-1}$ is inserted in the word $x_1^{e_1} x_2^{e_2} \ldots x_l^{e_l}$ we obtain a new word $x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} x_n^{-1} x_n^{e_n} \ldots x_l^{e_l}$. If $y_1^{d_1} y_2^{d_2} \ldots y_m^{d_m}$ is the word $x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} \ldots x_l^{e_l}$ then we have that $\tilde{x}[y_1^{d_1} y_2^{d_2} \ldots y_m^{d_m}] = \tilde{x}[x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} \ldots x_l^{e_l}] = [(\pi \circ x_1)^{e_1} (\pi \circ x_2)^{e_2} \ldots (\pi \circ x_l)^{e_l}]$. Therefore, if $\varphi$ is equivariant, then $\psi$ is also equivariant.
3.2 Generalized Multisets in Finitely Supported Mathematics

Let $\pi: S_A \times F(\Sigma) \to F(\Sigma)$ be a group action on $F(\Sigma)$ in the sense of Definition 2.2 because $\circ: S_A \times \Sigma \to \Sigma$ is an $S_A$-action on $\Sigma$ and it satisfies the axioms of a group action on $\Sigma$ presented in Definition 2.2. It is trivial to prove that $\delta \circ [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}] = [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]$, and $\pi \circ [\pi^*(x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n})] = (\pi \circ \pi^*)\pi(x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n})$ for all $\pi, \pi' \in S_A$ and $[x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}] \in F(\Sigma)$. Let $[x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]$ be an arbitrary element from $F(\Sigma)$. It is routine to check that the finite set $\text{supp}(x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n})$ supports $[x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]$. Finally, $\pi \circ [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}] = \pi(x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n})$.

Theorem 3.16 which represents the universality property of $F(\Sigma)$ in the ZF framework has an analogue in FSM.

**Theorem 3.29.** Let $(\Sigma, \circ_\Sigma)$ be an invariant set. Let $i: \Sigma \to F(\Sigma)$ be the standard inclusion of $\Sigma$ into $F(\Sigma)$ which maps each element $a \in \Sigma$ into the word $[a]$. If $(G, \cdot, \circ_G)$ is an arbitrary invariant group and $\phi: \Sigma \to G$ is an arbitrary finitely supported function, then there exists a unique finitely supported homomorphism of groups $\psi: F(\Sigma) \to G$ with $\psi \circ i = \phi$. Moreover, if a finite set $S$ supports $\phi$, then the same set $S$ supports $\psi$. Therefore, if $\phi$ is equivariant, then $\psi$ is also equivariant.

**Proof.** First we show that the statement of the theorem is well formed in FSM. For this, we have to prove that $i$ is finitely supported. We prove that $i$ is equivariant. Following the view of Corollary 2.3 we must prove that $i(\pi \circ_\Sigma x) = \pi \circ i(x)$ for each $\pi \in S_A$ and each $x \in \Sigma$. Let $\pi \in S_A$ and $x \in \Sigma$ be arbitrary elements. From the definition of $i$, we know that $\pi \circ i(x) = [\pi \circ_\Sigma x]$. From the definition of $\pi$, we know that $\pi \circ i(x) = \pi \circ i[x] = [\pi \circ_\Sigma x]$. If $(G, \cdot, \circ_G)$ is an invariant group, then, clearly, $(G, \cdot)$ is a group. From the general theory of groups, we can define a unique homomorphism of groups $\psi: F(\Sigma) \to G$ with $\psi \circ i = \phi$. It remains to prove that $\psi$ is indeed finitely supported.

We prove that $S = \text{supp}(\phi)$ supports $\psi$. Let $\pi \in \text{Fix}(S)$. We have $\phi(\pi \circ_\Sigma x) = \pi \circ_G \phi(x)$ for all $x \in \Sigma$. In the view of Proposition 2.4 for proving that $\psi$ is finitely supported, it is sufficient to prove that $\psi(\pi \circ_\Sigma [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]) = \pi \circ_G \psi([x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}])$ for each $[x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}] \in F(\Sigma)$. However, $\psi$ is a group homomorphism between $F(\Sigma)$ and $G$, and $\psi \circ i = \phi$. This means $\psi([x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]) = \phi([x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}])$. Hence, $\psi(\pi \circ_\Sigma [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]) = \pi \circ G \psi([x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}])$. However, we have $\pi \circ_\Sigma [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}] = ([\pi \circ_\Sigma x_1^{e_1}]\ldots [\pi \circ_\Sigma x_n^{e_n}])$, and so we obtain $\psi(\pi \circ_\Sigma [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]) = \psi(([\pi \circ_\Sigma x_1^{e_1}]\ldots [\pi \circ_\Sigma x_n^{e_n}])) = \phi([\pi \circ_\Sigma x_1^{e_1}]\ldots [\pi \circ_\Sigma x_2^{e_2}\ldots [\pi \circ_\Sigma x_n^{e_n}]).$ Hence, $\psi(\pi \circ_\Sigma [x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}]) = \pi \circ G \psi([x_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}])$ for each $\pi \in \text{Fix}(S)$, which means $S$ supports $\psi$. 


Several results obtained in the previous subsection (in the ZF framework) can be translated into FSM.

If in the statement of Theorem 3.29, we replace \( G \) with \( \mathbb{Z}_{\text{ext}}(\Sigma) \), and \( \varphi : \Sigma \to G \) with \( j : \Sigma \to \mathbb{Z}_{\text{ext}}(\Sigma) \) where \( j \) maps each \( a \) into \( \tilde{a} \), we get an equivariant group homomorphism \( \psi : F(\Sigma) \to \mathbb{Z}_{\text{ext}}(\Sigma) \) such that \( \psi \circ i = j \), where \( i : \Sigma \to F(\Sigma) \) is the standard inclusion of \( \Sigma \) into \( F(\Sigma) \) which maps each element \( a \in \Sigma \) into the word \([a]\). Now if \( w = [x_1^1x_2^2 \ldots x_n^n] \) then we obtain that \( \psi(w) = \varepsilon_1 j(x_1) + \varepsilon_2 j(x_2) + \ldots + \varepsilon_n j(x_n) \). Now, clearly, \( \psi \) is surjective and, from the first isomorphism theorem for groups, we have \( F(\Sigma)/\text{Ker }\psi \cong \mathbb{Z}_{\text{ext}}(\Sigma) \). Moreover, in FSM we have the next result.

**Proposition 3.12.** \( F(\Sigma)/\text{Ker }\psi \) is an invariant group and the isomorphism \( \Theta \) between the groups \( F(\Sigma)/\text{Ker }\psi \) and \( \mathbb{Z}_{\text{ext}}(\Sigma) \) defined by \( \Theta(w \uparrow \text{Ker }\psi) = \psi(w) \) for each \( w \in F(\Sigma) \) (where \( w \uparrow \text{Ker }\psi \) is the left coset of \( w \) modulo \( \text{Ker }\psi \)) is equivariant.

**Proof.** We remark that \( \Theta \) is defined as in the standard proof of the first isomorphism theorem for groups. First we prove that we can define an invariant structure on \( F(\Sigma)/\text{Ker }\psi \). We know that \( (F(\Sigma), \varkappa) \) is an invariant set (Theorem 3.28). We define \( \circ : S_A \times F(\Sigma)/\text{Ker }\psi \to F(\Sigma)/\text{Ker }\psi \) by \( \pi \circ (w \uparrow \text{Ker }\psi) = (\pi \circ w) \uparrow \text{Ker }\psi \) for each \( w \in F(\Sigma) \) and each \( \pi \in S_A \). First we show that \( \circ \) is a well-defined function. Let \( w = [x_1^1x_2^2 \ldots x_n^n] \) and \( v = [y_1^1y_2^2 \ldots y_m^m] \) be two elements in \( F(\Sigma) \) such that \( \circ \uparrow \text{Ker }\psi = v \uparrow \text{Ker }\psi \). This means \( \psi(w) = \psi(v) \) which by the definition of \( \psi \) is the same as \( \varepsilon_1 j(x_1) + \varepsilon_2 j(x_2) + \ldots + \varepsilon_n j(x_n) = \delta_1 j(y_1) + \delta_2 j(y_2) + \ldots + \delta_m j(y_m) \). Now we have \( \pi \ast (\varepsilon_1 j(x_1) + \varepsilon_2 j(x_2) + \ldots + \varepsilon_n j(x_n)) = \pi \ast (\delta_1 j(y_1) + \delta_2 j(y_2) + \ldots + \delta_m j(y_m)) \) for each \( \pi \in S_A \). Therefore, \( (\pi \circ w) \uparrow \text{Ker }\psi = (\pi \circ v) \uparrow \text{Ker }\psi \) for each \( \pi \in S_A \), which means that \( \circ \) is well defined. Since \( \varkappa \) is an \( S_A \)-action on \( F(\Sigma) \), an easy calculation shows us that \( \circ \) is an \( S_A \)-action on \( F(\Sigma)/\text{Ker }\psi \). Moreover, each element in \( F(\Sigma)/\text{Ker }\psi \) is supported by the support of its representative. Therefore, \( (F(\Sigma)/\text{Ker }\psi, \circ) \) is an invariant set. Since \( (F(\Sigma), \varkappa, \varkappa) \) is an invariant group (the axioms in Definition 3.20 are satisfied), it is trivial to check that \( (F(\Sigma)/\text{Ker }\psi, \uparrow, \circ) \) (we denote also by \( \uparrow \) the internal law on the factor group \( F(\Sigma)/\text{Ker }\psi \)) is an invariant group; the proof is an easy calculation which uses only the definition of \( \circ \) and the distributivity property of \( \varkappa \) over \( \uparrow \). We claim that \( \Theta \) is equivariant. For this, in the view of Proposition 2.4, it is sufficient to prove that for each \( \pi \in S_A \) we have \( \Theta((\pi \circ (w \uparrow \text{Ker }\psi)) = \pi \ast (\Theta(w \uparrow \text{Ker }\psi)) \), \( \forall w \in F(\Sigma) \). Let \( \pi \in S_A \) be an arbitrary element. Since \( \psi \) is equivariant, we have \( \Theta((\pi \circ (w \uparrow \text{Ker }\psi)) = \Theta((\pi \circ w) \uparrow \text{Ker }\psi) = \psi(\pi \circ w) = \pi \ast \psi(w) = \pi \ast (\Theta(w \uparrow \text{Ker }\psi)) \). This means \( \Theta \) is equivariant. \( \square \)

If \( \Sigma = \{a_1, \ldots, a_k\} \), the Parikh image \( \varphi_\Sigma : F(\Sigma) \to \mathbb{Z}^k \) is finitely supported. Indeed, \( \mathbb{Z} \) is an \( S_A \)-set with the \( S_A \)-action \( \cdot : S_A \times \mathbb{Z} \to \mathbb{Z} \) defined by \( \pi \cdot x := x \) for all \( \pi \in S_A \) and \( x \in \mathbb{Z} \). From Subsection 2.4.2, we know how an \( S_A \)-action on the Cartesian product of two invariant sets looks like. Therefore, \( \mathbb{Z}^k \) is endowed with a trivial \( S_A \)-action defined by \( \pi \cdot x := x \) for all \( \pi \in S_A \) and \( x \in \mathbb{Z}^k \). Also \( \mathbb{Z}^k \) is an invariant set because
for each \( x \in \mathbb{Z}^k \) we have that \( \emptyset \) supports \( x \). We prove that \( U = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k) \) supports \( \varphi \Sigma \). In the view of Proposition 2.4 we must prove that we have \( \varphi \Sigma ((\pi \ast [x_1^1 x_2^2 \ldots x_n^n]) = \varphi \Sigma ([x_1^1 x_2^2 \ldots x_n^n]) \) (because the \( S_A \)-action \( \pi \ast [x_1^1 x_2^2 \ldots x_n^n] \) is trivial) for each \( \pi \in \text{Fix}(U) \) and each \([x_1^1 x_2^2 \ldots x_n^n] \in F(\Sigma) \). Indeed, if \( \pi \in \text{Fix}(U) \), then we have \( \pi \ast [x_1^1 x_2^2 \ldots x_n^n] = [x_1^1 x_2^2 \ldots x_n^n] \) (Theorem 3.28) and hence we obtain the relation: \( \varphi \Sigma ((\pi \ast [x_1^1 x_2^2 \ldots x_n^n]) = \varphi \Sigma ([x_1^1 x_2^2 \ldots x_n^n]) \) (because the \( S_A \)-action \( \pi \ast [x_1^1 x_2^2 \ldots x_n^n] \) is trivial) for each \( \pi \in \text{Fix}(U) \) and each \([x_1^1 x_2^2 \ldots x_n^n] \in F(\Sigma) \).

If in the statement of Theorem 3.27, we replace \( G \) with \( \mathbb{Z}^k \) and \( \varphi : \Sigma \rightarrow G \) with the function \( \varphi_\Sigma \circ i \) where \( i : \Sigma \rightarrow F(\Sigma) \) is the standard inclusion of \( \Sigma \) into \( F(\Sigma) \) which maps each element \( a_u \in \Sigma \) into the word \( [a_u] \), then there exists a unique finitely supported homomorphism of abelian groups \( \varphi_\Sigma : \mathbb{Z}(\Sigma) \rightarrow \mathbb{Z} \) with \( \varphi_\Sigma \circ j = \varphi \Sigma \circ i \), that is, \( \varphi_\Sigma (\tilde{a}_u) = \varphi_\Sigma ([a_u]) = (0, \ldots, 0, 1, 0, \ldots, 0) = e_u \) for all \( a_u \in \Sigma \).

Loeb’s order introduced in Definition 3.12 can be naturally extended to \( \mathbb{Z}_{\text{ext}}(\Sigma) \). The following theorem characterizes Loeb’s order in FSM.

**Theorem 3.30.** If \( (\Sigma, \cdot) \) is an invariant set, then \( (\mathbb{Z}_{\text{ext}}(\Sigma), \ast, \subseteq) \) is an invariant partially ordered set, where \( \subseteq \) represents Loeb’s order introduced in Definition 3.12.

**Proof.** According to Proposition 3.11, we have that \( (\mathbb{Z}_{\text{ext}}(\Sigma), \ast) \) is an invariant set with the \( S_A \)-action \( \ast : S_A \times \mathbb{Z}_{\text{ext}}(\Sigma) \rightarrow \mathbb{Z}_{\text{ext}}(\Sigma) \) defined by \( (\pi \ast f)(x) = f(\pi^{-1} \cdot x) \) for all \( \pi \in S_A \), \( f \in \mathbb{Z}_{\text{ext}}(\Sigma) \) and \( x \in \Sigma \). Let \( f, g \in \mathbb{Z}_{\text{ext}}(\Sigma) \) such that \( f \subseteq g \). This means either \( f(u) \ll g(u) \) for all \( u \in \Sigma \), or \( g(u) = f(u) \) for all \( u \in \Sigma \). We must prove that \( \pi \ast f \subseteq \pi \ast g \).

Case \( f(u) \ll g(u) \) for all \( u \in \Sigma \). Let \( x \in \Sigma \). We have \( (\pi \ast f)(x) = f(\pi^{-1} \cdot x) \ll g(\pi^{-1} \cdot x) = (\pi \ast g)(x) \). Thus, \( (\pi \ast f)(x) \ll (\pi \ast g)(x) \) for all \( x \in \Sigma \), and \( \pi \ast f \subseteq \pi \ast g \).

Case \( g(u) = f(u) \) for all \( u \in \Sigma \). Let \( x \in \Sigma \). We have \( (\pi \ast g)(x) - (\pi \ast f)(x) = g(\pi^{-1} \cdot x) - f(\pi^{-1} \cdot x) \ll 0 \). Therefore, \( (\pi \ast g)(x) - (\pi \ast f)(x) \ll (\pi \ast g)(x) \) for all \( x \in \Sigma \), and \( \pi \ast f \subseteq \pi \ast g \). \( \square \)

Analogously we can prove the following.

**Theorem 3.31.** If \( (\Sigma, \cdot) \) is an invariant set, then \( (\mathbb{Z}_{\text{ext}}(\Sigma), \ast, \preceq) \) is an invariant partially ordered set.

A subsection which would be the analogue of Subsection 3.1.3 for generalized multisets can also be presented. However, we consider that the results would be very similar to those obtained in the case of multisets, so they do not deserve special attention.

### 3.3 Order Theory in Finitely Supported Mathematics

Order theory enters into computer science in a variety of ways and at a variety of levels. In particular, partially ordered sets are employed in logic, formal methods, programming languages and static analysis.
3.3.1 Partially Ordered Sets

We translate the classical notions from the theory of partially ordered sets into FSM.

**Definition 3.21.** An invariant partially ordered set (invariant poset) is an invariant set \((E, \cdot)\) together with an equivariant partial order relation \(\sqsubseteq\) on \(E\). An invariant poset is denoted by \((E, \sqsubseteq, \cdot)\) or simply \(E\).

A partial order relation \(\sqsubseteq\) on \(E\) is a subset of the Cartesian product \(E \times E\); this relation is reflexive, anti-symmetric and transitive. According to Definition 2.5, \(\sqsubseteq\) is equivariant if it is finitely supported as a subset of the Cartesian product \(E \times E\) in the sense of Definition 2.6 and its support is empty. This means that \(\sqsubseteq\) is equivariant iff for each pair \((e, e') \in \sqsubseteq\) and each \(\pi \in S_A\) we have that \(\pi \cdot (e, e') \in \sqsubseteq\) (where \(\cdot\) represents the \(S_A\)-action on the Cartesian product \(E \times E\) constructed as in Subsection 2.4.2). If we write “\((e, e') \in \sqsubseteq\)” as “\(e \sqsubseteq e'\)” , the equivariance property of \(\sqsubseteq\) can be expressed by 

\[
e \sqsubseteq e' \text{ implies } \pi \cdot e \sqsubseteq \pi \cdot e', \text{ whenever } \pi \in S_A.
\]

**Definition 3.22.** An invariant lattice is an invariant set \((L, \cdot)\) together with an equivariant lattice order \(\sqsubseteq\) on \(L\).

From the general theory of lattices, we know that if \(\sqsubseteq\) is a lattice order on \(L\) we can define two binary operations called meet and join:

- \(\wedge : L \times L \to L, (x, y) \triangleright z\), where \(z = \inf\{x, y\}\)
- \(\vee : L \times L \to L, (x, y) \triangleright z\), where \(z = \sup\{x, y\}\)

such that \((L, \wedge, \vee)\) is a lattice (which means \(\wedge\) and \(\vee\) satisfy the properties of commutativity, associativity and absorption). We prove that these binary operations make sense in FSM.

**Proposition 3.13.** Let \((L, \sqsubseteq, \cdot)\) be an invariant lattice. Then the operators meet and join are equivariant functions on \(L \times L\).

**Proof.** According to Subsection 2.4.2, \(L \times L\) is an invariant set with the \(S_A\)-action \(* : S_A \times (L \times L) \to (L \times L)\) defined by \(\pi \cdot (x, y) = (\pi \cdot x, \pi \cdot y)\) for all \(\pi \in S_A\) and all \(x, y \in L\). According to Corollary 2.3, we have to prove that \(\pi \cdot (x \wedge y) = \pi \cdot x \wedge \pi \cdot y\) and \(\pi \cdot (x \vee y) = \pi \cdot x \vee \pi \cdot y\) for all \(\pi \in S_A\) and all \(x, y \in L\). We prove one of these assertions; the other one is similar. Let \(x, y \in L\) and \(\pi \in S_A\). Let \(c = x \wedge y\). Then \(c \sqsubseteq x\) and \(c \sqsubseteq y\). Since \(\sqsubseteq\) is equivariant, we have \(\pi \cdot c \sqsubseteq \pi \cdot x\) and \(\pi \cdot c \sqsubseteq \pi \cdot y\). Let \(d \in L\) such that \(d \sqsubseteq \pi \cdot x\) and \(d \sqsubseteq \pi \cdot y\). Then \(\pi^{-1} \cdot d \sqsubseteq x\) and \(\pi^{-1} \cdot d \sqsubseteq y\). Since \(c = \inf\{x, y\}\), we have \(\pi^{-1} \cdot d \sqsubseteq c\). Since \(\sqsubseteq\) is equivariant, we obtain \(d \sqsubseteq \pi \cdot c\). Therefore, \(\pi \cdot c = \inf\{\pi \cdot x, \pi \cdot y\} = (\pi \cdot x) \wedge (\pi \cdot y)\). \(\square\)

**Definition 3.23.** An invariant complete lattice is an invariant poset \((L, \sqsubseteq, \cdot)\) such that every finitely supported subset \(X \subseteq L\) has a least upper bound with respect to the order relation \(\sqsubseteq\). The least upper bound of \(X\) is denoted by \(\sqcup X\).
Theorem 3.32. Let \((L, \sqsubseteq, \cdot)\) be an invariant complete lattice. Then every finitely-supported subset \(X \subseteq L\) has a greatest lower bound with respect to the order relation \(\sqsubseteq\). The greatest lower bound of \(X\) is denoted by \(\sqcap X\).

Proof. Let \(X\) be a finitely supported subset of \(L\) in the sense of Definition 2.6. Let \(D = \cap \{\downarrow x \mid x \in X\}\), where by \(\downarrow x\) we denote the set \(\{y \in L \mid y \sqsubseteq x\}\). Informally, \(D\) is the set of lower bounds of \(X\) with respect to the order relation \(\sqsubseteq\). If \(X\) is empty, we take \(D = L\). First we show that \(D\) is finitely supported in the sense of Definition 2.6. If we prove this, \(D\) will have a least upper bound (denoted by \(\sqcup D\)) according to Definition 3.32. We know that \(X\) has a finite support \(\text{supp}(X)\), and we show that \(\text{supp}(X)\) supports \(D\). Let \(\pi\) be a permutation that fixes \(\text{supp}(X)\) pointwise, i.e. \(\pi \in \text{Fix}(\text{supp}(X))\). Let \(d \in D\) be arbitrarily chosen; then \(d \sqsubseteq x\) for all \(x \in X\). We claim that \(\pi \cdot d \in D\), which is the same as saying that \(\pi \cdot d\) is a lower bound of \(X\). Indeed, let \(y \in X\) be an arbitrary element of \(X\). Since \(\pi \in \text{Fix}(\text{supp}(X))\) and \(\text{supp}(X)\) supports \(X\) in the sense of Definition 2.6 (cf. Theorem 2.4), we get \(\pi \star X = X\) (where the \(S_A\)-action \(\star\) on \(\wp(L)\) is defined as in Subsection 2.4.1). This means that for our \(y \in X\) there is an \(x \in X\) such that \(\pi \cdot x = y\). However, \(d \sqsubseteq x\), and because \(\pi\) is equivariant we also have \(\pi \cdot d \sqsubseteq \pi \cdot x = y\). Hence \(\pi \cdot d \in D\). Since \(d\) is chosen arbitrarily from \(D\), we can say that \(\pi \star D \subseteq D\) whenever \(\pi \in \text{Fix}(\text{supp}(X))\) (1).

We have two methods of proving that \(\pi \star D = D\) for \(\pi \in \text{Fix}(\text{supp}(X))\). First we remark that \(\pi \in \text{Fix}(\text{supp}(X))\) iff \(\pi^{-1} \in \text{Fix}(\text{supp}(X))\). According to (1), we get \(\pi^{-1} \star D \subseteq D\), which means \(\pi \star (\pi^{-1} \star D) \subseteq \pi \star D\), and \(D \subseteq \pi \star D\). Another method of proving that \(\pi \star D = D\) is to use a proof by contradiction. Let us suppose that there is \(\pi \in \text{Fix}(\text{supp}(X))\) such that \(\pi \star D \subseteq D\). By induction, we get \(\pi^n \star D \subseteq D\) for all \(n \geq 1\). However, \(\pi\) is a finitary permutation, and so there is \(k \in \mathbb{N}\) such that \(\pi^k = \text{Id}\). We obtain \(D \subseteq D\), a contradiction. It follows that \(\pi \star D = D\) whenever \(\pi \in \text{Fix}(\text{supp}(X))\), and hence \(\text{supp}(X)\) supports \(D\) according to Definition 2.3. Thus, there exists \(\sqcup D\).

We prove now that \(\sqcup D\) is the greatest lower bound of \(X\). If \(x \in X\), then \(x\) is an upper bound of \(D\), and so \(\sqcup D \sqsubseteq x\). Since \(x\) was chosen arbitrarily from \(X\), we have \(\sqcup D \in D\). Since \(\sqcup D\) is maximal between the lower bounds of \(X\) and it is a lower bound of \(X\), then \(\sqcup D = \sqcap X\), where \(\sqcap X\) represents the greatest lower bound of \(X\).

\(\square\)

Proposition 3.14. Let \((L, \sqsubseteq, \cdot)\) be an invariant complete lattice and \(X\) a finitely supported subset of \(L\). Then \(\pi \cdot \sqcup X = \sqcup (\pi \star X)\) for all \(\pi \in S_A\), where \(\star\) is the \(S_A\)-action on the powerset of \(L\). Analogously, \(\pi \cdot \sqcap X = \sqcap (\pi \star X)\) for all \(\pi \in S_A\).

Proof. Let \(X\) be a finitely supported subset of \(L\). Since \(L\) is an invariant complete lattice, \(\sqcup X\) exists. According to Proposition 2.1, we have that \(\pi \star X\) is finitely supported, and there exists \(\sqcup (\pi \star X)\). Let \(x \in X\). We have \(x \sqsubseteq \sqcup X\). Since \(\sqsubseteq\) is equivariant, we have \(\pi \cdot x \sqsubseteq \pi \cdot \sqcup X\) for all \(\pi \in S_A\). Therefore, \(\sqcup (\sigma \star Y) \subseteq \sigma \cdot \sqcup Y\) for all \(\sigma \in S_A\) and all finitely supported subsets \(Y\) of \(L\) (1). Now, fix some \(\pi \in S_A\) and \(X \in \wp_{\mathcal{B}}(L)\). According to (1), we have \(\sqcup (\pi \star X) \subseteq \pi \cdot \sqcup X\). We can also apply (1) for \(\pi^{-1}\) and \(\pi \star X\), and we obtain \(\sqcup X \subseteq \pi^{-1} \cdot \sqcup (\pi \star X)\). Since \(\sqsubseteq\) is equivariant, we obtain \(\pi \cdot \sqcup X \subseteq \sqcup (\pi \star X)\). According to Theorem 3.32, whenever \(X\) is a finitely supported
subset of $L$, there exists $\cap X$. We can provide an analogous proof for the relation $\pi \cdot \cap X = \cap (\pi \star X)$ for all $\pi \in S_A$.

**Theorem 3.33.** Let $(L, \sqsubseteq, \cdot)$ be an invariant complete lattice and $f : L \to L$ a finitely supported monotone function. Then there exist a greatest $e \in L$ such that $f(e) = e$ and a least $e \in L$ such that $f(e) = e$, which are denoted by $\text{gfp}(f)$ and $\text{lfp}(f)$, respectively.

**Proof.** Let $D = \{d \in L | d \sqsubseteq f(d)\}$. First we prove that $D$ is finitely supported in the sense of Definition 2.6. We claim that $\text{supp}(f)$ supports $D$. Let $\pi \in \text{Fix}(\text{supp}(f))$ and $d \in D$ be arbitrarily chosen. Then $d \sqsubseteq f(d)$, and because $\sqsubseteq$ is equivariant we also have $\pi \cdot d \sqsubseteq \pi \cdot f(d)$. Since $\pi \in \text{Fix}(\text{supp}(f))$ and $\text{supp}(f)$ supports $f$, according to Proposition 2.4, we have $\pi \cdot d \sqsubseteq \pi \cdot f(d) = f(\pi \cdot d)$ and hence $\pi \cdot d \in D$. Since $d$ was chosen arbitrarily from $D$, we have $\pi \star D \subseteq D$ whenever $\pi \in \text{Fix}(\text{supp}(f))$ (where $\star$ is the $S_A$-action on $\wp(L)$ defined in Subsection 2.4.1) $\dagger$. As in the last part of the proof of Theorem 3.32, we have two methods of proving that $\pi \star D = D$ for $\pi \in \text{Fix}(\text{supp}(f))$. First we remark that $\pi \in \text{Fix}(\text{supp}(f))$ iff $\pi^{-1} \in \text{Fix}(\text{supp}(f))$. Hence by (†) we get $\pi^{-1} \star D \subseteq D$, which means that $\pi \star (\pi^{-1} \star D) \subseteq \pi \star D$ (because of the definition of $\star$), and finally $D \subseteq \pi \star D$. Another method to prove that $\pi \star D = D$ is to prove this by contradiction. Let us suppose that there exists $\pi \in \text{Fix}(\text{supp}(f))$ such that $\pi \star D \subsetneq D$. By induction, we get $\pi^n \star D \subsetneq D$ for all $n \geq 1$. However, $\pi$ is a finitary permutation, and so there exists $k \in \mathbb{N}$ such that $\pi^k = \text{Id}$. We obtain $D \subsetneq D$, a contradiction. It follows that $\pi \star D = D$ whenever $\pi \in \text{Fix}(\text{supp}(f))$, and hence $\text{supp}(f)$ supports $D$. Since $\text{supp}(f)$ is finite, we have that $\cap D$ exists according to Definition 3.23.

Let $e = \cap D$. Then for each $d \in D$ we have $d \sqsubseteq e$. Since $f$ preserves the order relation, we have $f(d) \sqsubseteq f(e)$. Since $d \in D$, it follows that $d \sqsubseteq f(d) \sqsubseteq f(e)$. Therefore, $d \sqsubseteq f(e)$ for each $d \in D$. According to the definition of a least upper bound, we have that $e \sqsubseteq f(e)$, which means that $e \in D$. However, because $f$ is order preserving, we have $f(x) \in D$ for each $x \in D$. Since $e \in D$, it follows that $f(e) \in D$. Thus, $f(e) \sqsubseteq e$ because $e = \cap D$. Therefore, we get $f(e) = e$. Whenever $e'$ is an element in $L$ such that $f(e') = e'$, it follows that $e' \in D$, and so $e' \sqsubseteq e$. Therefore, $e = \text{gfp}(f)$.

Analogously we can prove that the set $D' = \{d \in L | f(d) \sqsubseteq d\}$ is finitely supported by $\text{supp}(f)$. According to Theorem 3.32, there exists $\cap D'$, a similar calculation shows us that $\cap D'$ satisfies $\cap D' = f(\cap D')$, and $\text{lfp}(f) = \cap D'$.

**Remark 3.6.** According to the proof of Theorem 3.33, we have $\text{gfp}(f) = \cup\{d \in L | d \sqsubseteq f(d)\}$ and $\text{lfp}(f) = \cap\{d \in L | f(d) \sqsubseteq d\}$.

The following result represents the analogue of the classical Tarski theorem [151] for invariant complete lattices.

**Theorem 3.34.** Let $(L, \sqsubseteq, \cdot)$ be an invariant complete lattice and $f : L \to L$ an equivariant monotone function over $L$. Let $P$ be the set of fixed points of $f$. Then $(P, \sqsubseteq, \cdot)$ is an invariant complete lattice.

**Proof.** Since $f$ is equivariant, it follows that for all $\pi \in S_A$ and all $x \in L$ we have $f(\pi \cdot x) = \pi \cdot f(x)$. Whenever $x$ is a fixed point of $f$, we have $f(\pi \cdot x) = \pi \cdot f(x) = \pi \cdot x$,
and so \( \pi \cdot x \) is also a fixed point of \( f \). We proved that the application \( \cdot |_P \) (where \( \cdot |_P \) represents the restriction of the \( S_A \)-action \( \cdot \) to \( P \)) has codomain equal to \( P \). Therefore, the application \( \cdot |_P : S_A \times P \to P \) defined by \( \pi \cdot |_P x = \pi \cdot x \) for all \( \pi \in S_A \) and all \( x \in P \) is an \( S_A \)-action of \( S_A \) on \( P \) (it satisfies the axioms of a group action whenever \( \cdot \) does). Moreover, \( (P, \cdot |_P) \) is an invariant set. According to the \( S_A \)-action \( \cdot |_P \), the support of each element in \( P \) is the same as the support of that element according to the \( S_A \)-action \( \cdot \). It is somehow natural to denote the action \( \cdot |_P \) by \( \cdot \).

Let \( X \) be an arbitrary finitely supported subset in \( P \). We have to prove that \( X \) has a least upper bound in \( P \). We already know that \( X \) has a least upper bound (denoted by \( \sqcup X \)) in \( L \) because \( (L, \sqsubseteq, \cdot) \) is an invariant complete lattice.

Let \( x \in X \) be an arbitrary element. We have that \( x \sqsubseteq \sqcup X \), and so \( f(x) \sqsubseteq f(\sqcup X) \). However, \( X \) contains only fixed points of \( f \), and so \( f(x) = x \) and \( x \subseteq f(\sqcup X) \). According to the definition of a least upper bound, it follows that \( \sqcup X \subseteq f(\sqcup X) \). Now, let \( y \sqsubseteq \sqcup X \). Since \( f \) is a monotone function, we also have \( f(y) \sqsubseteq f(\sqcup X) \). We have already proved that \( \sqcup X \subseteq f(\sqcup X) \), and hence \( f(y) \sqsubseteq \sqcup X \). We get that \( f(y) \sqsubseteq \sqcup X \) whenever \( y \sqsubseteq \sqcup X \).

Let \( D = \{ d \in L \mid f(d) \sqsubseteq d \text{ and } \sqcup X \sqsubseteq d \} \). We can prove that \( \text{supp}(\sqcup X) \) supports \( D \) in the sense of Definition 2.6, and so \( D \) is a finitely supported set. Indeed, \( \text{supp}(\sqcup X) \) exists according to Corollary 2.1 because \( L \) is an invariant set and \( \sqcup X \subseteq L \). Let \( \pi \in \text{Fix}(\text{supp}(\sqcup X)) \), and \( d \in D \) be arbitrarily chosen. Then \( f(d) \sqsubseteq d \). Since \( \sqsubseteq \) is equivariant, we also have \( \pi \cdot f(d) \sqsubseteq \pi \cdot d \). Moreover, by Corollary 2.3, because \( f \) is equivariant, we have \( \pi \cdot f(d) = f(\pi \cdot d) \). Thus, \( f(\pi \cdot d) \sqsubseteq \pi \cdot d \). Since \( d \in D \), we also have \( \sqcup X \sqsubseteq d \). Therefore, \( \pi \cdot \sqcup X \sqsubseteq \pi \cdot d \). However, \( \pi \cdot \sqcup X = \sqcup X \) because \( \pi \in \text{Fix}(\text{supp}(\sqcup X)) \). Finally, we obtain \( \sqcup X \sqsubseteq \pi \cdot d \), and so \( \pi \cdot D \subseteq D \) whenever \( \pi \in \text{Fix}(\text{supp}(\sqcup X)) \) (the \( S_A \)-action on \( \varnothing(L) \) is defined as in Subsection 2.4.1). Since \( \pi \in \text{Fix}(\text{supp}(\sqcup X)) \) iff \( \pi^{-1} \in \text{Fix}(\text{supp}(\sqcup X)) \), it follows that \( \pi^{-1} \cdot D \subseteq D \), from which \( \pi \cdot (\pi^{-1} \cdot D) \subseteq \pi \cdot D \) (because of the definition of \( \cdot \)), and, finally, \( D \subseteq \pi \cdot D \). Thus, \( D \) is finitely supported, and there exists the greatest lower bound of \( D \) denoted by \( \sqcap D \) (Theorem 3.32).

Let \( e = \sqcap D \). Then for each \( d \in D \), we have \( e \sqsubseteq d \). Since \( f \) preserves the order relation, we have also \( f(e) \sqsubseteq f(d) \). Since \( d \in D \), it follows that \( f(e) \sqsubseteq f(d) \sqsubseteq d \). Therefore, \( f(e) \sqsubseteq d \) for each \( d \in D \). According to the definition of a greatest lower bound, we have that \( f(e) \sqsubseteq e \). Also, \( d \sqsupseteq \sqcup X \) for each \( d \in D \) implies \( \sqcap D \sqsupseteq \sqcup X \), which means \( e \in D \). However, because \( f \) is order preserving and because \( f(y) \sqsupseteq \sqcup X \) whenever \( y \sqsupseteq \sqcup X \), we have that \( f(x) \in D \) for each \( x \in D \). Since \( e \in D \), it follows that \( f(e) \in D \), and so \( e \sqsubseteq f(e) \) because \( e = \sqcap D \).

We proved that \( e \) is a fixed point of \( f \) such that \( \sqcup X \subseteq e \). Therefore, \( e \in P \) is an upper bound for \( X \). What remains to be proved is that \( e \) is the least upper bound for \( X \) in the system \( (P, \sqsubseteq) \). Let \( e' \in P \) be another upper bound for \( X \). Then \( \sqcup X \subseteq e' \) (since \( \sqcup X \) is the least upper bound for \( X \) in \( L \) and, clearly, \( e' \) is an upper bound for \( X \) in \( L \)); it follows that \( e' \in D \). Since \( e = \sqcap D \), we get \( e \sqsubseteq e' \). This means \( e = \sqcup X \) in \( (P, \sqsubseteq) \).

**Remark 3.7.** The previous theorem suggests that it is a bit tricky to formalize a certain ZF result in FSM. Thus, when translating a ZF result into FSM we have to be careful when choosing either “finitely supported” or “equivariant” in the statement.
of the desired FSM result. For example, the FSM weak form of the Tarski theorem (i.e. Theorem 3.33) holds for all finitely supported, monotone functions defined on an invariant complete lattice, whilst the FSM strong form of the Tarski theorem (i.e. Theorem 3.34) holds only for those equivariant monotone functions defined on an invariant complete lattice. Actually, Theorem 3.34 works as expected. This is because the set of fixed points of \( f \) is \( S \)-supported whenever \( f \) is \( S \)-supported, and so the set of fixed points of \( f \) is empty supported (invariant) only if \( f \) is equivariant. However, when translating a ZF result into FSM, one cannot just insert “equivariant” or “finitely supported” without a preliminary analysis about which of the previous terms is adequate for the desired FSM result.

**Definition 3.24.** An invariant lattice \((L, \sqsubseteq, \cdot)\) is called an invariant Boolean lattice if the following conditions are satisfied:

- \( L \) is a distributive lattice.
- \( L \) is bounded by a unique least element denoted by 0 and a unique greatest element denoted by 1.
- \( L \) is uniquely complemented, that is, for each element \( x \in L \) there exists a unique element \( x' \in L \) such that \( x \land x' = 0 \) and \( x \lor x' = 1 \).

**Proposition 3.15.** Let \((L, \sqsubseteq, \cdot)\) be an invariant Boolean lattice. Then \((\pi \cdot x)' = \pi \cdot x'\) for each \( \pi \in S_A \) and each \( x \in L \). Moreover, \( \text{supp}(x') = \text{supp}(x) \).

**Proof.** Since \( \sqsubseteq \) is equivariant and 0, 1 are unique, we have \( \pi \cdot 0 = 0 \) and \( \pi \cdot 1 = 1 \). Let \( x \in L \). According to Proposition 3.13, we have \((\pi \cdot x) \land (\pi \cdot x') = \pi \cdot (x \land x') = \pi \cdot 0 = 0\) and \((\pi \cdot x) \lor (\pi \cdot x') = \pi \cdot (x \lor x') = \pi \cdot 1 = 1\). Therefore, since the complement of each element in \( L \) is unique, we have \((\pi \cdot x)' = \pi \cdot x'\), and \( \text{supp}(x') = \text{supp}(x) \). \( \square \)

The next property holds directly from the general theory of lattices without requiring the validity of a certain distributivity property on infinite families of elements.

**Proposition 3.16.** Let \((L, \sqsubseteq, \cdot)\) be an invariant complete Boolean lattice and \( S \) a finitely supported subset of \( L \). Then \((\sqcap S)' = (\sqcup S)'\). Similarly, \((\sqcup S)' = (\sqcap S)'\)

**Proof.** According to Proposition 3.15, whenever \( S \) is a finitely supported subset of \( L \) we have that \( S' = \{ x' \mid x \in S \} \) is also a finitely supported subset of \( L \) with the same support as \( S \). Therefore, the statement of the property makes sense. We prove that \((\sqcap S) \land (\sqcup S)' = 0\). Let \( d \in L \) such that \( d \sqsubseteq \sqcap S \) and \( d \sqsubseteq \sqcup S' \). Then \( d \sqsubseteq s, \forall s \in S \), and so \( s' \sqsubseteq d', \forall s \in S \). Therefore, \( \sqcup S' \sqsubseteq d' \). Since \( d \sqsubseteq \sqcup S' \), we obtain \( d \sqsubseteq d' \), that is, \( d = 0 \). Similarly, we prove that \((\sqcap S)' \lor (\sqcup S)' = 1\). Let \( e \in L \) such that \( \sqcap S' \sqsubseteq e \) and \( \sqcap S \sqsubseteq e \). Then \( s' \sqsubseteq e, \forall s \in S \), and so \( e' \sqsubseteq s, \forall s \in S \). Therefore, \( e' \sqsubseteq \sqcap S \). Since \( \sqcap S \sqsubseteq e \) we obtain \( e' \sqsubseteq e \), that is, \( e = 1 \). \( \square \)

**Definition 3.25.** Let \((P, \sqsubseteq_P, \cdot_P)\) and \((Q, \sqsubseteq_Q, \cdot_Q)\) be two invariant posets. Let \( f: P \to Q \).

- \( f \) is an invariant join-morphism if \( f \) is equivariant, and whenever \( a, b \in P \) and \( a \lor b \) exists in \( P \), then \( f(a) \lor f(b) \) exists in \( Q \) and \( f(a \lor b) = f(a) \lor f(b) \).
- \( f \) is an invariant complete join-morphism if \( f \) is equivariant, and whenever \( X \subseteq P \) is finitely supported and \( \sqcup X \) exists in \( P \), then \( f(X) \) is finitely supported, \( \sqcup f(X) \) exists in \( Q \) and \( f(\sqcup X) = \sqcup f(X) \).

Invert (complete) meet-morphisms are defined dually.
3.3 Order Theory in Finitely Supported Mathematics

3.3.2 Galois Connections

Galois connections, which appear at a large scale in theoretical computer science, are pairs of maps which enable us to move back and forth between two different structures. After an element is mapped to the other structure and back, a certain stability is reached in such a way that further mappings give the same results. Furthermore, the image sets of the maps forming the Galois connection are isomorphic. The ZF concept of Galois connection can be extended to FSM in the following way.

Definition 3.26. Let \((P, \sqsubseteq_P, \cdot_P)\) and \((Q, \sqsubseteq_Q, \cdot_Q)\) be two invariant posets, and \(f: P \rightarrow Q, g: Q \rightarrow P\) two functions. The pair \((f, g)\) is an invariant Galois connection between \(P\) and \(Q\) if and only if the following conditions are satisfied:

- \(f\) and \(g\) are equivariant functions.
- for all \(p \in P\) and \(q \in Q\) we have that \(f(p) \sqsubseteq_Q q\) if and only if \(p \sqsubseteq_P g(q)\).

The map \(g\) is called the invariant adjoint and \(f\) is called the invariant co-adjoint. Moreover, if \((f, g)\) is an invariant Galois connection, then we say that \(f\) has an invariant adjoint \(g\), and \(g\) has an invariant co-adjoint \(f\).

The following FSM characterization of Galois connections can be directly proved as in the ZF framework (see Lemma 79 from [94]).

Proposition 3.17. Let \((P, \sqsubseteq_P, \cdot_P)\) and \((Q, \sqsubseteq_Q, \cdot_Q)\) be two invariant posets, and \(f: P \rightarrow Q, g: Q \rightarrow P\) two functions. The pair \((f, g)\) is an invariant Galois connection between \(P\) and \(Q\) if and only if the following conditions are satisfied:

- \(f\) and \(g\) are equivariant monotone functions.
- for all \(p \in P\) and \(q \in Q\) we have that \(f(g(q)) \sqsubseteq_Q q\) and \(p \sqsubseteq_P g(f(p))\).

Proposition 3.18. Let \((P, \sqsubseteq_P, \cdot_P)\) and \((Q, \sqsubseteq_Q, \cdot_Q)\) be two invariant posets and \((f, g)\) an invariant Galois connection between \(P\) and \(Q\). The map \(f\) is an invariant complete join-morphism and \(g\) is an invariant complete meet-morphism.

Proof. We prove only that \(f\) is an invariant complete join-morphism (the other part can be proved in a similar way). Let \(X \subseteq P\) be finitely supported such that \(\sqcup X\) exists in \(P\). Since there exists a finite set \(S\) supporting \(X\), we obtain that the set \(f(X) = \{f(p) \mid p \in X\}\) is also supported by \(S\). Indeed, because \(f\) is equivariant, for each \(p \in X\) and each \(\pi \in S_A\) we have \(\pi \cdot f(p) = f(\pi \cdot p)\). Let \(\pi \in \text{Fix}(S)\) and \(p \in X\). Since \(\pi\) fixes \(S\) pointwise and \(S\) supports \(X\), we have \(\pi \cdot p \in X\). Therefore, \(\pi \cdot f(p) \in f(X)\) for all \(\pi \in \text{Fix}(S)\) and \(x \in X\). This means that \(S\) supports \(f(X)\). The rest of the proof is standard and does not involve FSM results - see Proposition 82(e) from [94].

Proposition 3.19. Let \((L, \sqsubseteq_L, \cdot_L)\) and \((K, \sqsubseteq_K, \cdot_K)\) be two invariant complete lattices.

- An equivariant function \(f: L \rightarrow K\) has an invariant adjoint if and only if \(f\) is an invariant complete join-morphism.
- An equivariant function \(g: K \rightarrow L\) has an invariant co-adjoint if and only if \(g\) is an invariant complete meet-morphism.
Proof. We prove the first assertion (the other is similar). According to Proposition 3.18, whenever \( f \) has an invariant adjoint we have that \( f \) is an invariant complete join-morphism. Conversely, let \( f \) be an invariant complete join-morphism. For each \( k \in K \) we consider the set \( X_k = \{ l \in L \mid f(l) \sqsubseteq k \} \). We claim that \( \text{supp}(k) \) supports \( X_k \) in the sense of Definition 2.6. Let \( \pi \in \text{Fix}(\text{supp}(k)) \), and \( l \in X_k \) be arbitrarily chosen. Then \( f(l) \sqsubseteq K k \). Since \( \sqsubseteq \) is equivariant, we also have \( \pi \cdot K f(l) \sqsubseteq K \pi \cdot K k \). Since \( f \) is equivariant and \( \pi \) fixes \( \text{supp}(k) \) pointwise, we have that \( f(\pi \cdot L l) = \pi \cdot K f(l) \sqsubseteq K \pi \cdot k = k \). Therefore, \( \pi \star X_k \subseteq X_k \) whenever \( \pi \in \text{Fix}(\text{supp}(k)) \) (the \( S_A \)-action \( \star \) on \( \rho(L) \) is defined as in Section 2.4.1). Since \( \pi \in \text{Fix}(\text{supp}(k)) \) iff \( \pi^{-1} \in \text{Fix}(\text{supp}(k)) \), it follows that \( \pi^{-1} \star X_k \subseteq X_k \), from which \( \pi \star (\pi^{-1} \star X_k) \subseteq \pi \star X_k \) (according to the definition of \( \star \)), and finally \( X_k \subseteq \pi \star X_k \). Since \( X_k \) is finitely supported, there exists its supremum \( \sqcup X_k \). We define \( g : K \to L \) by \( g(k) = \sqcup X_k \) for each \( k \in K \). Since \( f \) and \( \sqsubseteq K \) are equivariant, we have for each \( \pi \in S_A \) that \( f(\pi^{-1} \cdot L l) \sqsubseteq K k \iff f(\pi^{-1} \cdot L f(l)) \sqsubseteq K \pi \cdot K k \). Therefore, \( \{ l \in L \mid f(l) \sqsubseteq K \pi \cdot K k \} = \{ l \in L \mid f(\pi^{-1} \cdot L l) \sqsubseteq K k \} = \{ \pi \cdot L l \in L \mid f(l) \sqsubseteq K k \} = \pi \star \{ l \in L \mid f(l) \sqsubseteq K k \} \).

Now, fix \( \pi \in S_A \) and \( k \in K \). We have \( g(\pi \cdot K k) = \sqcup \{ l \in L \mid f(l) \sqsubseteq K \pi \cdot K k \} \). According to Proposition 3.14, we have \( \pi \cdot L g(k) = \pi \cdot L \sqcup \{ l \in L \mid f(l) \sqsubseteq K k \} = \sqcup (\pi \star \{ l \in L \mid f(l) \sqsubseteq K k \}) \). Therefore, \( g \) is equivariant. We have to check the rest of the conditions in Definition 3.26. Let us consider \( l \in L \) and \( k \in K \). If \( f(l) \sqsubseteq K k \), then \( l \in X_k \), which means \( l \sqsubseteq L \sqcup X_k = g(k) \). Conversely, assume \( l \sqsubseteq L g(k) = \sqcup \{ l \in L \mid f(l) \sqsubseteq K k \} \). Since \( X_k = \{ l \in L \mid f(l) \sqsubseteq K k \} \) is supported by \( \text{supp}(k) \) and \( f \) is equivariant, according to Corollary 2.3, we obtain that \( \{ f(l) \in L \mid f(l) \sqsubseteq K k \} = f(X_k) \) is also supported by \( \text{supp}(k) \) (see also the proof of Proposition 3.18). Therefore, there exists \( \sqcup \{ f(l) \in L \mid f(l) \sqsubseteq K k \} \). Since \( f \) is a monotone invariant complete join-morphism, we have \( f(l) \sqsubseteq K \sqcup \{ f(l) \in L \mid f(l) \sqsubseteq K k \} \sqsubseteq K k \).

In the following we study the invariant conjugate functions on an invariant Boolean lattice, and we establish a connection between the invariant Galois connections and invariant conjugate function pairs.

**Definition 3.27.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant Boolean lattice, and \( f, g : L \to L \) two functions. We say that \( g \) is an invariant conjugate of \( f \) if the following conditions are satisfied:

- \( f \) and \( g \) are equivariant.
- for all \( x, y \in L \) we have \( x \sqcap f(y) = 0 \) if and only if \( y \sqcap g(x) = 0 \).

Clearly, if \( g \) is an invariant conjugate of \( f \), then \( f \) is also an invariant conjugate of \( g \). If a map \( f \) is the invariant conjugate of itself, we say that \( f \) is an invariant self-conjugate. Note that each map has at most one conjugate [94]. Hence every equivariant function has at most one invariant conjugate.

**Proposition 3.20.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete Boolean lattice, and \( f : L \to L \) a function on \( L \). Then \( f \) has an invariant conjugate if and only if \( f \) is an invariant complete join-morphism.

**Proof.** Let \( f : L \to L \) be a function on \( L \) which has an invariant conjugate. A simple calculation which does not involve FSM results show us that \( f \) is monotone. Let
3.3 Order Theory in Finitely Supported Mathematics

Let \( X \subseteq L \) be a finitely supported subset. According to the proof of Proposition 3.18, because \( f \) is equivariant, \( f(X) \) is also finitely supported and \( \sqcup X \) \( \sqcup f(X) \) exist. The relation \( f(\sqcup X) = \sqcup f(X) \) follows directly, using the technical details presented in Proposition 86 from [94].

Conversely, let us suppose that \( f \) is an invariant complete join-morphism. For each \( y \in L \) we consider the set \( X_y = \{ x \mid f(x) \subseteq y' \} \). We claim that \( \text{supp}(y') = \text{supp}(y) \) supports \( X_y \) in the sense of Definition 2.6. Let \( \pi \in \text{Fix}(\text{supp}(y')) \), and \( x \in X_y \) be arbitrarily chosen. Then \( f(x) \subseteq y' \). Since \( \subseteq \) is equivariant, we also have \( \pi \cdot f(x) \subseteq \pi \cdot y' \). Therefore, \( \pi \cdot X_y \subseteq X_y \) whenever \( \pi \in \text{Fix}(\text{supp}(y')) \) (the \( S_A \)-action \( \ast \) on \( \wp(L) \) is defined as in Section 2.4.1). Since \( \pi \in \text{Fix}(\text{supp}(y')) \), \( \pi^{-1} \cdot X_y \subseteq X_y \), from which \( X_y \subseteq \pi \ast X_y \).

Since \( X_y \) is finitely supported, there exists its supremum \( \sqcup X_y \). We define \( g : L \rightarrow L \) by \( g(y) = (\sqcup X_y)' \) for each \( y \in L \). Since \( f \) and \( x \) are equivariant, we have for each \( \pi \in S_A \) that \( f((\pi^{-1} \cdot x) \subseteq y') \Leftrightarrow (\pi^{-1} \cdot f(x) \subseteq y') \Leftrightarrow (\pi \cdot f(x) \subseteq (\pi \cdot y') \). Therefore, \( \{ x \in L \mid f(x) \subseteq (\pi \cdot y') \} = \{ \pi \cdot x \in L \mid f(x) \subseteq y' \} = \pi \ast \{ x \in L \mid f(x) \subseteq y' \} \). Now, fix \( \pi \in S_A \) and \( y \in L \). According to Proposition 3.15, we have \( g(\pi \cdot y) = (\sqcup \{ x \in L \mid f(x) \subseteq (\pi \cdot y') \})' = (\sqcup \{ x \in L \mid f(x) \subseteq \pi \cdot y' \})' \). According to Proposition 3.15 and Proposition 3.14, we have \( \pi \cdot g(y) = \pi \cdot (\sqcup \{ x \in L \mid f(x) \subseteq y' \})' = (\sqcup \{ x \in L \mid f(x) \subseteq (\pi \cdot y') \})' \). Therefore, \( g \) is equivariant.

According to the definition of \( g \) and Proposition 3.16, we can say that \( g(y) = \sqcup \{ x' \mid f(x) \land y = 0 \} \). According to Proposition 3.15 and Proposition 3.13, and because \( f \) is equivariant, we have that \( \{ x' \mid f(x) \land y = 0 \} \) is supported by \( \text{supp}(y) \) for each \( y \in L \). Therefore, its infimum exists according to Theorem 3.32. Let us consider \( x, y \in L \). If \( f(x) \land y = 0 \), then \( g(y) \subseteq x' \), that is, \( g(y) \land x = 0 \). On the other hand, because \( X_y \) is finitely supported we have that \( f(X_y) \) is also finitely supported. Therefore, \( f(g(y)) = f(\sqcup \{ x \mid f(x) \subseteq y' \}) = \sqcup \{ f(x) \mid f(x) \subseteq y' \} \subseteq y' \). If \( x \) and \( y \) are such that \( g(y) \land x = 0 \), then \( x \subseteq g(y)' \). Thus, \( f(x) \subseteq f(g(y))', y' \), which means \( f(x) \land y = 0 \).

**Definition 3.28.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete Boolean lattice, and \( f, g : L \rightarrow L \) two functions. We say that \( g \) is the **invariant dual** of \( f \) if the following conditions are satisfied:

- \( f \) and \( g \) are equivariant.
- for any \( x \in L \) we have \( f(x') = g(x)' \).

For any equivariant function \( f \) on an invariant complete Boolean lattice \( (L, \sqsubseteq, \cdot) \), there exists a function \( g : L \rightarrow L \) defined by \( g(x) = f(x') \) for all \( x \in L \). According to Proposition 3.15, we have \( g(\pi \cdot x) = f((\pi \cdot x)')' = f(\pi \cdot x)' \). On the other hand, because \( f \) is equivariant, we obtain \( \pi \cdot g(x) = \pi \cdot f(x)' = (\pi \cdot f(x')')' = f(\pi \cdot x')' \).

Therefore, \( g \) is equivariant, and \( g \) is the invariant dual of \( f \). The invariant dual of \( f \) is denoted by \( f^0 \).

**Proposition 3.21.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete Boolean lattice. A function \( f : L \rightarrow L \) is an invariant complete join-morphism if and only if \( f^0 \) is an invariant complete meet-morphism.
Then, according to Proposition 3.16, we have $f$ is an invariant complete Boolean lattice and $f : L \to L$ is an invariant complete join-morphism, then $f$ has at most one invariant adjoint because each invariant adjoint of $f$ has to satisfy the second condition in Definition 3.26 which is in fact the ZF condition of being a ZF adjoint of $f$. Moreover, according to Proposition 3.19, if $L$ is an invariant complete Boolean lattice and $f : L \to L$ is an invariant complete join-morphism, then $f$ has at least one invariant adjoint. Therefore, if $L$ is an invariant complete Boolean lattice and $f : L \to L$ is an invariant complete join-morphism, then $f$ has a unique invariant adjoint which can be defined in the following way.

**Theorem 3.35.** Let $(L, \sqsubseteq, \cdot)$ be an invariant complete Boolean lattice.

- For any invariant complete join-morphism $f : L \to L$, its invariant adjoint is the invariant dual of the invariant conjugate of $f$.
- For any invariant complete meet-morphism $g : L \to L$, its invariant co-adjoint is the invariant conjugate of the invariant dual of $g$.

**Proof.** Let $f : L \to L$ be an invariant complete join-morphism. According to Proposition 3.19, it has an invariant adjoint $f_{\text{adj}} : L \to L$ defined by $f_{\text{adj}}(x) = \sqcup\{y \mid f(y) \sqsubseteq x\}$ for all $x \in L$. According to Proposition 3.20 and Proposition 3.16, the invariant conjugate of $f$ is the function $g : L \to L$ defined by $g(x) = (\sqcup\{y \mid f(y) \sqsubseteq x'\})' = \sqcap\{y' \mid f(y') \sqsubseteq x\}$ for all $x \in L$. The invariant dual of $g$ is $g_{\delta} : L \to L$ defined by $g_{\delta}(x) = g(x')'$ for all $x \in L$. A simple calculation which does not involve specific FSM results shows us that $g_{\delta} = f_{\text{adj}}$. The second part of the theorem can be proved analogously.

**Theorem 3.36.** Let $(L, \sqsubseteq, \cdot)$ be an invariant complete Boolean lattice and $(f, f_{\text{adj}})$ an invariant Galois connection on $L$. If $f$ is invariant self-conjugate and $x \sqsubseteq f(x)$ for all $x \in L$, then the set of all fixed points of $f$ forms an invariant complete Boolean sublattice of $L$.

**Proof.** We denote by $P$ the set of all fixed points of $f$. Since $f$ is equivariant, by Theorem 3.34, we know that $(P, \cdot)$ is an invariant set and $(P, \sqsubseteq, \cdot)$ is an invariant complete lattice. Clearly, $P$ is a sublattice of $L$. According to Proposition 3.35, since $f$ is invariant self-conjugate, its invariant adjoint coincides with its invariant dual. Therefore, $f_{\text{adj}} = f_{\delta}$. If $x \in P$, then $f_{\delta}(x') = f(x)' = x'$. Moreover, by Proposition 3.17, we have $x' \sqsupseteq f(f_{\delta}(x')) = f(x')$. However, $x' \sqsubseteq f(x')$, that is, $x' \in P$. 

\[\square\]
3.3 Order Theory in Finitely Supported Mathematics

3.3.3 Rough Set Approximations

Rough set theory represents a mathematical tool to manage the notions of vagueness and uncertainty, and it is considered one of the first non-statistical approaches in data analysis. This approach is very important in artificial intelligence and cognitive sciences, especially in the areas of data mining, decision analysis, expert systems, machine learning, inductive reasoning and pattern recognition [119]. Applications of rough set theory can also be found in medicine, engineering, economics, molecular biology and social sciences. For a complete list of applications of rough sets, see Section 1.11 in [99].

The central idea of the rough set theory is to approximate a set by using a pair of sets called the lower and the upper approximation of this set. The rough set approximations are defined by means of indiscernibility relations which are equivalences interpreted so that two objects are equivalent if we cannot distinguish them by their properties. This means that our ability to discern objects is limited, and so we cannot observe individual objects, but only their equivalence classes. The lower approximation is characterized by objects that definitely belong to a subset of interest, and the upper approximation is characterized by objects that possibly belong to a subset of interest. Precisely, the lower and the upper approximations of a set are the interior and, respectively, the closure of this set in the topology generated by an indiscernibility relation.

The rough set concept overlaps with some other mathematical tools developed to deal with imprecision and vagueness, in particular with the theory of evidence [138] and fuzzy set theory [161]. A relationship between the rough set theory and the theory of evidence was established in [80, 139, 143], and some comparisons between rough sets and fuzzy sets appear in [63, 64, 120]. However, rough set theory and fuzzy set theory are independent approaches to imperfect knowledge. One of the main advantages of rough set theory is that it does not need any preliminary or additional information about data, such as basic probability assignment in the theory of evidence, grade of membership or the value of possibility in fuzzy set theory, or probability distribution in statistics.

Rough set approximations were defined and studied in [118] in the ZF framework. Let us consider a non-empty set $U$, and an equivalence relation $\epsilon$ on $U$. The set of all $\epsilon$-equivalence classes of elements in $U$ is denoted by $U/\epsilon$. Any element from the factor set $U/\epsilon$ can be viewed as a set of similar objects characterized by the same available information about them [121]. Any set formed from a union of $\epsilon$-equivalence classes of elements in $U$ is called a definable, or crisp set. Otherwise, it is called a rough (vague) set. Any subset $X \subseteq U$ is approximated by two sets called the lower and upper $\epsilon$-approximations of $X$. The lower $\epsilon$-approximation of $X$ is the union of all the elements from $U/\epsilon$ which are subsets of $X$, whilst the upper $\epsilon$-approximation of $X$ is the union of all the elements from $U/\epsilon$ which have a non-empty intersection with $X$.

Our goal is to formalize the concept of Pawlak approximations in the framework of invariant sets. So, we define and study the FSM approximations of finitely supported subsets of some possibly infinite invariant sets; these approximations are de-
fined according to a certain equivariant equivalence (indiscernibility) relation. The results in this subsection represent our original research published in [22].

Definition 3.29. Let \((U, \cdot)\) be an invariant set and \(\varepsilon\) an equivariant equivalence relation on \(U\). We denote by \([x]_\varepsilon\) the equivalence class of an element \(x \in U\), i.e. \([x]_\varepsilon = \{ y | y \varepsilon x \}\). An invariant Pawlak’s approximation pair of \(\varepsilon\) is a pair of functions \((\underline{\varepsilon}, \overline{\varepsilon})\) defined in the following way:

- \(\underline{\varepsilon} : \wp_f \rightarrow \wp_U, \underline{\varepsilon}(X) = \{ x \in U \mid [x]_\varepsilon \subseteq X \}\)
- \(\overline{\varepsilon} : \wp_f \rightarrow \wp_U, \overline{\varepsilon}(X) = \{ x \in U \mid [x]_\varepsilon \cap X \neq \emptyset \}\).

Proposition 3.32. Let \((U, \cdot)\) be an invariant set and \(\varepsilon\) an equivariant equivalence relation on \(U\). The functions \(\underline{\varepsilon}\) and \(\overline{\varepsilon}\) are well defined and equivariant.

Proof. According to Subsection 2.4.1, we know that \(\wp_f (U)\) is an invariant set with the \(S_A\)-action * : \(S_A \times \wp_f (U) \rightarrow \wp_f (U)\) defined by \(\pi \ast X := \{ \pi \cdot x \mid x \in X \}\) for all permutations \(\pi \in S_A\) and all finitely supported subsets \(X\) of \(U\). Let \(\pi \in S_A\) and \(x \in U\). We have \(\pi \ast [x]_\varepsilon = \{ \pi \cdot y \mid y \varepsilon x \}\) and \([\pi \cdot x]_\varepsilon = \{ z \mid z \varepsilon (\pi \cdot x) \}\). Let \(t \in [\pi \cdot x]_\varepsilon\). Then \(t = \pi \cdot y\), for some \(y \in \pi \cdot x\). Since \(\varepsilon\) is equivariant, we have \((\pi \cdot y) \varepsilon (\pi \cdot x)\), and so \(t \in [\pi \cdot x]_\varepsilon\). Conversely, if \(t \in [\pi \cdot x]_\varepsilon\), then \(t \varepsilon (\pi \cdot x)\). Since \(\varepsilon\) is equivariant, we also have \((\pi^{-1} \cdot t) \varepsilon x\), that is, \(t \in [\pi \cdot x]_\varepsilon\). Therefore, \(\pi \ast [x]_\varepsilon = [\pi \cdot x]_\varepsilon\).

In order to prove that \(\underline{\varepsilon}\) and \(\overline{\varepsilon}\) are well defined, we have to prove that the sets \(C_X = \{ x \in U \mid [x]_\varepsilon \subseteq X \}\) and \(D_X = \{ x \in U \mid [x]_\varepsilon \cap X \neq \emptyset \}\) are finitely supported for each \(X \in \wp_f (U)\). Fix some \(X \in \wp_f (U)\). We claim that \(C_X\) and \(D_X\) are supported by \(supp(X)\). Let \(\pi \in Fix(supp(X))\). This means \(\pi \ast X = X\). Let \(c \in C_X\), that is, \([c]_\varepsilon \subseteq X\). We have \([\pi \cdot c]_\varepsilon = \pi \ast [c]_\varepsilon \subseteq \pi \ast X = X\). Therefore, \(\pi \cdot c \in C_X\), and so \(C_X\) is finitely supported. Let \(d \in D_X\), that is, \([d]_\varepsilon \cap X \neq \emptyset\). There exists \(d_1 \in [d]_\varepsilon\) and \(d_1 \in X\). Since \(\pi\) fixes \(supp(X)\), we have \(\pi \cdot d_1 = \pi \ast [d]_\varepsilon = [\pi \cdot d]_\varepsilon\) and \(\pi \cdot d_1 \in X\). Therefore, \(\pi \cdot d_1 \in [\pi \cdot d]_\varepsilon \cap X\), and so \(\pi \cdot d \in D_X\) and \(D_X\) is finitely supported.

It remains to prove that \(\underline{\varepsilon}\) and \(\overline{\varepsilon}\) are equivariant. Let \(\pi\) be a permutation of \(A\) and \(X\) an arbitrary finitely supported subset of \(U\). We have to prove that \(\underline{\varepsilon}(\pi \ast X) = \pi \ast \underline{\varepsilon}(X)\) and \(\overline{\varepsilon}(\pi \ast X) = \pi \ast \overline{\varepsilon}(X)\). Let \(y \in \underline{\varepsilon}(\pi \ast X)\), that is, \([y]_\varepsilon \subseteq \pi \ast X\). We have \(y = \pi \cdot (\pi^{-1} \cdot y)\), where \([\pi^{-1} \cdot y]_\varepsilon = \pi^{-1} \ast [y]_\varepsilon \subseteq \pi^{-1} \ast (\pi \ast X) = X\). Therefore, \(y \in \pi \ast \underline{\varepsilon}(X)\). Conversely, let \(y \in \pi \ast \underline{\varepsilon}(X)\), that is, \(y = \pi \cdot x\) where \([x]_\varepsilon \subseteq X\). We have \([y]_\varepsilon = [\pi \cdot x]_\varepsilon = \pi \ast [x]_\varepsilon \subseteq \pi \ast X\), and so \(y \in \underline{\varepsilon}(\pi \ast X)\).

Now, let \(y \in \overline{\varepsilon}(\pi \ast X), \) that is, \([y]_\varepsilon \cap (\pi \ast X) \neq \emptyset\). Let \(z \in [y]_\varepsilon \cap (\pi \ast X)\). We have \(\pi^{-1} \cdot z \in \pi^{-1} \ast [y]_\varepsilon = [\pi^{-1} \cdot y]_\varepsilon\) and \(\pi^{-1} \cdot z \in \pi^{-1} \ast (\pi \ast X) = X\). Therefore, \([\pi^{-1} \cdot y]_\varepsilon \cap X \neq \emptyset\). Since \(y = \pi \cdot (\pi^{-1} \cdot y)\), we have \(y \in \pi \ast \overline{\varepsilon}(X)\). Conversely, let \(y \in \pi \ast \overline{\varepsilon}(X)\). We have \(y = \pi \cdot x\) where \([x]_\varepsilon \cap X \neq \emptyset\). If \(z \in [x]_\varepsilon \cap X\), then \(\pi \cdot z \in [y]_\varepsilon \cap (\pi \ast X)\). Therefore, \([y]_\varepsilon \cap (\pi \ast X) \neq \emptyset\), and so \(y \in \overline{\varepsilon}(\pi \ast X)\). □

Theorem 3.37. Let \((U, \cdot)\) be an invariant set and \(\varepsilon\) an equivariant equivalence relation on \(U\). The pair \((\overline{\varepsilon}, \underline{\varepsilon})\) is an invariant Galois connection on \(\wp_f (U)\).

Proof. According to Proposition 3.32, the functions \(\underline{\varepsilon}\) and \(\overline{\varepsilon}\) are well defined and equivariant. Moreover, \(\underline{\varepsilon}\) and \(\overline{\varepsilon}\) are monotone by Definition 3.29. Now, fix some \(X \in \wp_f (U)\). Let \(x\) be an arbitrary element of \(X\). Let \(y \in [x]_\varepsilon\). Since \(\varepsilon\) is an equivalence
relation, we also have $x \in [y]_e$. However, $x \in X$, and so $[y]_e \cap X \neq \emptyset$. Therefore, $[x]_e \subseteq \bar{e}(X)$. Since $x$ is an arbitrary element from $X$, we obtain $X \subseteq \bar{e}(\bar{e}(X))$. Now, let $x$ be an arbitrary element from $\bar{e}(\bar{e}(X))$, that is, $[x]_e \cap \bar{e}(X) \neq \emptyset$. Let $y \in [x]_e \cap \bar{e}(X)$. This means $x \in [y]_e$, and $[y]_e \subseteq X$. Therefore, $x \in X$, and so $\bar{e}(\bar{e}(X)) \subseteq X$. According to Proposition 3.17, we have that $(\bar{e}, \bar{e})$ is an invariant Galois connection on $\varrho_{fs}(U)$.

**Lemma 3.1.** Let $(U, \cdot)$ be an invariant set. Then $(\varrho_{fs}(U), \subseteq, \ast)$ is an invariant Boolean lattice.

**Proof.** Clearly, $\subseteq$ is an equivariant order relation on $\varrho_{fs}(U)$ by the definition of $\ast$ (Subsection 2.4.1). Therefore, $(\varrho_{fs}(U), \subseteq, \ast)$ is an invariant lattice. The distributivity property over $(\varrho_{fs}(U), \subseteq, \ast)$ follows directly from the distributivity property on $\varrho(U)$ because the intersection and the union of every two finitely supported subsets of $U$ is finitely supported by the union of the related supports. The greatest lower bound and the least upper bound in $\varrho_{fs}(U)$ are $U$ and $\emptyset$, respectively. Let $X \in \varrho_{fs}(U)$. The complement of $X$ is $U \setminus X$. If $S$ is a finite set of atoms supporting $X$, we claim that $S$ supports $U \setminus X$. Indeed, let $\pi \in \text{Fix}(S)$, which means $\pi \cdot x \in X$, $\forall x \in X$. We also have $\pi^{-1} \in \text{Fix}(S)$. Let $y \in U \setminus X$. If $\pi \cdot y \in X$, then $y \in \pi^{-1} \ast X = X$. Therefore, $\pi \cdot y \in U \setminus X$, which means $S$ supports $U \setminus X$. Therefore, $U \setminus X \in \varrho_{fs}(U)$, and $(\varrho_{fs}(U), \subseteq, \ast)$ is an invariant Boolean lattice.

**Lemma 3.2.** Let $(U, \cdot)$ be an invariant set. Then $(\varrho_{fs}(U), \subseteq, \ast)$ is an invariant complete lattice.

**Proof.** Let $\mathcal{F} = (X_i)_{i \in I}$ be a finitely supported family of finitely supported subsets of $U$. We know that $\bigcup_{i \in I} X_i$ exists in $U$. We have to prove that $\bigcup_{i \in I} X_i \in \varrho_{fs}(U)$.

We claim that $\text{supp}(\mathcal{F})$ supports $\bigcup_{i \in I} X_i$. Let $\pi \in \text{Fix}(\text{supp}(\mathcal{F}))$. Let $x \in \bigcup_{i \in I} X_i$. There exists $j \in I$ such that $x \in X_j$. Since $\pi \in \text{Fix}(\text{supp}(\mathcal{F}))$, we have $\pi \ast X_j \in \mathcal{F}$, that is, there exists $k \in I$ such that $\pi \ast X_j = X_k$. Therefore, $\pi \cdot x \in \pi \ast X_j = X_k$, and so $\pi \cdot x \in \bigcup_{i \in I} X_i$. We obtain $\pi \ast \bigcup_{i \in I} X_i = \bigcup_{i \in I} X_i$, and so $\bigcup_{i \in I} X_i$ is finitely supported.

**Theorem 3.38.** Let $(U, \cdot)$ be an invariant set and $\varepsilon$ an equivariant equivalence relation on $U$. The set of all fixed points of $\bar{e}$ forms an invariant complete Boolean sublattice of $\varrho_{fs}(U)$.

**Proof.** According to Lemma 3.1 and Lemma 3.2, we have that $(\varrho_{fs}(U), \subseteq, \ast)$ is an invariant complete Boolean lattice. According to Definition 3.29, we have that $X \subseteq \bar{e}(X)$, $\forall X \in \varrho_{fs}(X)$. Also, by Definition 3.29, we can prove immediately that $\bar{e}(X) = U \setminus (\bar{e}(U \setminus X)) = e(X)$, $\forall X \in \varrho_{fs}(X)$, that is, $\bar{e} = e$. According to Theorem 3.37 and Theorem 3.35, we have that the invariant conjugate of $\bar{e}$ coincides with $e$, that is, $\bar{e}$ is invariant self-conjugate. According to Theorem 3.36, the set of all fixed points of $\bar{e}$ forms an invariant complete Boolean sublattice of $\varrho_{fs}(U)$.

**Example 3.4.** According to Example 2.4, the set of all $\lambda$-terms in the $\lambda$-calculus is an invariant set, and the $\alpha$-equivalence relation in the $\lambda$-calculus is an equivariant equivalence relation on the set of all $\lambda$-terms. Therefore, finitely supported
sets of \( \lambda \)-terms can be invariantly approximated according to \( \alpha \)-conversion in the sense of Definition 3.29, and the FSM approximation results in this section can be applied to approximations of finitely supported sets of \( \lambda \)-terms.

- Similarly, finitely supported subsets of the invariant set \( A \times X \), where \( X \) is an invariant set, can be approximated according to the equivariant equivalence relation \( \sim_A \) defined by \((a,x) \sim_A (b,y)\) if and only if either \( a = b \) and \( x = y \), or \( b \not= a \), \( b \notin \text{supp}(x) \) and \( y = (ba) \cdot x \); according to Section 2.10, \( \sim_A \) is induced by the FSM abstraction.

### 3.3.4 Abstract Interpretation

The concrete semantics of a program is a mathematical model given by the set of all its possible executions. Many program properties are undecidable in this semantics. Thus, naturally appears the idea of mapping the concrete semantics to an abstract semantics where program properties are decidable. The theory of abstract interpretation was originally developed in [57, 58]. It represents a theory of approximation of mathematical structures, in particular those involved in the semantic models of computer programs. The concrete execution of a program is approximated by a refined analysis that sacrifices precision for speed. The theory of abstract interpretation expresses the connection between these two analyses using a Galois connection between the associated properties lattices. The theory of abstract interpretation is sound, but not complete. Thus, every property of a program which can be proved using the theory of abstract interpretation is correct; however, the statement that all properties about a program can be determined using this technique is not valid. The main idea of the theory of abstract interpretation of a program is to define a local interpretation function for basic instructions, and to use fixed-point approximations in order to discover properties without effectively executing the program line by line.

The theory of abstract interpretation has been successfully applied to generate methods of approximating complex or undecidable problems in various areas of computer science such as semantics, static analysis, proof theory, security and safety of software or hardware computer systems It also found applications in automatically verifying complex properties of real-time, safety critical, embedded systems.

The theory of abstract-interpretation is developed in [113] by the means of correctness relations and representation functions. Let us consider an arbitrary programming language. Its semantics identifies some set \( V \) of \textit{values} and specifies what transitions between these values look like, without necessarily imposing determinacy of such transitions. A program analysis identifies the set \( L \) of \textit{properties} and a transition function \( f_t : L \to L \) on the space of properties. Unlike the case of semantics, the transition between properties should be deterministic.

Every program analysis should be correct with respect to the semantics. Therefore, there exists a connection between the set of values and the set of properties described by the correctness relation: \( R : V \times L \to \{\text{true, false}\} \). The theory of abstract interpretation is developed in [113] by considering the set of properties \( L \)
as a complete lattice equipped with a partial ordering \( \sqsubseteq \); related to this relation, “smaller” informally means “more precise”. The correctness relation satisfies the following properties:

- whenever \( vRl_1 \) and \( l_1 \sqsubseteq l_2 \), we also have \( vRl_2 \);
- whenever \( L' \subseteq L \) and \( vRl \) for all \( l \in L' \), we also have \( vR(\sqcap L') \).

The required properties of \( R \) are motivated in Subsection 4.1.1 from [113]. The correctness criterion for the analysis is formulated in the following way:

If \( v_1Rl_1, v_1 \) is transformed into \( v_2 \) and \( f_L(l_1) = l_2 \), then \( v_2Rl_2 \).  

(1)

An alternative approach to the use of a correctness relation between values and properties is to employ a representation function \( \beta : V \rightarrow L \), where \( \beta \) maps each value to the best property describing it. The correctness criterion for the analysis is formulated in the following way:

If \( \beta(v_1) \sqsubseteq l_1, v_1 \) is transformed into \( v_2 \) and \( f_L(l_1) = l_2 \), then \( \beta(v_2) \sqsubseteq l_2 \).  

(2)

A ZF relationship between correctness relations and representation functions is established in Subsection 4.1.2 from [113]. The formulations (1) and (2) of the correctness of the analysis are equivalent in the ZF framework according to Lemma 4.5 in [113].

Our goal is to study the theory of abstract interpretation in the framework of invariant sets. For this, let us consider an invariant set \( (V, \cdot V) \) of values endowed with an equivariant/finitely supported transition relation between these values and an invariant complete lattice \( (L, \cdot L, \sqsubseteq) \) of properties endowed with an equivariant/finitely supported function \( f_L : L \rightarrow L \) which models the transitions between properties. As in the ZF framework, we usually require \( f_L \) to be monotone. Informally, this requirement means that whenever \( l_1 \) describes at least the values that \( l_2 \) does, then also \( f_L(l_1) \) describes at least the values that \( f_L(l_2) \) does.

We present the concepts of correctness relation and representation function in FSM.

**Definition 3.30.** An invariant correctness relation is an equivariant function \( R : V \times L \rightarrow \{true, false\} \), i.e. an equivariant subset of the Cartesian product \( V \times L \) that satisfies the following properties:

- whenever \( vRl_1 \) and \( l_1 \sqsubseteq l_2 \), we also have \( vRl_2 \);
- whenever \( L' \subseteq L \) is finitely supported and \( vRl \) for all \( l \in L' \), we also have \( vR(\sqcap L') \).

**Definition 3.31.** An invariant representation function is an equivariant function \( \beta : V \rightarrow L \) where \( \beta \) maps each value to the best property describing it.

The correctness criteria of the analysis are presented in FSM in forms (1) and (2) above, with the caveat that the transitions appearing in their statements are equivariant. A relationship between the concepts of invariant correctness relation and invariant representation function is presented in Theorem 3.39. According to this theorem, the formulations (1) and (2) of the correctness of the program analysis are equivalent in FSM.
Theorem 3.39. 1. Let $\beta : V \to L$ be an invariant representation function. The relation $R_\beta : V \times L \to \{true, false\}$ defined by $vR_\beta l$ if and only if $\beta(v) \subseteq l$ is an invariant correctness relation. $R_\beta$ is called the invariant correctness relation generated by $\beta$.

2. Let $R : V \times L \to \{true, false\}$ be an invariant correctness relation. The function $\beta_R : V \to L$ defined by $\beta_R(v) = \cap\{l \in L | vRl\}$ for all $v \in V$ is an invariant representation function. $\beta_R$ is called the invariant representation function generated by $R$.

3. $\beta_{R_\beta} = \beta$ and $R_{\beta_R} = R$.

Proof. Let $\beta : V \to L$ be an invariant representation function. We prove that $R_\beta$ is equivariant. Consider $(v, l) \in V \times L$ such that $vR_\beta l$ and $\pi \in S_A$. We have $\beta(\pi(v)) \subseteq l$. Since $L$ is an invariant lattice, we have that $\subseteq$ is equivariant, and $\pi \:: L \beta(v) \subseteq \pi \\cdot Ll$. Since $\beta$ is equivariant, according to Corollary 2.3, we have $\beta(\pi \cdot v) \subseteq \pi \cdot Ll$. Therefore, $(\pi \cdot v)R_\beta(\pi \cdot Ll)$, that is, $R_\beta$ is equivariant. From the definition of $R_\beta$, because $\subseteq$ is a lattice order, we have that $R_\beta$ satisfies the conditions in Definition 3.30.

Now, let $R : V \times L \to \{true, false\}$ be an invariant correctness relation. We claim that, for any $v \in V$, the set $X_v = \{l \in L | vRl\}$ is supported by $supp(v)$. Let $v \in V$ be an arbitrary element. Let $\pi \in Fix(supp(v))$ and $l \in X_v$. Since $R$ is equivariant, we have $(\pi \cdot v)R(\pi \cdot Ll)$. However, since $\pi \in Fix(supp(v))$, we have $\pi \cdot v = v$. Therefore, $vR(\pi \cdot Ll)$, and $\pi \cdot Ll \in X_v$. This means $\pi \cdot v = \pi \cdot Lx$, for all $v \in V$, where $\pi \cdot v$ represents the $S_A$-action on $\phi(V)$ defined in Subsection 2.4.1. Since $X_v$ is finitely supported for all $v \in V$, according to Theorem 3.32, there exists $\cap X_v$ for all $v \in V$. Therefore, $\beta_R$ is well defined. We claim that $\beta_R$ is equivariant. Let $\pi \in S_A$. First we prove that the sets $Y_v = \{\pi \cdot Ll \in L | vRl\}$ and $Z_v = \{l \in L | (\pi \cdot v)Rl\}$ coincide for all $v \in V$. Let $x \in Y_v$. Then $x = \pi \cdot Ll$ for some $l \in L$ with $vRl$. However, since $R$ is equivariant, we have $(\pi \cdot v)R(\pi \cdot Ll)$, that is, $(\pi \cdot v)Rx$. Therefore, $x \in Z_v$. Conversely, let $x \in Z_v$. Then $(\pi \cdot v)Rx$. Since $R$ is equivariant, we have $vR(\pi^{-1} \cdot Lx)$, that is, $x = \pi \cdot L(\pi^{-1} \cdot Lx)$, for all $v \in V$. According to Proposition 3.14, we have $\beta_R(\pi \cdot v) = \cap\{l \in L | (\pi \cdot v)Rl\} = \cap Y_v = \pi \cdot Ll \in L | vRl\} = \cap(\pi \cdot Ll \in L | vRl\} = \pi \cdot Ll \in L | vRl\} = \pi \cdot L\beta_R(v)$, where $\pi \cdot L$ represents the $S_A$-action on $\phi(L)$ defined in Subsection 2.4.1. Therefore, $\beta_R$ is a well-defined equivariant function.

Clearly, $\beta_{R_\beta}(v) = \cap\{l \in L | vR_\beta l\} = \cap\{l \in L | \beta(v) \subseteq l\} = \beta(v)$ for all $v \in V$. Therefore, $\beta_{R_\beta} = \beta$. It remains to prove that $vRl$ if and only if $vR_{\beta_R}l$. Suppose that $vRl$. Then, by the definition of $\beta_R$, we have $\beta_R(v) \subseteq l$ and hence $vR_{\beta_R}l$. Conversely, suppose $vR_{\beta_R}l$. Then $\beta_R(v) \subseteq l$. Let $l' = \{l | vRl\}$. Since $R$ is an invariant correctness relation and $vRl'$ for all $l' \in L'$, we obtain $vR(\cap L') = \cap(\beta_R(v)).$ Now, because $\beta_R(v) \subseteq l$ and because $R$ is an invariant correctness relation we have $vRl$. 

Galois connections are used in program analysis [113] in order to replace a costly space of properties with a simpler one. Actually, a Galois connection describes the relationship between such two spaces. Using the notion of invariant Galois connection described in Subsection 3.3.2 we can prove the following result.

Theorem 3.40. Let $(V, \cdot v)$ be an invariant set of values, $(L, \cdot L, \subseteq)$ be an invariant complete lattice of properties and $\beta : V \to L$ be an invariant representation function.
There exists an invariant Galois connection \((f, g)\) between the invariant complete lattices \((\mathcal{P}_f(V), \subseteq, \cdot_V)\) and \(L\) defined as follows:

- \(f: \mathcal{P}_f(V) \to L, f(W) = \sqcup\{\beta(v) | v \in W\}\) for all \(W \in \mathcal{P}_f(V)\).
- \(g: L \to \mathcal{P}_f(V), g(l) = \{v \in V | \beta(v) \sqsubseteq l\}\) for all \(l \in L\).

**Proof.** First we remark that \((\mathcal{P}_f(V), \subseteq, \cdot_V)\) is an invariant complete lattice according to Lemma 3.2. Let \(W \subseteq V\) be finitely supported. Since there exists a finite set \(S\) supporting \(W\), we obtain that the set \(\beta(W) = \{\beta(v) | v \in W\}\) is also supported by \(S\). Indeed, because \(\beta\) is equivariant, for each \(v \in W\) and each \(\pi \in S_A\) we have \(\pi \cdot L \beta(v) = \beta(\pi \cdot V v)\). Let \(\pi \in Fix(S)\) and \(v \in W\). Since \(\pi\) fixes \(S\) pointwise and \(S\) supports \(W\), we have \(\pi \cdot V v \in W\). Therefore, \(\pi \cdot L \beta(v) \in (\beta(W)\) for all \(\pi \in Fix(S)\) and \(v \in W\). This means \(S\) supports \(\beta(W)\). Since \(L\) is an invariant complete lattice, there exists the least upper bound of \(\beta(W)\) for all \(W \in \mathcal{P}_f(V)\), and so \(f\) is well-defined. We claim that \(f\) is equivariant. In order to prove this we have to prove that \(f(\pi \cdot V W) = \pi \cdot L f(W)\) for all \(\pi \in S_A\) and \(W \in \mathcal{P}_f(V)\). Fix some such \(\pi\) and \(W\). By the definition of \(f\), we have \(f(\pi \cdot V W) = \sqcup\{\beta(v) | v \in \pi \cdot V W\}\) = \(\sqcup\beta(\pi \cdot V W)\) = \(\sqcup\{\beta(\pi \cdot V v) | v \in W\}\). According to Proposition 3.14 and because \(\beta\) is equivariant, we obtain \(\pi \cdot L f(W) = \pi \cdot L \sqcup\{\beta(v) | v \in W\} = \sqcup(\pi \cdot L \{\beta(v) | v \in W\}) = \sqcup\{\pi \cdot L \beta(v) | v \in W\} = \sqcup\{\beta(\pi \cdot V v) | v \in W\}\). Therefore, \(f\) is equivariant.

Now we have to prove that \(g\) is well defined and equivariant. Let \(X_l = \{v \in V | \beta(v) \sqsubseteq l\}\). We claim that \(supp(l)\) supports \(X_l\). Let \(\pi \in Fix(supp(l))\), and \(v \in X_l\) be arbitrarily chosen. Then, \(\beta(v) \sqsubseteq l\). Since \(\subseteq\) is equivariant, we also have \(\pi \cdot L \beta(v) \sqsubseteq \pi \cdot L l\). Since \(\beta\) is equivariant and \(\pi\) fixes \(supp(l)\) pointwise, we have that \(\beta(\pi \cdot V v) = \pi \cdot L \beta(v) \sqsubseteq \pi \cdot L l = l\). Therefore, \(\pi \cdot V X_l \subseteq X_l\) whenever \(\pi \in Fix(supp(l))\). Since \(\pi \in Fix(supp(l))\) iff \(\pi^{-1} \in Fix(supp(l))\), it follows that \(\pi^{-1} \cdot V X_l \subseteq X_l\), from which \(\pi \cdot V (\pi^{-1} \cdot V X_l) \subseteq \pi \cdot V X_l\) (according to Lemma 3.2), and finally \(X_l \subseteq \pi \cdot V X_l\). Since \(X_l\) is finitely supported for all \(l \in L\), the definition of \(g\) makes sense. In order to prove that \(g\) is equivariant we have to prove that \(g(\pi \cdot L l) = \pi \cdot V g(l)\) for all \(\pi \in S_A\) and \(l \in L\). Fix \(\pi \in S_A\) and \(l \in L\). Since \(\subseteq\) and \(\beta\) are both equivariant, we have \(\beta(v) \sqsubseteq \pi \cdot L l\) if and only if \(\beta(\pi^{-1} \cdot V v) \sqsubseteq l\). Thus, \(g(\pi \cdot L l) = \{v \in V | \beta(v) \sqsubseteq \pi \cdot L l\} = \{v \in V | \beta(\pi^{-1} \cdot V v) \sqsubseteq l\} = \pi \cdot V \{v \in V | \beta(\pi^{-1} \cdot V v) \sqsubseteq l\} = \pi \cdot V g(l)\). Let us fix \(W \in \mathcal{P}_f(V)\) and \(l \in L\). Then \(f(W) \sqsubseteq l\) iff \(\sqcup\{\beta(v) | v \in W\} \sqsubseteq l\) iff \(\beta(v) \sqsubseteq l, \forall v \in W\) iff \(W \sqsubseteq g(l)\). According to Definition 3.26, we get that \((f, g)\) is an invariant Galois connection between \(\mathcal{P}_f(V)\) and \(L\).

The next results show us that the correctness results still hold in FSM when we replace the invariant complete lattice of properties \((L, \sqsubseteq, \cdot L)\) with another (simpler) invariant complete lattice \((K, \subseteq, \cdot K)\) by using an invariant Galois connection. Therefore, whenever we have an invariant Galois connection between \(L\) and \(K\), we can define an invariant correctness relation and an invariant representation function, respectively, between \(V\) and \(K\).

**Theorem 3.41.** Let us consider an invariant Galois connection \((f, g)\) between the invariant complete lattices \((L, \subseteq, \cdot L)\) and \((K, \subseteq, \cdot K)\). Let \(R: V \times L \to \{true, false\}\) be an invariant correctness relation between \(V\) and \(L\). There exists an invariant correctness relation \(R': V \times K \to \{true, false\}\) between \(V\) and \(K\) defined by \(v R' k\) if and only if \(v R g(k)\), for all \(v \in V\) and \(k \in K\).
Proof. First we prove that $R'$ is equivariant. Let $\pi \in S_\Delta$ and $v \in V$, $k \in K$ such that $vR'k$, namely $vRg(k)$. Since $R$ is equivariant, then $(\pi \cdot v)R(\pi \cdot Lg(k))$. Since $g$ is equivariant, then $(\pi \cdot v)R(\pi \cdot Kk)$, that is $(\pi \cdot v)R'(\pi \cdot Kk)$. Therefore, $R'$ is equivariant. We should also prove that $R'$ satisfies the conditions of Definition 3.30. Let us consider $v \in V$ and $k_1, k_2 \in K$ such that $vR'k_1$ and $k_1 \subseteq K k_2$. By the definition of $R'$, we have $vRg(k_1)$. Since $g$ is monotone, we obtain $g(k_1) \subseteq Lg(k_2)$. Now, because $R$ is an invariant correctness relation, we get $vRg(k_2)$, that is $vR'k_2$. Let $K' \subseteq K$ be finitely supported such that $vR'k$ for all $k \in K'$. Then $vRg(k)$ for all $k \in K'$. Since $g$ is equivariant and $K'$ is finitely supported, we have that the set $\{g(k) | k \in K'\}$ is finitely supported (Proposition 3.18). Since $R$ is an invariant correctness relation, we have $vR(\cap \{g(k) | k \in K'\})$. Using Proposition 3.18, we obtain $vR(g(\cap K'))$, that is $vR'(\cap K')$. Thus, $R'$ defines an invariant correctness relation between $V$ and $K$. \hfill $\Box$

Theorem 3.42. Let us consider an invariant Galois connection $(f, g)$ between the invariant complete lattices $(L, \sqsubseteq_L, L)$ and $(K, \sqsubseteq_K, K)$, $R: V \times L \rightarrow \{true, false\}$ an invariant correctness relation between $V$ and $L$, and $R': V \times K \rightarrow \{true, false\}$ the invariant correctness relation between $V$ and $K$ defined as in Theorem 3.41. There exists an invariant representation function $\beta': V \rightarrow K$ such that $R'$ is the invariant correctness relation generated by $\beta'$.

Proof. Let $\beta: V \rightarrow L$ be the invariant representation function generated by $R$. According to Theorem 3.39, we have $\beta(v) \subseteq_L l$ if and only if $vRl$. Since $(f, g)$ is an invariant Galois connection between the invariant complete lattices $L$ and $K$, for each $v \in V$ and $k \in K$ we obtain $vR'k \iff vR(g(k)) \iff \beta(v) \subseteq_L g(k) \iff (f \circ \beta)(v) \subseteq_K k$. Since $f$ and $\beta$ are both equivariant, then $f \circ \beta$ is equivariant. Therefore, according to Theorem 3.39, $R'$ is the invariant correctness relation generated by $\beta' = f \circ \beta$. \hfill $\Box$

Note also that the results in this subsection could be extended by considering finitely supported functions instead of equivariant functions. We do not present amply such an extension due to the more laborious calculations. An example of what such a result could look like is the next theorem, an extension of Theorem 3.39.

Theorem 3.43. 1. Let $\beta: V \rightarrow L$ be a finitely supported representation function. The relation $R_\beta: V \times L \rightarrow \{true, false\}$ defined by $vR_\beta l$ if and only if $\beta(v) \subseteq l$ is a finitely supported correctness relation. Moreover, $\text{supp}(R_\beta) \subseteq \text{supp}(\beta)$.

2. Let $R: V \times L \rightarrow \{true, false\}$ be a finitely supported correctness relation. The function $\beta_R: V \rightarrow L$ defined by $\beta_R(v) = \cap \{l \in L | vRl\}$ for all $v \in V$ is a finitely supported representation function. Moreover, $\text{supp}(\beta_R) \subseteq \text{supp}(R)$.

3. $\beta_{R_\beta} = \beta$ and $R_{\beta_\beta} = R$.

This result can be proved by a direct refinement of the proof of Theorem 3.39. The rest of the results can be reformulated similarly to the previous theorem.

In order to emphasize that in this new framework we can get abstract interpretations of some programming languages that cannot be obtained with standard abstract interpretation techniques, we provide an example of a lattice which is invariant complete, but fails to be complete in the classical ZF approach. Let us consider the set $A$ of atoms. Let $L$ be the set of those subsets of $A$ which are either finite or cofinite (i.e.
3.3 Order Theory in Finitely Supported Mathematics

their complements are finite). Therefore, \( L \) is represented exactly by those finitely supported subsets of \( A \) according to the \( S_A \)-action defined in Subsection 2.4.1, i.e. \( L \) coincides with \( (\wp_{fs}(A), \subseteq, \ast) \). Since \( A \) is a fixed ZF set, the construction of the lattice \( (\wp_{fs}(A), \subseteq, \ast) \) makes sense in ZF. According to Lemma 3.2, \( L = (\wp_{fs}(A), \subseteq, \ast) \) is an invariant complete lattice.

However, \( L = (\wp_{fs}(A), \subseteq, \ast) \) is no longer a complete lattice in the classical ZF framework. This is because the union of an infinite (possibly not finitely supported) family of finitely supported subsets of \( A \) is not necessarily itself finitely supported. For example, consider an infinite and coinfinite set of atoms, generically denoted by \( \{a, c, \ldots\} \). The family formed by singletons from \( A \), \( \mathcal{F} = \{a\}, \{c\}, \ldots \) is a family of finitely supported subsets of \( A \) (because each \( \{a\}, \{c\} \) is finitely supported). The union of the members of \( \mathcal{F} \) coincides with \( \{a, c, \ldots\} \), which is not finitely supported. Therefore, \( \mathcal{F} \) does not have a least upper bound in \( (\wp_{fs}(A), \subseteq, \ast) \).

Since there exist such invariant complete lattices that fail to be ZF complete, there may also exist abstract interpretations of some programming languages that can be easily described by using invariant sets. However, a case study requires laborious calculations, and is not analyzed in this book.

3.3.5 Calculability: Approximations of Fixed Points

Let us consider an invariant complete lattice \( (L, \cdot, \leq) \) of properties endowed with an equivariant/finitely supported function \( f_L : L \rightarrow L \) which models the transitions between properties. For recursive or iterative program constructs we want to obtain the least fixed point of \( f_L \) as the result of a finite iterative process. Such a least fixed point exists in FSM according to Theorem 3.33.

As in the ZF framework, we can provide an algorithm to approximate the least fixed point of \( f_L \). The idea is to approximate \( lfp(f) \) by the upper bound of a finitely supported ascending sequence.

**Definition 3.32.** Let \( (D, \cdot, \leq) \) be an invariant poset. A **finitely supported countable sequence** (finitely supported countable chain) in \( D \) is a sequence \( (d_n | n < \omega) \in D \) for which there exists a finite set \( S \subset A \) such that \( supp(d_n) \subseteq S \) for all \( n < \omega \). For a finitely supported sequence \( (d_n | n < \omega) \) we write \( supp(d_n | n < \omega) \) for the least such \( S \).

**Remark 3.8.** According to Definition 3.32, a sequence \( (d_n | n < \omega) \in D \) is finitely supported if and only if the mapping \( n \mapsto d_n \) is a finitely supported function from \( \mathbb{N} \) to \( D \).

**Definition 3.33.** Let \( (L, \leq, \cdot) \) be an invariant complete lattice. An **invariant upper bound operator** on \( L \) is a finitely supported function \( \phi : L \times L \rightarrow L \) with the property that for all \( l_1 \) and \( l_2 \) in \( L \) we have \( l_1 \sqsubseteq \phi(l_1, l_2) \) and \( l_2 \sqsubseteq \phi(l_1, l_2) \).
Lemma 3.3. Let \((L, \subseteq, \cdot)\) be an invariant complete lattice and \(\phi : L \times L \to L\) a finitely supported function. If \((l_n \mid n < \omega) \in L\) is a finitely supported sequence, then \((l^n_0 \mid n < \omega) \in L\) is also a finitely supported sequence, where

\[
L_n^\phi = \begin{cases} 
  l_n, & \text{for } n = 0; \\
  \phi(l_{n-1}^\phi, l_n), & \text{for } n > 0.
\end{cases}
\]

Proof. Let \(S = \text{supp}(l_n \mid n < \omega)\). This means \(\pi \cdot l_n = l_n\) for all \(n < \omega\) and all \(\pi \in \text{Fix}(S)\). We claim that \(S \cup \text{supp}(\phi)\) supports the sequence \((l^n_0 \mid n < \omega) \in L\), that is, \(S \cup \text{supp}(\phi)\) supports each element \(l^n_0\). Let \(\pi \in \text{Fix}(S \cup \text{supp}(\phi))\). We have \(\pi \cdot l_0 = l_0 = l_0^\phi\) because \(S\) supports \(l_0\). This means \(\text{supp}(l_0^\phi) \subseteq S \cup \text{supp}(\phi)\).

Let \(n > 0\), and assume that \(\pi \in \text{Fix}(S \cup \text{supp}(\phi) \cup \text{supp}(l^\phi_{n-1}))\). According to Proposition 2.4, we have \(\pi \cdot l_0 = \phi(\pi \cdot l_{n-1}^\phi, \pi \cdot l_n) = \phi(l_{n-1}^\phi, l_n) = l^n_0\). Therefore, \(\text{supp}(l_0^\phi) \subseteq S \cup \text{supp}(\phi) \cup \text{supp}(l^\phi_{n-1})\) for all \(0 < n < \omega\). By recursion, \(\text{supp}(l_0^\phi) \subseteq S \cup \text{supp}(\phi) \cup \text{supp}(l^\phi_0) = S \cup \text{supp}(\phi)\) for all \(0 < n < \omega\).

From Lemma 3.3 and Fact 4.11 in [113], we obtain the following result.

Proposition 3.23. Let \((L, \subseteq, \cdot)\) be an invariant complete lattice and \(\phi : L \times L \to L\) an invariant upper bound operator in \(L\). If \((l_n \mid n < \omega) \in L\) is a finitely supported sequence, then \((l^n_0 \mid n < \omega) \in L\) is a finitely supported ascending sequence.

We introduce a particular class of invariant upper bound operators which help us to approximate least fixed points in FSM. According to Proposition 3.23, the following definition makes sense.

Definition 3.34. Let \((L, \subseteq, \cdot)\) be an invariant complete lattice. A function \(\nabla : L \times L \to L\) is an invariant widening operator on \(L\) if and only if:

- \(\nabla\) is an invariant upper bound operator on \(L\);
- for any finitely supported ascending sequence \((l_n \mid n < \omega) \in L\), the finitely supported ascending sequence \((l^n_0 \mid n < \omega) \in L\) eventually stabilizes (i.e. the sequence \((l^n_0 \mid n < \omega) \in L\) becomes constant for a sufficiently large \(n\)).

Lemma 3.4. Let \((L, \subseteq, \cdot)\) be an invariant complete lattice, \(f : L \to L\) a finitely supported monotone function and \(\nabla\) an invariant widening operator on \(L\). The sequence \((f^n_0 \mid n < \omega) \in L\) is finitely supported, where

\[
f^n_\nabla = \begin{cases} 
  \bot, & \text{for } n = 0; \\
  f^{n-1}_\nabla, & \text{for } n > 0 \land f(f^{n-1}_\nabla) \subseteq f^{n-1}_\nabla; \\
  \nabla(f^{n-1}_\nabla, f(f^{n-1}_\nabla)), & \text{otherwise}.
\end{cases}
\]

Proof. According to the definition of \(\bot\), we have \(\bot \subseteq \pi \cdot \bot\) and \(\bot \subseteq \pi^{-1} \cdot \bot\) for each \(\pi\), which means \(\bot = \pi \cdot \bot\) and \(\text{supp}(f^n_\nabla) = \text{supp}(\bot) = \emptyset\). We claim that \(\text{supp}(f) \cup \text{supp}(\nabla)\) supports \(f^n_\nabla\) for each \(0 < n < \omega\). Let \(\pi \in \text{Fix}(\text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(f^{n-1}_\nabla))\). According to Proposition 2.4, we have \(\pi \cdot f^n_\nabla = \pi \cdot f^{n-1}_\nabla = f^{n-1}_\nabla = f^{n-1}_\nabla\). Therefore, \(\pi \cdot f^n_\nabla = f^n_\nabla\) for all \(0 < n < \omega\).
if $f(f^n_{\mathcal{V}}) \sqsubseteq f^n_{\mathcal{V}}$, and $\pi \cdot f^n_{\mathcal{V}} = \nabla(\pi \cdot f^{n-1}_{\mathcal{V}}, \pi \cdot f(f^{n-1}_{\mathcal{V}})) = \nabla(f^{n-1}_{\mathcal{V}}, f(f^{n-1}_{\mathcal{V}})) = f^n_{\mathcal{V}}$ otherwise. Therefore, in either case we have $\pi \cdot f^n_{\mathcal{V}} = f^n_{\mathcal{V}}$ for $\pi \in \text{Fix}(\text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(f^{n-1}_{\mathcal{V}}))$ and $0 < n < \omega$. This means $\text{supp}(f^n_{\mathcal{V}}) \subseteq \text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(f^{n-1}_{\mathcal{V}})$. By recursion, we have $\text{supp}(f^n_{\mathcal{V}}) \subseteq \text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(f^0_{\mathcal{V}})$ for all $n < \omega$. Thus, the sequence $(f^n_{\mathcal{V}} | n < \omega)$ is finitely supported.

The following proposition follows directly from Lemma 3.4 and Fact 4.14 in [113]; the last item follows from Remark 3.6.

**Proposition 3.24.** Let $(L, \sqsubseteq, \cdot)$ be an invariant complete lattice, $f : L \rightarrow L$ a finitely supported monotone function and $\nabla$ an invariant widening operator on $L$:

- the sequence $(f^n_{\mathcal{V}} | n < \omega)$ is a finitely supported ascending sequence;
- if $f(f^n_{\mathcal{V}}) \sqsubseteq f^m_{\mathcal{V}}$, then the finitely supported sequence $(f^n_{\mathcal{V}} | n < \omega) \in L$ eventually stabilizes and furthermore $\forall n > m : f^n_{\mathcal{V}} = f^m_{\mathcal{V}}$ and $\sqcup((f^n_{\mathcal{V}} | n < \omega) = f^m_{\mathcal{V}}$;
- if the finitely supported sequence $(f^n_{\mathcal{V}} | n < \omega) \in L$ eventually stabilizes, then there exists an $m$ such that $f(f^n_{\mathcal{V}}) \subseteq f^m_{\mathcal{V}}$;
- if the finitely supported sequence $(f^n_{\mathcal{V}} | n < \omega) \in L$ eventually stabilizes, then $\text{lfp}(f) \sqsubseteq \sqcup((f^n_{\mathcal{V}} | n < \omega)$.

**Theorem 3.44.** Let $(L, \sqsubseteq, \cdot)$ be an invariant complete lattice, $f : L \rightarrow L$ a finitely supported monotone function and $\nabla$ an invariant widening operator on $L$. The sequence $(f^n_{\mathcal{V}} | n < \omega) \in L$ eventually stabilizes.

**Proof.** Assume that $(f^n_{\mathcal{V}} | n < \omega) \in L$ never stabilizes. According to Proposition 3.24, $f(f^n_{\mathcal{V}}) \sqsubseteq f^m_{\mathcal{V}}$ never holds for any $n > 0$. Therefore, the sequence $(f^n_{\mathcal{V}} | n < \omega) \in L$ is defined by:

$$f^n_{\mathcal{V}} = \begin{cases} \bot, & \text{for } n = 0; \\ \nabla(f^{n-1}_{\mathcal{V}}, f(f^{n-1}_{\mathcal{V}})) , & \text{otherwise.} \end{cases}$$

We define the sequence $(l_n | n < \omega) \in L$ as follows:

$$l_n = \begin{cases} \bot, & \text{for } n = 0; \\ f(f^{n-1}_{\mathcal{V}}), & \text{for } n > 0. \end{cases}$$

We claim that $\text{supp}(f) \cup \text{supp}(\nabla)$ supports $l_n$ for each $n < \omega$. Let $\pi \in \text{Fix}(\text{supp}(f) \cup \text{supp}(\nabla))$. According to the proof of Proposition 3.4, $\pi \cdot f^{n-1}_{\mathcal{V}} = f^{n-1}_{\mathcal{V}}$. Clearly, $\pi \cdot l_0 = l_0$. For $n > 0$, according to Proposition 2.4, we have $\pi \cdot l_n = \pi \cdot f(f^{n-1}_{\mathcal{V}}) = f(\pi \cdot f^{n-1}_{\mathcal{V}}) = f(l_{n-1}) = l_n$. Thus, the sequence $(l_n | n < \omega) \in L$ is finitely supported. Since $f$ is monotone and $(l^n_{\mathcal{V}} | n < \omega) \in L$ is a finitely supported ascending sequence, we have that $(l_n | n < \omega) \in L$ is a finitely supported ascending sequence. Since $(l^n_{\mathcal{V}} | n < \omega) \in L$ is a finitely supported ascending sequence and $\nabla$ is an invariant widening operator, we have that the sequence $(l^n_{\mathcal{V}} | n < \omega) \in L$ eventually stabilizes. A trivial induction on $n$ shows us that $l^n_{\mathcal{V}} = f^n_{\mathcal{V}}$ for all $n < \omega$. Therefore, the sequence $(f^n_{\mathcal{V}} | n < \omega) \in L$ eventually stabilizes. We obtained a contradiction with the assumption that $(f^n_{\mathcal{V}} | n < \omega) \in L$ never stabilizes, and the desired result follows. 

According to Proposition 3.24 and Theorem 3.44, the least fixed point of a finitely supported monotone function \( f : L \to L \) can be approximated in the framework of invariant sets by \( \sqcup (f^n_\omega | n < \omega) \), which is the least upper bound of the sequence \( (f^n_\omega | n < \omega) \). According to Proposition 3.24, there exists an \( m \) such that \( f(f^n_\omega) \sqsubseteq f^m_\omega \), i.e. \( \sqcup (f^n_\omega | n < \omega) = f^m_\omega \). Therefore, we can consider \( \text{lfp}_\omega(f) = f^m_\omega \) as a safe approximation of \( \text{lfp}(f) \).

In the view of Lemma 3.3 the following definition makes sense.

**Definition 3.35.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete lattice. A function \( \Delta : L \times L \to L \) is an invariant narrowing operator on \( L \) if and only if:

- \( \Delta \) is finitely supported;
- \( l_2 \sqsubseteq l_1 \) implies \( l_2 \sqsubseteq (l_1 \Delta l_2) \sqsubseteq l_1 \) for all \( l_1, l_2 \in L \);
- for any finitely supported descending sequence \( (l_n | n < \omega) \in L \) the finitely supported descending sequence \( (l^n_\Delta | n < \omega) \in L \) eventually stabilizes.

**Lemma 3.5.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete lattice, \( f : L \to L \) a finitely supported monotone function, \( \nabla \) an invariant widening operator and \( \Delta \) an invariant narrowing operator on \( L \). Let \( m < \omega \) be an element with the property that \( f(f^m_\omega) \sqsubseteq f^m_\omega \), i.e. \( \text{lfp}_\omega(f) = f^m_\omega \). The sequence \( ([f]_\Delta^n | n < \omega) \in L \) is finitely supported, where

\[
[f]_\Delta^n = \begin{cases} f^m_\omega, & \text{for } n = 0; \\
\Delta([f]_\Delta^{n-1}, f([f]_\Delta^{n-1})), & \text{for } n > 0.
\end{cases}
\]

**Proof.** According to Lemma 3.4, \( f^m_\omega \) is supported by \( \text{supp}(f) \cup \text{supp}(\nabla) \). We claim that \( \text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(\Delta) \) supports \( [f]_\Delta^n \) for each \( n < \omega \). Let \( n > 0 \) and \( \pi \in \text{Fix}((\text{supp}(f) \cup \text{supp}(\Delta) \cup \text{supp}([f]_\Delta^{n-1}))) \). According to Proposition 2.4, for \( n > 0 \) we have \( \pi \cdot [f]_\Delta^n = \Delta(\pi \cdot [f]_\Delta^{n-1}, \pi \cdot f([f]_\Delta^{n-1})) = \Delta(\pi \cdot [f]_\Delta^{n-1}, f([f]_\Delta^{n-1})) = [f]_\Delta^n \). Thus, \( \text{supp}([f]_\Delta^n) \subseteq \text{supp}(f) \cup \text{supp}(\Delta) \cup \text{supp}([f]_\Delta^{n-1}) \) for each \( 0 < n < \omega \). By recursion, we have \( \text{supp}([f]_\Delta^n) \subseteq \text{supp}(f) \cup \text{supp}(\Delta) \cup \text{supp}([f]_\Delta^n) \subseteq \text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(\Delta) \) for all \( n < \omega \). Thus, the sequence \( ([f]_\Delta^n | n < \omega) \in L \) is finitely supported. □

Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete lattice and \( f : L \to L \) a finitely supported monotone function. According to Remark 3.6, we have that the set \( \text{Red}(f) = \{ d \in L | f(d) \sqsubseteq d \} \) is finitely supported and \( \text{lfp}(f) = \cap \{ d \in L | f(d) \sqsubseteq d \} \). Note that whenever \( f \) is finitely supported, by Proposition 2.4, we have that the \( n \)-time composition of \( f \) (denoted by \( f^n \)) is also supported by \( \text{supp}(f) \). According to Lemma 3.5 and Lemma 4.16 in [113], we get the following result.

**Proposition 3.25.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete lattice, \( f : L \to L \) a finitely supported monotone function, \( \nabla \) an invariant widening operator and \( \Delta \) an invariant narrowing operator on \( L \). Let \( m < \omega \) be an element with the property that \( f(f^m_\omega) \sqsubseteq f^m_\omega \). The sequence \( ([f]_\Delta^n | n < \omega) \in L \) is a finitely supported descending sequence in \( \text{Red}(f) \) and \( \text{lfp}(f) \sqsubseteq f^n(f^m_\omega) \sqsubseteq [f]_\Delta^n \).

**Theorem 3.45.** Let \( (L, \sqsubseteq, \cdot) \) be an invariant complete lattice, \( f : L \to L \) a finitely supported monotone function, \( \nabla \) an invariant widening operator and \( \Delta \) an invariant narrowing operator on \( L \). For any finitely supported descending sequence \( (l_n | n < \omega) \in L \), the sequence \( (l^n_\Delta | n < \omega) \in L \) eventually stabilizes.
narrowing operator on \( L \). Let \( m < \omega \) be an element with the property that \( f(f^m) \subseteq f^m \). The sequence \((f^n_{\Delta} | n < \omega) \in L \) eventually stabilizes.

**Proof.** We define the sequence \((l_n | n < \omega) \in L \) as follows:

\[
l_n = \begin{cases} 
  f^m, & \text{for } n = 0; \\
  f([f]^n_{\Delta}), & \text{for } n > 0.
\end{cases}
\]

We claim that \( \text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(\Delta) \) supports \( l_n \) for each \( n < \omega \). Let \( \pi \in \text{Fix}(\text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(\Delta)) \). According to the proof of Proposition 3.4, if \( n = 0 \) we have \( \pi \cdot f^m = f^m \) because \( \text{supp}(f) \cup \text{supp}(\nabla) \) supports \( f^m \). According to the proof of Lemma 3.5, if \( n > 0 \) we have \( \pi \cdot [f]_{\Delta}^{n-1} = [f]^{n-1}_{\Delta} \) because \( \text{supp}(f) \cup \text{supp}(\nabla) \cup \text{supp}(\Delta) \) supports \([f]_{\Delta}^{n-1} \). For \( n > 0 \), according to Proposition 2.4, we have \( \pi \cdot l_n = \pi \cdot [f]_{\Delta}^{n-1} = f(\pi \cdot [f]_{\Delta}^{n-1}) = f([f]_{\Delta}^{n-1}) = l_n \). Thus, the sequence \((l_n | n < \omega) \in L \) is finitely supported. Since \((f^n_{\Delta} | n < \omega) \in L \) is a finitely supported descending sequence and because \( f([f]^n_{\Delta}) \subseteq f^m \), we have that \((l_n | n < \omega) \in L \) is a finitely supported descending sequence. Therefore, \((l^n_{\Delta} | n < \omega) \in L \) eventually stabilizes. By induction, \( l^n_{\Delta} = [f]^n_{\Delta} \) for all \( n < \omega \). Therefore, the sequence \(([f]_{\Delta}^{n} | n < \omega) \in L \) eventually stabilizes. \( \square \)

Let \((L, \sqsubseteq, \cdot)\) be an invariant complete lattice, \( f : L \rightarrow L \) a finitely supported monotone function, \( \nabla \) an invariant widening operator and \( \Delta \) an invariant narrowing operator on \( L \). Let \( m < \omega \) be an element with the property that \( f(f^m) \subseteq f^m \). Proposition 3.25 assure us that \( \ell \text{fp}(f) \subseteq [f]^m_{\Delta} \). According to Theorem 3.45, the sequence \(([f]_{\Delta}^{n} | n < \omega) \in L \) eventually stabilizes. Therefore, there exists an \( m' < \omega \) such that \([f]^{m'}_{\Delta} = [f]^{m'}_{\Delta} \). Like in the ZF framework, we consider \( \text{fp}_{\omega}^{\text{f}} = [f]^{m'}_{\Delta} \) as the desired approximation for \( \ell \text{fp}(f) \).

Several refinements of these FSM approximations can be done similarly to the ZF framework. Let us assume that \((f, g)\) is an invariant Galois connection between the invariant complete lattices \((L, \sqsubseteq, \cdot)\) and \((K, \sqsubseteq, \cdot)\). If \( \nabla_K : K \times K \rightarrow K \) is a finitely supported function, then consider the function \( \text{supp}(\nabla) : L \times L \rightarrow L \) defined by \( \text{supp}(l_1, l_2) = g(\nabla_K(f(l_1), f(l_2))) \). Since \( f \) and \( g \) are equivariant, according to Proposition 2.4, we get that \( \nabla_L \) is supported by \( \text{supp}(\nabla_K) \), that is, \( \nabla_L \) is finitely supported. Therefore, the results expressed as Proposition 4.44 and Lemma 4.45 in [113] hold also in FSM. Thus, if \( f \) is surjective (or, equivalently, if \( g \) is injective) and \( \nabla_K \) is an invariant widening operator, then \( \nabla_L \) is an invariant widening operator. Moreover, in this case, if we impose the additional condition that \( g(\bot_K) = \bot_L \), we have \( \ell \text{fp}_{\nabla_L}(\phi) = g(\ell \text{fp}_{\nabla_K}(f \circ \phi \circ g)) \) for all finitely supported monotone functions \( \phi : L \rightarrow L \).

The results from Subsection 3.3.4 and Subsection 3.3.5 represent an extension of the original research presented in [21] and [20].
3.3.6 Complete Partially Ordered Sets

We translate the notion of chain-complete partially ordered set (cpo) into FSM. The main results of this subsection are presented in a slightly different manner in [141], for describing Scott recursive domain equations in the framework of nominal sets.

**Definition 3.36.** An invariant cpo $D$ is an invariant poset with the additional condition that any finitely supported countable ascending chain $(d_n \mid n < \omega)$ in $D$ (cf. Definition 3.32) has a least upper bound denoted by $\bigcup_{n<\omega} d_n$.

From the equivariance property of $\sqsubseteq$ and from the definition of a least upper bound, we obtain the following corollaries.

**Corollary 3.4.** Let $(D, \cdot, \sqsubseteq)$ be an invariant cpo. Then for any finitely supported chain $(d_n \mid n < \omega)$ in $D$ we have $\pi \cdot \bigcup_{n<\omega} d_n = \bigcup_{n<\omega} \pi \cdot d_n$.

**Corollary 3.5.** Let $(D, \cdot, \sqsubseteq)$ be an invariant cpo. Then for any finitely supported chain $(d_n \mid n < \omega)$ in $D$ we have $\text{supp}(\bigcup_{n<\omega} d_n) \subseteq \text{supp}(d_n \mid n < \omega)$.

**Proof.** We have to prove that any permutation $\pi$ fixing $\text{supp}(d_n \mid n < \omega)$ pointwise also fixes $\bigcup_{n<\omega} d_n$. For such a $\pi$ we have that $\pi \cdot d_n = d_n$ for all $n < \omega$. Hence $\bigcup_{n<\omega} \pi \cdot d_n = \bigcup_{n<\omega} d_n$. However, by Corollary 3.4, we also have $\bigcup_{n<\omega} \pi \cdot d_n = \pi \cdot \bigcup_{n<\omega} d_n$, which means $\pi$ fixes $\bigcup_{n<\omega} d_n$.

**Definition 3.37.** An invariant pointed cpo (invariant cppo) $(D, \cdot, \sqsubseteq, \bot)$ is an invariant cpo $(D, \cdot, \sqsubseteq)$ together with a least element $\bot$ (i.e. $\bot \sqsubseteq d$ for all $d \in D$).

**Definition 3.38.** Let $(D, \cdot, \sqsubseteq_D)$ and $(E, \cdot, \sqsubseteq_E)$ be two invariant cpos. A function $f : D \to E$ is finitely supported continuous if and only if it is finitely supported and monotone, and for each finitely supported chain $(d_n \mid n < \omega)$ in $D$ we have $f(\bigcup_{n<\omega} d_n) = \bigcup_{n<\omega} (f(d_n))$.

**Definition 3.39.** Let $(D, \cdot, \sqsubseteq_D, \bot_D)$ and $(E, \cdot, \sqsubseteq_E, \bot_E)$ be two invariant cpos. A finitely supported function $f : D \to E$ is strict if and only if $f(\bot_D) = \bot_E$.

**Proposition 3.26.** Given two invariant cpos $(D, \cdot, \sqsubseteq_D, \bot_D)$ and $(E, \cdot, \sqsubseteq_E, \bot_E)$ the set of all finitely supported continuous and strict functions from $D^\omega$ together with the pointwise partial order form another invariant cppo. We denote this new cppo by $D \to E$.

**Proof.** We claim that $D \to E$ is an invariant set with the $S_\lambda$-action $\ast : S_\lambda \times (D \to E) \to (D \to E)$ defined by $(\pi \ast f)(x) = \pi \cdot E f(\pi^{-1} \cdot D x)$ for all $\pi \in S_\lambda$, $f \in D \to E$ and $x \in D$. Let $\pi \in S_\lambda$ and $f \in D \to E$. Since $f$ is monotone and $\sqsubseteq_D$, $\sqsubseteq_E$ are equivariant, we obtain that $\pi \ast f$ is monotone. According to Corollary 3.4 and Proposition 2.1, we have that $\pi \ast f$ is continuous whenever $f$ is continuous. Also $\pi \ast f$ is strict because $f$ is strict and $\bot = \pi^{-1} \cdot D \bot = \pi \cdot E \bot$. Therefore, the $S_\lambda$-action $\ast$ is well defined, and $D \to E$ is an invariant set. The partial order $\sqsubseteq_{D \to E}$
is defined by \( f \sqsubseteq_{D \to E} g \) if and only if \( f(x) \sqsubseteq_{E} g(x) \) for all \( x \in D \). Since \( \sqsubseteq_{E} \) is equivariant, we obtain that \( \sqsubseteq_{D \to E} \) is equivariant. Let \( (f_n \mid n < \omega) \) be a finitely supported chain from \( D \to E \). For each \( x \in D \) the chain \( (f_n(x) \mid n < \omega) \) is supported by \( \text{supp}(f_n \mid n < \omega) \sqcup \text{supp}(x) \). Since \( E \) is an invariant cppo, there exists \( \sqcup \) \( f_n(x) \) for each \( x \in D \). We claim that \( g \) is the least upper bound of the chain \( (f_n \mid n < \omega) \) in \( D \to E \). Clearly, \( g \) is the least upper bound of the chain \( (f_n \mid n < \omega) \) with respect to the partial order \( \sqsubseteq_{D \to E} \).

We have to prove that \( g \in D \to E \). Since each \( f_n \) is monotone, we have that \( g \) is monotone. Let us consider a finitely supported chain \( (x_m \mid m < \omega) \) in \( D \). Since each \( f_n \) is continuous, we have

\[
\bigcup_{m < \omega} f_n(x_m) = \bigcup_{m < \omega} \bigcup_{n < \omega} f_n(x_m) = \bigcup_{n < \omega} \bigcup_{m < \omega} f_n(x_m) = \bigcup_{m < \omega} f_n(x_m) = \bigcup_{m < \omega} (g(x_m)).
\]

Therefore, \( g \) is continuous. Clearly, \( g \) is strict, and we obtain \( g \in D \to E \). The least element in the invariant cppo \( D \to E \) is the constantly bottom function and, hence, \( D \to E \) is an invariant cppo. Moreover, according to Proposition 2.4 and Corollary 3.4, we have that \( g \) is finitely supported.

**Definition 3.40.** Given an invariant cppo \( (D, \cdot, \sqsubseteq) \) and a finitely supported function \( f : D \to D \) we define \( f^n(d) \) by induction as follows:

\[
f^0(d) \overset{\text{def}}{=} d \text{ and } f^{n+1}(d) = f(f^n(d)).
\]

**Theorem 3.46.** Let \( (D, \cdot, \sqsubseteq, \perp) \) be an invariant cppo. Each finitely supported continuous function \( f : D \to D \) possesses a least fixed point \( \text{fix}(f) \) with the property that \( \text{supp}(\text{fix}(f)) \subseteq \text{supp}(f) \).

**Proof.** Since \( \perp \sqsubseteq f(\perp) \) and \( f \) is monotone, we have that \( (f^n(\perp) \mid n < \omega) \) is an ascending chain. We prove that \( (f^n(\perp) \mid n < \omega) \) is finitely supported, that is, there exists a finite \( S \subset A \) such that \( \text{supp}(f^n(\perp)) \subseteq S \) for each \( n < \omega \). We claim that \( S = \text{supp}(f) \) and we prove by induction that \( \text{supp}(f^n(\perp)) \subseteq \text{supp}(f) \) for each \( n < \omega \).

From the definition of \( \perp \), we have \( \perp \sqsubseteq \pi \cdot \perp \) and \( \perp \sqsubseteq \pi^{-1} \cdot \perp \) for each \( \pi \), which means \( \perp = \pi \cdot \perp \) and \( \text{supp}(\perp) = \emptyset \). Therefore, \( \text{supp}(f^0(\perp)) = \text{supp}(\perp) \subseteq \text{supp}(f) \).

Let us suppose that \( \text{supp}(f^n(\perp)) \subseteq \text{supp}(f) \) for some \( n < \omega \). We have to prove that \( \text{supp}(f^{n+1}(\perp)) \subseteq \text{supp}(f) \). So, we have to prove that each permutation \( \pi \) which fixes \( f^m(\perp) \) pointwise also fixes \( f^{n+1}(\perp) \). Let \( \pi \) be such a permutation. From the inductive hypothesis, we have \( \pi \cdot f^n(\perp) = f^n(\perp) \). According to Proposition 2.4, we have \( \pi \cdot f^{n+1}(\perp) = \pi \cdot f(f^n(\perp)) = f(\pi \cdot f^n(\perp)) = f^{n+1}(\perp) \). Therefore, \( (f^n(\perp) \mid n < \omega) \) is finitely supported, and there exists \( \bigcup_{n < \omega} f^n(\perp) \). According to Corollary 3.5, we have \( \text{supp}(\bigcup_{n < \omega} f^n(\perp)) \subseteq \text{supp}(f) \).

It remains to prove that \( \bigcup_{n < \omega} f^n(\perp) \) is a fixed point of \( f \). From the continuity of \( f \), we have \( f(\bigcup_{n < \omega} f^n(\perp)) = \bigcup_{n < \omega} f^{n+1}(\perp) = \bigcup_{n < \omega} f^n(\perp) \). If \( x \) is another fixed point of \( f \), then from \( \perp \sqsubseteq x \) we get \( f(\perp) \sqsubseteq f(x) \) and \( f(\perp) \sqsubseteq f(x) \) by induction. Therefore, \( x \) is an upper bound for the chain \( (f^n(\perp) \mid n < \omega) \). It follows from the definition of a least upper bound that \( \bigcup_{n < \omega} f^n(\perp) \subseteq x \) and hence \( \bigcup_{n < \omega} f^n(\perp) = \text{fix}(f) \). \( \square \)

**Definition 3.41.** For each invariant cppo \( (D, \cdot, \sqsubseteq) \) we define the binary relation \( \leq_A \) on \( A \times D \) by:
Definition 3.42. For each invariant cpo \((D, \cdot, \sqsubseteq)\), \((a, x) \preceq_A (b, y)\) if and only if \(\exists c \in A \setminus supp(a, b, x, y)(ac) \cdot x \sqsubseteq (bc) \cdot y\).

Proposition 3.27. For each invariant cpo \((D, \cdot, \sqsubseteq)\), \((a, x) \preceq_A (b, y)\) if and only if \(\forall c \in A \setminus supp(a, b, x, y)(ac) \cdot x \sqsubseteq (bc) \cdot y\).

Proof. The reverse direction is trivial because \(A \setminus supp(a, b, x, y)\) is non-empty. Let us suppose now that \((a, x) \preceq_A (b, y)\). Therefore, \(\exists c \in A \setminus supp(a, b, x, y)\) such that \((ac) \cdot x \sqsubseteq (bc) \cdot y\). Let \(d ∈ A \setminus supp(a, b, x, y)\). Since \(\sqsubseteq\) is equivariant, we have \((cd) \cdot (ac) \cdot x \sqsubseteq (cd) \cdot (bc) \cdot y\). It follows by easy calculation that \((ad) \cdot (cd) \cdot x \sqsubseteq (bd) \cdot (cd) \cdot y\). Since \(c, d \# x, y\), we get \((ad) \cdot x \sqsubseteq (bd) \cdot y\).

Proposition 3.28. For each invariant cpo \((D, \cdot, \sqsubseteq)\) the binary relation \(\sim_A\) is a pre-order on \(A \times D\).

Proof. Reflexivity is trivial. Let us suppose \((a, x) \preceq_A (b, y)\) and \((b, y) \preceq_A (c, z)\). Then there exists \(d ∈ A \setminus supp(a, b, x, y)\) such that \((ad) \cdot x \sqsubseteq (bd) \cdot y\) and \(e ∈ A \setminus supp(b, c, x, y)\) such that \((be) \cdot y \sqsubseteq (ce) \cdot z\). According to Proposition 3.27, for \(f ∈ A \setminus supp(a, b, c, x, y, z)\) we have that \((af) \cdot x \sqsubseteq (bf) \cdot y \sqsubseteq (ce) \cdot z\). By transitivity of \(\sqsubseteq\), we obtain \((a, x) \preceq_A (c, z)\).

Definition 3.42. For each invariant cpo \((D, \cdot, \sqsubseteq)\) we define the binary relation \(\sim\) on \(A \times D\) by:

\[(a, x) \sim (b, y)\text{ if and only if } (a, x) \preceq_A (b, y)\text{ and } (b, y) \preceq_A (a, x)\text{.}\]

According to Lemma 2.3, we obtain that \(\sim\) coincides with the equivalence relation \(\sim_A\) defined in Section 2.10. Therefore, for each \(a ∈ A\) and \(x ∈ D\) we have \([a]x = (a, x)/\sim\). Recall that \([A]D\) is an invariant set with the \(S_A\)-action defined as in Proposition 2.14.

Theorem 3.47. For each invariant cppo \((D, \cdot, \sqsubseteq)\), \([A]D\) is an invariant poset with the partial order defined by \([a]x \sqsubseteq_{[A]D} [b]y\) if and only if \((a, x) \preceq_A (b, y)\).

Proof. It is trivial to prove that \(\sqsubseteq_{[A]D}\) is a well-defined partial order on \([A]D\). It remains to prove that \(\sqsubseteq_{[A]D}\) is equivariant. Therefore, we have to prove that \((a, x) \preceq_A (b, y)\) implies \((\pi(a), \pi \cdot x) \preceq_A (\pi(b), \pi \cdot y)\) for each \(\pi ∈ S_A\). Let \((a, x) \preceq_A (b, y)\). Then there exists \(c ∈ A \setminus supp(a, b, x, y)\) such that \((ac) \cdot x \sqsubseteq (bc) \cdot y\). Let \(\pi ∈ S_A\). Since \(\sqsubseteq\) is equivariant, we obtain \((\pi(a), \pi(c)) \cdot (\pi \cdot x) \sqsubseteq (\pi(b), \pi(c)) \cdot (\pi \cdot y)\). Since \(c ∈ A \setminus supp(a, b, x, y)\), we obtain \(\pi(c) ∈ A \setminus supp(\pi(a), \pi(b), \pi \cdot x, \pi \cdot y)\) (see Lemma 2.1). Therefore, \((\pi(a), \pi \cdot x) \preceq_A (\pi(b), \pi \cdot y)\).

From the equivariance of \(\sqsubseteq\) and \(\sqsubseteq_{[A]D}\), we obtain the following result.

Proposition 3.29. Let \((D, \cdot, \sqsubseteq)\) be an invariant cpo and \(x, y ∈ D\). Then \(x \sqsubseteq y\) if and only if \([a]x \sqsubseteq_{[A]D} [a]y\) for each \(a ∈ A\).

Proposition 3.30. Let \(D\) be an invariant set. For each \([a]x\) in \([A]D\) and \(b ∈ A \setminus supp([a]x)\), there exists a unique \(y = (ab) \cdot x\) such that \([a]x = [b]y\). We call this \(y\) the concretion of \([a]x\) and \(b\), and we denote it by \((([a]x)@b)\).
3.3 Order Theory in Finitely Supported Mathematics

Proof. Let \( b \in A \setminus \text{supp}([a]x) \). We have either \( b = a \), or \( b \neq a \) and \( b \notin \text{supp}(x) \). The required result follows immediately from Lemma 2.3 \( \Box \)

By easy calculation, we obtain the following result.

Proposition 3.31. Let \( D \) be an invariant set. For each \([a]x \in [A]D\) and \( b, c \in A \), \( b \neq c \) with \( b, c \notin \text{supp}([a]x) \) we have \( (bc) \cdot (([a]x)@b) = ([a]x)@c \).

Proposition 3.32. Let \( D \) be an invariant set. For each \( b \in A \setminus \text{supp}([a]x) \) we have \( \text{supp}((([a]x)@b) \subseteq \text{supp}([a]x) \cup \{b\}) \).

Proof. Let \( b \in A \setminus \text{supp}([a]x) \). We have either \( b = a \), or \( b \neq a \) and \( b \notin \text{supp}(x) \). If \( b = a \) we have \( \text{supp}(([a]x)@b) = \text{supp}((ab) \cdot x) = \text{supp}(x) = \text{supp}([a]x) \cup \{a\} \). If \( b \neq a \) and \( b \notin \text{supp}(x) \), by Proposition 2.1, we obtain \( \text{supp}((ab) \cdot x) = (ab) \cdot \text{supp}(x) \subseteq \text{supp}(x) \setminus \{a\} \cup \{b\} = \text{supp}([a]x) \cup \{b\} \). \( \Box \)

Proposition 3.33. Let \( (D, \cdot, \sqsubseteq) \) be an invariant cpo and \( x, y \in D \). If \([a]x \sqsubseteq [A]D \) \([b]y \) for some \( a, b \in A \), then \([a]x@c \sqsubseteq ([b]y)@c \) for any \( c \in A \setminus \text{supp}([a]x, [b]y) \).

Proof. From the definition of concretion, we have \([a]x = [c](([a]x)@c) = [c](ac) \cdot x \) and \([b]y = [c]([b]y@c) = [c](bc) \cdot y \). Therefore, \([c](ac) \cdot x \sqsubseteq [A]D [c](bc) \cdot y \). According to Proposition 3.29, we obtain \((ac) \cdot x \sqsubseteq (bc) \cdot y \) as required. \( \Box \)

Theorem 3.48. Let \( (D, \cdot, \sqsubseteq) \) be an invariant cppo. Then \([A]D\) is an invariant cppo.

Proof. We have to prove that any finitely supported chain \(([a_n]x_n \mid n < \omega) \in [A]D\) has a least upper bound. Let us consider \( a \notin \text{supp}([a_n]x_n) \) for each \( n < \omega \). According to Proposition 3.33, we obtain another ascending chain \(([a_n]x_n)@a \mid n < \omega) \in D \). Since by Proposition 3.32 it holds \( \text{supp}(([a_n]x_n)@a) \subseteq \text{supp}([a_n]x_n) \cup \{a\} \) for all \( n < \omega \), we have that \( \text{supp}([a_n]x_n \mid n < \omega) \cup \{a\} \) supports the chain \(([a_n]x_n)@a \mid n < \omega) \). Since \( D \) is an invariant cpo, we obtain that \(([a_n]x_n)@a \mid n < \omega) \) has a least upper bound denoted by \( \sqcup \{([a_n]x_n)@a \mid n < \omega\} \). Hence \([a_n]x_n @a \sqsubseteq \sqcup \{([a_n]x_n)@a \mid n < \omega\} \) for each \( n < \omega \). Since \( \sqsubseteq \) is equivariant, we obtain \([a](([a_n]x_n)@a) \sqsubseteq [A]D [a] \sqcup \{([a_n]x_n)@a \mid n < \omega\} \) for each \( n < \omega \). Thus, \([a] \sqcup \{([a_n]x_n)@a \mid n < \omega\} \) is an upper bound for the chain \(([a_n]x_n \mid n < \omega) \in [A]D \). It remains to prove that \([a] \sqcup \{([a_n]x_n)@a \mid n < \omega\} \) is the least such upper bound. Suppose that there is another upper bound \([b]y \) such that \([a_n]x_n \sqsubseteq [A]D [b]y \) for all \( n < \omega \). We have to prove that \([a] \sqcup \{([a_n]x_n)@a \mid n < \omega\} \sqsubseteq [A]D [b]y \). Let us consider \( c \in A \setminus \text{supp}(ab, y, ([a_n]x_n \mid n < \omega)) \). We claim that \((ac) \cdot \sqcup \{([a_n]x_n)@a \mid n < \omega\} \sqsubseteq (bc) \cdot y \). Indeed, by Corollary 3.4 and Proposition 3.31, we have \((ac) \cdot \sqcup \{([a_n]x_n)@a \mid n < \omega\} = \sqcup \{((ac) \cdot ([a_n]x_n)@a) \mid n < \omega\} = \sqcup \{([a_n]x_n)@c \mid n < \omega\} \). Since \([b]y \) is an upper bound and because of Proposition 3.33, we obtain \([a_n]x_n @c \sqsubseteq ([b]y)@c \). Therefore, \( \sqcup \{([a_n]x_n)@c \mid n < \omega\} \sqsubseteq (bc) \cdot y \). Therefore, \([a] \sqcup \{([a_n]x_n)@a \mid n < \omega\} \sqsubseteq [A]D [b]y \). \( \Box \)

Corollary 3.6. Let \( (D, \cdot, \sqsubseteq, \sqcup, \sqcap) \) be an invariant cppo. Then \([A]D\) is an invariant cppo.
Proof. According to Theorem 3.48, we have that $[A]D$ is an invariant cpo. Since $\bot$ is the least element in $D$, we obtain that for each $a \in A$ we have $[a] \bot$ is less than any element in $[A]D$ (see Proposition 3.29). Also, by Lemma 2.3, we obtain that $[a] \bot = [b] \bot$ for any $b \in A$. Thus, $[a] \bot$ is the least element in $[A]D$ for each $a \in A$. $\square$

3.3.7 Recursive Equations over CPOs

Programming languages abound, explicitly or implicitly, in recursive definitions of datatypes. The classical example is the type-free $\lambda$-calculus. To give a mathematical semantics for the $\lambda$-calculus is to find a mathematical structure $D$ such that terms of the $\lambda$-calculus can be interpreted as elements of $D$ in such a way that application in the calculus is interpreted by function application. Now consider the self-application term $\lambda x.xx$. By the usual condition for type-compatibility of a function with its argument, we remark that if the second occurrence of $x$ in $xx$ has type $D$, and the whole term $xx$ has type $D$, then the first occurrence must have (or be constructed as having) type $(D \to D)$. Thus, we must have $(D \to D) \cong D$.

If we view $(\cdot \to \cdot)$ as a functor $F : C^{op} \times C \to C$ over a suitable category $C$ of mathematical structures, then we have to find a fixed point of the functor $F$, i.e. an element $D \in C$ such that $D \cong F(D,D)$. Therefore, it is enough to find such a $D$ and an isomorphism $i : F(D,D) \to D$. The question is which solution to choose if there is more than one: we are interested in finding the solution which is canonical in some sense.

Solutions of recursive equations on domains in the ZF framework are presented in [1]. The results from [1] were translated into FSM in [141]. Such recursive equations were solved in [141] for the category of invariant pointed cpos. The following notion captures the idea of canonicity of solution.

Definition 3.43. The solution $(i,D)$ of the recursive equation $F(D,D) \cong D$ has the minimal fixing property\(^2\) if the least fixed point $fix(\varphi)$ of the strict finitely supported continuous function $\varphi \in (D \to D) \to (D \to D)$ defined by $\varphi(f) = i \circ F(f,f) \circ i^{-1}$ is the identity on $D$.

We consider the categories:

- $\text{Inv} - \text{Cpo}$: objects are invariant cpos and morphisms are equivariant functions between invariant cpos.
- $\text{Inv} - \text{Cpo}_{\bot}$: objects are invariant cppos and morphisms are strict, equivariant functions between invariant cppos.

Working in $\text{Inv} - \text{Cpo}$ is equivalent to working in the functor category $\text{Cpo}^I$ where $I$ is the category of finite subsets of $A$ and injections between them. Elements of $\text{Inv} - \text{Cpo}$ correspond to elements of $\text{Cpo}^I$ with reverse pullbacks.

\(^2\) In the original reference [141] this property is called minimal invariant property; however, we choose to change the definition in order not to overlap with the notion of invariant introduced in Definition 2.4.
Definition 3.44. A locally invariant continuous functor (LIC-functor)
\[ F : \text{Inv} - \text{Cpo}_\perp \to \text{Inv} - \text{Cpo}_\perp \]
is characterized by the following properties:

1. for each invariant cppo \( D \) we have that \( F(D) \) is an invariant cppo.
2. for each function \( f : D \to E \) we obtain a function \( F(f) \in F(D) \to F(E) \) preserving identities and composition such that the following conditions are satisfied:
   - given \( f \sqsubseteq g \) in \( D \to E \) we require \( F(f) \sqsubseteq F(g) \) in \( F(D) \to F(E) \).
   - for any finitely supported chain \( (f_n \mid n < \omega) \in D \to E \), \( F(\bigsqcup_{n<\omega} f_n) = \bigsqcup_{n<\omega} (F(f_n)) \).
   - for all \( \pi \in S_A \) and \( f \in D \to E \) we have \( \pi \cdot (F(f)) = F(\pi \cdot f) \).

Definition 3.45. A mixed-variance locally invariant continuous functor
\[ F : \text{Inv} - \text{Cpo}_{\perp}^{\text{op}} \times \text{Inv} - \text{Cpo}_\perp \to \text{Inv} - \text{Cpo}_\perp \]
is characterized by the following properties:

1. for each invariant cppos \( D \) and \( E \) we have that \( F(D,E) \) is an invariant cppo.
2. for each pair of functions \( (f,g) \in (E \to D) \times (D \to E) \) we obtain a function \( F(f,g) \in F(D,D) \to F(E,E) \) such that \( F(\text{id}_D, \text{id}_D) = \text{id}_{F(D,D)} \), and for \( f' \in E' \to E \) and \( g' \in E \to E' \) we have \( F(f',g') \circ F(f,g) = F(f \circ f', g' \circ g) \).

The following conditions have to be satisfied:
   - given \( f \sqsubseteq f' \in E \to D \) and \( g \sqsubseteq g' \in D \to E \) we require \( F(f,g) \sqsubseteq F(f',g') \in F(D,D) \to F(E,E) \).
   - for any finitely supported chain \( ((f_n,g_n) \mid n < \omega) \in (E \to D) \times (D \to E) \), \( F(\bigsqcup_{n<\omega} f_n, \bigsqcup_{n<\omega} g_n) = \bigsqcup_{n<\omega} (F(f_n,g_n)) \).
   - for all \( \pi \in S_A \) and functions \( (f,g) \in (E \to D) \times (D \to E) \) we have \( \pi \cdot (F(f,g)) = F(\pi \cdot f, \pi \cdot g) \).

Some examples of LIC functors on the category \( \text{Inv} - \text{Cpo}_\perp \) are presented in Lemma 4.4.6 from [141]. The following theorem (which is the analogue of Theorem 5.3.7 from [1] in FSM) provides a solution of the recursive equation on invariant cppos. For a complete proof, see Theorem 4.5.2 from [141].

Theorem 3.49 ([141]). Let us consider a locally invariant continuous functor \( F : \text{Inv} - \text{Cpo}_{\perp}^{\text{op}} \times \text{Inv} - \text{Cpo}_\perp \to \text{Inv} - \text{Cpo}_\perp \). Then there exists a solution \( (i,D) \) of the recursive equation \( D \cong F(D,D) \) satisfying the minimal fixing property which is unique up to an isomorphism.

3.4 Groups in Finitely Supported Mathematics

The aim of this section is to study the notion of “group” in FSM. We define “invariant groups” and present also some properties of this new concept. The analogy between the properties of groups obtained in the framework of invariant sets and
those obtained in the usual ZF framework is also discussed. We focus on the study of invariant homomorphisms and present several FSM correspondence, isomorphism and embedding theorems in terms of finitely supported objects. The results in this section are an extension of the papers [14, 23].

### 3.4.1 Basic Results

We present groups in FSM in terms of finitely supported objects. Invariant groups have already been introduced in Definition 3.20.

**Definition 3.46.** Let \((G, \cdot, \diamond)\) be an invariant group. We say that \(H \subseteq G\) is an invariant subgroup of \(G\) if the following conditions are satisfied:

1. \((H, \cdot)\) is a group.
2. \((H, \diamond)\) is an invariant set.
3. for all \(\pi \in S_A\) and each \(x, y \in H\) we have \(\pi \diamond (x \cdot y) = (\pi \diamond x) \cdot (\pi \diamond y)\).

Let \((G, \cdot, \diamond)\) be an invariant group. If \(H\) is an invariant subgroup of \(G\) we denote this by \(H \leq G\). If \(H\) is an invariant normal subgroup of \(G\) we denote this by \(H \triangleleft G\).

Informally, a subgroup \(H\) of an invariant group \((G, \cdot, \diamond)\) is an invariant subgroup of \(G\) if and only if we obtain an \(S_A\)-action on \(H\) by restricting the domain of the action \(\diamond\) to \(S_A \times H\). The following lemma is trivial.

**Lemma 3.6.** Let \((G, \cdot, \diamond)\) be an invariant group. A subgroup \(H \leq G\) is an invariant subgroup of \(G\) if and only if for each \(\pi \in S_A\) and each \(h \in H\) we have \(\pi \diamond h \in H\).

**Remark 3.9.** Let \((G, \cdot, \diamond)\) be an invariant group and \(H \subseteq G\). Then \(\pi \diamond H\), which is defined as in Subsection 2.4.1, coincides with \(H\) for all \(\pi \in S_A\). Indeed, by Lemma 3.6, we have \(\pi \diamond H \subseteq H\) for all \(\pi \in S_A\). If \(h \in H\) we have \(h = \pi \diamond (\pi^{-1} \diamond h) \in \pi \diamond H\). Hence \(H \subseteq \pi \diamond H\), and \(\pi \diamond H = H\).

**Proposition 3.34.** Let \((G, \cdot, \diamond)\) be an invariant group. The centre of \(G\) is \(Z(G) = \{g \in G | g \cdot x = x \cdot g \text{ for all } x \in G\}\). We have that \(Z(G)\) is an invariant subgroup of \(G\).

**Proof.** From general group theory, \(Z(G)\) is a subgroup of \(G\). As stated in Lemma 3.6, it remains to prove that \(\pi \diamond g \in Z(G)\) for all \(\pi \in S_A\) and \(g \in Z(G)\). Let \(\pi \in S_A\), \(g \in Z(G)\) and \(x \in G\). We have \((\pi \diamond g) \cdot x = (\pi \diamond g) \cdot ((\pi \diamond \pi^{-1}) \diamond x) = (\pi \diamond g) \cdot (\pi \diamond (\pi^{-1} \diamond x)) = \pi \diamond (g \cdot (\pi^{-1} \diamond x)) = \pi \diamond ((\pi^{-1} \diamond x) \cdot g) = ((\pi \diamond \pi^{-1}) \diamond x) \cdot (\pi \diamond g) = x \cdot (\pi \diamond g)\). Therefore, \(\pi \diamond g \in Z(G)\).

**Proposition 3.35.** Let \((G, \cdot, \diamond)\) be an invariant group and \(H\) an invariant subgroup of \(G\). The centralizer of \(H\) in \(G\) is \(C_G(H) = \{g \in G | g \cdot h = h \cdot g \text{ for all } h \in H\}\). We have that \(C_G(H)\) is an invariant subgroup of \(G\).

**Proof.** From general group theory, we know that \(C_G(H)\) is a subgroup of \(G\). According to Lemma 3.6, we have to prove that \(\pi \diamond g \in C_G(H)\) for all \(\pi \in S_A\) and
Proof. Let \( \pi \in S_A, g \in C_G(H) \) and \( h \in H \). Then \( \pi^{-1} \circ h \in H \). We have
\[
(\pi \circ g) \cdot h = (\pi \circ g) \cdot ((\pi \circ \pi^{-1}) \circ h) = (\pi \circ g) \cdot (\pi \circ (\pi^{-1} \circ h)) = (\pi \circ g \cdot (\pi^{-1} \circ h))
\]
and
\[
\pi^{-1} \circ h \in H \quad \pi \circ ((\pi^{-1} \circ h) \cdot g) = ((\pi \circ \pi^{-1}) \circ h) \cdot (\pi \circ g) = h \cdot (\pi \circ g).
\]
Thus, \( \pi \circ g \in C_G(H) \).

\[\Box\]

**Proposition 3.36.** Let \((G, \cdot, \circ)\) be an invariant group and \( H \) an invariant subgroup of \( G \). The normalizer of \( H \) in \( G \) is \( N_G(H) = \{ g \in G | g^{-1} \cdot H \cdot g = H \} \). We have that \( N_G(H) \) is an invariant subgroup of \( G \).

**Proof.** We know that \( N_G(H) \) is a subgroup of \( G \). According to Lemma 3.6, it remains to prove that \( \pi \circ g \in N_G(H) \) for all \( \pi \in S_A \) and \( g \in N_G(H) \). Let \( \pi \in S_A \) and \( g \in N_G(H) \). Since \( H \) is an invariant subgroup of \( G \), we obtain \( \pi \circ H = H \). We have
\[
(\pi \circ g)^{-1} \cdot H \cdot (\pi \circ g) = (\pi \circ g)^{-1} \cdot (\pi \circ H) \cdot (\pi \circ g) = \pi \circ (g^{-1} \cdot H \cdot g) = \pi \circ H = H.
\]
Hence \( \pi \circ g \in N_G(H) \).

\[\Box\]

**Proposition 3.37.** Let \((G, \cdot, \circ)\) be an invariant group and \( H, K \) invariant subgroups of \( G \). The commutator subgroup \([H, K]\) is the subgroup generated by all the commutators \([h, k] = h^{-1} \cdot k^{-1} \cdot h \cdot k \) with \( h \in H \) and \( k \in K \). We have that \([H, K]\) is an invariant subgroup of \( G \).

**Proof.** Indeed \([H, K]\) is a subgroup of \( G \). According to Lemma 3.6, it remains to prove that \( \pi \circ g \in [H, K] \) for all \( \pi \in S_A \) and \( g \in [H, K] \). From the distributivity property of \( \circ \) and from the definition of the commutator subgroup, it is enough to prove that \( \pi \circ [h, k] \) is a commutator for all \( \pi \in S_A \) and all \( h \in H, k \in K \). Let \( \pi \in S_A, h \in H, k \in K \). We have \( \pi \circ [h, k] = \pi \circ (h^{-1} \cdot k^{-1} \cdot h \cdot k) = [\pi \circ h, \pi \circ k] \). This means \([H, K]\) is an invariant subgroup of \( G \).

The particular subgroup \([G, G]\) (usually denoted by \( G' \) or \( D(G) \)) called the derived subgroup of \( G \) is an invariant subgroup of \( G \).

**Proposition 3.38.** Let \((G, \cdot, \circ)\) be an invariant group and \( H, K \) invariant subgroups of \( G \). Then \( H \cap K \) is an invariant subgroup of \( G \).

**Proof.** From general group theory, we know that \( H \cap K = \{ g \in G | g \in H \text{ and } g \in K \} \) is a subgroup of \( G \). According to Lemma 3.6, it remains to prove that \( \pi \circ g \in H \cap K \) for all \( \pi \in S_A \) and \( g \in H \cap K \). Let \( \pi \in S_A \) and \( g \in H \cap K \). We have \( \pi \circ g \in H \) because \( H \) is an invariant subgroup of \( G \), and \( \pi \circ g \in K \) because \( K \) is an invariant subgroup of \( G \). Therefore, \( \pi \circ g \in H \cap K \).

\[\Box\]

**Proposition 3.39.** Let \((G, \cdot, \circ)\) be an invariant group and \( H, K \) invariant subgroups of \( G \) with \( HK = KH \). Then \( HK \) is an invariant subgroup of \( G \).

**Proof.** From the general theory of groups, we know that \( HK = \{ h \cdot k | h \in H, k \in K \} \) is a subgroup of \( G \) when the condition \( HK = KH \) is satisfied. According to Lemma 3.6, it remains to prove that \( \pi \circ g \in HK \) for all \( \pi \in S_A \) and \( g \in HK \). Let \( \pi \in S_A \) and \( g \in HK \). This means that \( g = h \cdot k \) for some \( h \in H \) and \( k \in K \). From the definition of an invariant group, we have \( \pi \circ g = (\pi \circ h) \cdot (\pi \circ k) \). Since \( H \) and \( K \) are invariant subgroups of \( G \), we have \( \pi \circ h \in H \) and \( \pi \circ k \in K \). Therefore, \( \pi \circ g \in HK \).

\[\Box\]
Proposition 3.40. Let \((G_1, \cdot, \circ_1), (G_2, \cdot, \circ_2)\) be invariant groups and \(f : G_1 \to G_2\) an equivariant homomorphism. Then the kernel of \(f\) is an invariant normal subgroup of \(G_1\).

Proof. From the theory of groups, we know that the kernel of \(f\) is \(\text{Ker} f = \{g \in G_1 | f(g) = 1\}\). We also know that \(\text{Ker} f\) is a normal subgroup of \(G_1\). According to Lemma 3.6, it remains to prove that \(\pi \circ_1 g \in \text{Ker} f\) for all \(\pi \in S_A\) and \(g \in \text{Ker} f\). Let \(\pi \in S_A\) and \(g \in \text{Ker} f\). We have \(f(g) = 1\). According to Corollary 2.3, we have \(f(\pi \circ_1 g) = \pi \circ_2 f(g) = \pi \circ_2 1\). However, \(1 = 1 \cdot 1\) and \(\pi \circ_2 1 = (\pi \circ_2 1) \cdot (\pi \circ_2 1)\) from the definition of an invariant group. We obtain \(\pi \circ_2 1 = 1\) and \(\pi \circ_1 g \in \text{Ker} f\). \(\square\)

Let \((G, \cdot)\) and \((H, \cdot)\) be two groups. Then \(G^H = \{f : H \to G\}\) is a group with respect to component-wise multiplication. Moreover, \(G^H\) is the direct product of \(|H|\) copies of \(G\). We can define an action of the group \(H\) on \(G^H\) by: \((h, \phi) \mapsto \phi^h \in G^H\), where \(\phi^h(x) = \phi(xh^{-1})\) for all \(x \in H\). According to this action, we have that \(H\) acts on \(G^H\) as a group in the sense of Definition 9.1 from [133]. The complete wreath product of \(G\) and \(H\) is the semi-direct product of \(H\) and \(G^H\), that is, the set \(\{(h, \phi) | h \in H, \phi \in G^H\}\) with multiplication given by \((h, \phi)(k, \psi) = (hk, \phi^k \psi)\). For each function \(f : H \to G\) we define \(S_f = \{x \in H | f(x) \neq 1\}\). Let \(G^{[H]} \overset{\text{def}}{=} \{f \in G^H | S_f \text{ is finite}\}\). Clearly, \(G^{[H]}\) is a subgroup of \(G^H\). The regular wreath product of \(G\) and \(H\) (denoted by \(G \wr H\)) is defined as the semi-direct product of \(H\) and \(G^{[H]}\), that is, the set \(\{(h, \phi) | h \in H, \phi \in G^{[H]}\}\) with multiplication given by \((h, \phi)(k, \psi) = (hk, \phi^k \psi)\).

Proposition 3.41. If \((G, \cdot, \circ)\) and \((H, \cdot, \circ)\) are invariant groups, then \((G^{[H]}, \cdot, \circ, \star)\) is an invariant group with the \(S_A\)-action \(\star : S_A \times G^{[H]} \to G^{[H]}\) defined by: \((\pi \star \phi)(x) = \pi \circ (\phi(\pi^{-1} \circ x))\).

Proof. Since \((G, \cdot, \circ)\) is an invariant group, we have that \(\pi \circ 1 = 1\) for all \(\pi \in S_A\). For each \(\phi \in G^{[H]}\) we have that \(S_\phi\) is finite. Suppose there exists a \(\pi\) such that \(S_{\pi \circ \phi}\) is infinite, which means we have an infinite number of elements \(x\) for which \(\pi \circ (\phi(\pi^{-1} \circ x)) \neq 1\). Since \(x \mapsto \pi^{-1} \circ x\) is bijective, we obtain an infinite number of elements of the form \(\pi^{-1} \circ x\) for which \(\phi(\pi^{-1} \circ x) \neq 1\), which contradicts the assumption that \(S_\phi\) is finite. Therefore, \(S_{\pi \circ \phi}\) is finite for all \(\pi \in S_A\) and \(\phi \in G^{[H]}\), which means that \(\star\) is well defined. Let \(\phi \in G^{[H]}\) such that \(S_\phi = \{a_1, \ldots, a_n\}\). We claim that \(S = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_n) \cup \text{supp}(\phi(a_1)) \cup \ldots \cup \text{supp}(\phi(a_n))\) supports \(\phi\). Let \(\pi \in \text{Fix}(S)\). We have to prove that \(\phi(\pi \circ x) = \pi \circ \phi(x)\), \(\forall x \in H\). If \(x \notin S_\phi\), the things are clear. If \(x \notin S_\phi\), then \(\phi(x) = 1\) and \(\pi \circ \phi(x) = 1\). Suppose \(\phi(\pi \circ x) \neq 1\). Then \(\pi \circ x \in S_\phi\), and there exists \(y \in S_\phi\) such that \(x = \pi^{-1} \circ y\). However, \(\pi\) fixes the support of \(y\) pointwise, and, since \(\pi\) is bijective, it follows that \(\pi^{-1}\) fixes the support of \(y\) pointwise, which means \(\pi^{-1} \circ y = y\). We obtain \(x \in S_\phi\) which contradicts our assumption that \(x \notin S_\phi\). Therefore, \(\phi(\pi \circ x) = 1\). Now we have to prove that \(\pi \circ (\phi \psi) = (\pi \circ \phi)(\pi \circ \psi)\), for all \(\pi \in S_A\), and \(\phi, \psi \in G^{[H]}\). This follows by easy calculation from the distributivity property of \(\circ\) over \(\cdot\). \(\square\)

Lemma 3.7. Let \(k \in H\). Then \(\pi \circ \phi^k = (\pi \circ \phi)^{(\pi \circ k)}\) for each \(\pi \in S_A\).
Proof. Let \( x \in H \). We have \( (\pi \diamond \phi^k)(x) = \pi \circ (\phi^k(\pi^{-1} \cdot x)) = \pi \circ (\phi((\pi^{-1} \cdot x)k^{-1})) \). Also \((\pi \diamond \phi)^{(\pi \cdot k)}(x) = (\pi \diamond \phi)(x(\pi \cdot k)^{-1}) = (\pi \diamond \phi)(x(\pi \cdot k^{-1})) = \pi \circ (\phi((\pi^{-1} \cdot x)(\pi^{-1} \cdot (\pi \cdot k^{-1})))) = \pi \circ (\phi((\pi^{-1} \cdot x)k^{-1})). \) \( \square \)

**Theorem 3.50.** If \((G, \cdot, \circ)\) and \((H, \cdot, \circ)\) are invariant groups, then \(G \setminus H\) is an invariant group.

**Proof.** We define the \(S_A\)-action \( \alpha : S_A \times G \setminus H \to G \setminus H \) by \( \alpha(h, \phi) = (\pi \cdot h, \pi \cdot \phi) \), for all \( \pi \in S_A \) and \((h, \phi) \in G \setminus H\). According to Proposition 3.41 and the results in Section 2.4, we have that \((G \setminus H, \alpha)\) is an invariant set. It remains to prove that \( \pi \circ (h, \phi)(k, \psi) = (\pi \circ (h, \phi))(\pi \circ (k, \psi)) \) for all \( \pi \in S_A \) and \((h, \phi), (k, \psi) \in G \setminus H\). We have \( \pi \circ ((h, \phi)(k, \psi)) = \pi \circ (hk, \phi^k \psi) = (\pi \cdot (hk), \pi \cdot (\phi^k \psi)) = ((\pi \circ h)(\pi \circ k), (\pi \circ \phi)^{\pi \circ k}(\pi \circ \psi)). \) Also \((\pi \circ (h, \phi))(\pi \circ (k, \psi)) = (\pi \cdot h, \pi \cdot \phi)(\pi \cdot k, \pi \cdot \psi) = ((\pi \circ h)(\pi \circ k), (\pi \circ \phi)^{\pi \circ k}(\pi \circ \psi)). \) According to Lemma 3.7, we have \( \pi \circ ((h, \phi)(k, \psi)) = (\pi \circ (h, \phi))(\pi \circ (k, \psi)). \) \( \square \)

**Theorem 3.51.** Let \((G, \cdot, \circ)\) be an invariant group and \(H\) an invariant normal subgroup of \(G\). Then \(G/H = \{xH \mid x \in G\}\) is an invariant group.

**Proof.** From the general theory of groups, we know that \(G/H\) is a group. We define the function \( \star : S_A \times (G/H) \to (G/H) \) by \( \pi \star (xH) = (\pi \circ x)H \) for all \( \pi \in S_A \) and all \( xH \in G/H\).

We prove that \( \star \) is well defined (it does not depend on the chosen representatives for the equivalence classes modulo \(H\)) and is an \(S_A\)-action on \(G/H\). Let \(xH, yH \in G/H\) with \(xH = yH\). This means \(x \cdot y^{-1} \in H\). Since \(H\) is an invariant subgroup of \(G\), we have \(\pi \circ (x \cdot y^{-1}) \in H\). From the definition of an invariant group, we obtain \((\pi \circ x) \cdot (\pi \circ y)^{-1} \in H\). It follows that \((\pi \circ x)H = (\pi \circ y)H\). Therefore, \(\pi \star (xH) = \pi \star (yH)\) and \(\star \) is well defined. Since \(\circ\) satisfies the properties of an \(S_A\)-action on \(G\), it is clear that \(\star \) is an \(S_A\)-action on \(G/H\).

We prove that each element in \(G/H\) is finitely supported with respect to the \(S_A\)-action \(\star\). Let \(xH\) be an arbitrary element from \(G/H\). Since \(x \in G\), there exists a finite set \(S \subset A\) which supports \(x\). Let \(\pi \in \text{Fix}(S)\). We have \(\pi \star (xH) = (\pi \circ x)H = xH\), which means \(S\) supports \(xH\).

Finally, let us consider \(xH, yH \in G/H\). We have \(\pi \star (xH \cdot yH) = \pi \star ((x \cdot y)H) = ((\pi \circ x) \cdot (\pi \circ y))H = (\pi \circ x)H \cdot (\pi \circ y)H = (\pi \star (xH)) \cdot (\pi \star (yH))\).

We conclude that \((G/H, \cdot, \star)\) is an invariant group. \( \square \)

### 3.4.2 Isomorphism Theorems

In this section we translate the usual correspondence and isomorphism theorems for groups into FSM.

**Theorem 3.52 (FSM correspondence theorem).** Let \((G, \cdot, \circ)\) and \((G', \cdot, \circ)\) be invariant groups and \(f : G \to G'\) an equivariant homomorphism of groups. Then:

1. \(H \leq_i G \Rightarrow f(H) \leq_i G'\).
2. \(H' \leq i G' \Rightarrow f^{-1}(H') \leq i G\).
3. \(H' \ll i G' \Rightarrow f^{-1}(H') \ll i G\).

If \(f\) is an equivariant epimorphism, then:
1'. \(H \ll i G \Rightarrow f(H) \ll i G'\).
2'. \(H \leq i G\) and \(\ker f \subseteq H\) imply \(H = f^{-1}(f(H))\).
3'. \(H' \leq i G' \Rightarrow f(f^{-1}(H')) = H'\).
4'. There exists an equivariant bijection between the invariant set of invariant subgroups of \(G\) containing \(\ker f\) and the invariant set of invariant subgroups of \(G'\).
5'. There exists an equivariant bijection between the invariant set of invariant normal subgroups of \(G\) containing \(\ker f\) and the invariant set of invariant normal subgroups of \(G'\).

Proof. The assertions at items 1, 2, 3, 1', 2' and 3' follow by easy calculation using the general theory of groups (see Chapter 3 in [133]). All we have to prove is the property of invariance for \(f(H)\) and \(f^{-1}(H')\), respectively. Let \(H \leq i G\). We prove that \(f(H) \leq G\) is indeed an invariant subgroup. According to Lemma 3.6, we must prove that \(\pi \circ x \in f(H)\) for all \(\pi \in S_A\) and \(x \in f(H)\). Let \(\pi \in S_A\) and \(x \in f(H)\). There exists \(h \in H\) such that \(x = f(h)\). Since \(f\) is equivariant, by Corollary 2.3, we have \(\pi \circ x = \pi \circ f(h) = f(\pi \circ h) \in f(H)\). Hence \(f(H)\) is an invariant subgroup of \(G'\).

Now let \(H' \ll i G'\). We prove that \(f^{-1}(H') \leq G\) is indeed an invariant subgroup. According to Lemma 3.6, we must prove that \(\pi \circ x \in f^{-1}(H')\) for all \(\pi \in S_A\) and \(x \in f^{-1}(H')\). Let \(\pi \in S_A\) and \(x \in f^{-1}(H')\). We have \(f(x) \in H'\). Since \(f\) is equivariant, by Corollary 2.3, we have \(f(\pi \circ x) = \pi \circ f(x) \in H'\). Therefore, \(\pi \circ x \in f^{-1}(H')\), and \(f^{-1}(H')\) is an invariant subgroup of \(G\).

We prove item 4'. As in Subsection 2.4.1, the sets \(A = \{H \mid H \leq i G, \ker f \subseteq H\}\) and \(B = \{H' \mid H' \ll i G'\}\) are \(S_A\)-sets. According to Remark 3.9, each element in these sets is equivariant. Therefore, \(A\) and \(B\) are invariant sets. We define \(\psi : A \rightarrow B\) by \(\psi(H) = f(H)\) for all \(H \in A\). From 1, it follows that \(\psi\) is well defined. From 2', it follows that \(\psi\) is one-to-one. From 2 and 3', it follows that \(\psi\) is onto. We have to prove that \(\psi\) is equivariant. Let \(\pi \in S_A\) and \(H \in A\). According to Remark 3.9, we have \(\psi(\pi \circ H) = \psi(H) = f(H) = \pi \circ f(H) = \pi \circ \psi(H)\). Hence, by Corollary 2.3, we have that \(\psi\) is equivariant.

Corollary 3.7. Let \((G, \cdot, \circ)\) be an invariant group and \(H \ll i G\). Then for each subgroup \(K' \leq i G/H\) there exists a unique subgroup \(K \leq i G\) with \(H \subseteq K\) such that \(K' = K/H\).

Proof. Since \(H \ll i G\), we have that \(G/H\) is an invariant group with the \(S_A\)-action \(\ast : S_A \times (G/H) \rightarrow (G/H)\) defined by \(\pi \ast (xH) = (\pi \circ x)H\) for all \(\pi \in S_A\) and all \(xH \in G/H\). Let us consider the canonical surjection \(p : G \rightarrow G/H\) defined by \(p(x) = xH\) for all \(x \in G\). We have \(p(\pi \circ x) = (\pi \circ x)H = \pi \ast (xH) = \pi \ast p(x)\) for all \(\pi \in S_A\) and \(x \in G\). Therefore, \(p\) is equivariant. Also \(\ker p = H\). According to Theorem 3.52(4'), for each \(K' \leq i G/H\) there exists a unique subgroup \(K \leq i G\) with \(\ker p = H \subseteq K\) such that \(p(K) = K'\). However, \(p(K) = K/H\) and the proof is complete.

According to Theorem 3.52(5'), we can prove analogously the following result.
Corollary 3.8. Let \((G, \cdot, \circ)\) be an invariant group and \(H <_i G\). Then for each subgroup \(K' <_i G/H\) there exists an unique normal subgroup \(K <_i G\) with \(H \subseteq K\) such that \(K' = K/H\).

Corollary 3.9. Let \((G, \cdot, \circ)\) be an invariant group, \(H <_i G\) and \(K \leq_i G\). We have \(K <_i G\) if and only if \(K/H <_i G/H\).

Proof. Let us suppose that \(K <_i G\). According to Theorem 3.52(1'), we have \(p(K) <_i p(G)\) where \(p\) is the natural surjection of \(G\) onto \(G/H\). Therefore, \(K/H <_i G/H\). Conversely, let us suppose that \(K/H <_i G/H\). According to Theorem 3.52(3), we have \(p^{-1}(K/H) <_i G\). It is easy to check that \(p^{-1}(K/H) = K\). \(\square\)

Theorem 3.53 (First FSM isomorphism theorem). Let us consider the invariant groups \((G, \cdot, \circ)\) and \((H, \cdot, \circ)\) and an equivariant homomorphism \(f : G \to H\). Then there exists an equivariant isomorphism between the invariant groups \(G/Ker f\) and \(Im f\).

Proof. From Proposition 3.40, we know that \(Ker f\) is an invariant normal subgroup of \(G\). From Theorem 3.51, we know that \(G/Ker f\) is an invariant group with the \(S_A\)-action \(* : S_A \times (G/Ker f) \to (G/Ker f)\) by \(\pi * (xKer f) = (\pi \circ x)Ker f\) for all \(\pi \in S_A\) and all \(xKer f \in G/Ker f\). In order to prove that \(Im f\) is an invariant group it is enough to prove that \(Im f\) is an invariant subgroup of \(H\). Let \(h \in Im f\). Then there exists \(g \in G\) such that \(f(g) = h\). Let \(\pi \in S_A\). Since \(f\) is equivariant, by Corollary 2.3, we have \(\pi \circ h = \pi \circ f(g) = f(\pi \circ g) \in Im f\). As in the general theory of groups we can define an isomorphism \(\varphi\) between \(G/Ker f\) and \(Im f\) by \(\varphi(xKer f) = f(x)\). We must prove that \(\varphi\) is equivariant. Let \(\pi \in S_A\) and \(xKer f \in G/Ker f\). Since \(f\) is equivariant, we have \(\varphi(\pi * (xKer f)) = \varphi((\pi \circ x)Ker f) = f(\pi \circ x) = \pi \circ f(x) = \pi \circ \varphi(xKer f)\). Hence, by Corollary 2.3, we obtain that \(\varphi\) is equivariant. \(\square\)

Theorem 3.54 (Second FSM isomorphism theorem). Let \((G, \cdot, \circ)\) be an invariant group, \(H <_i G\) and \(K <_i G\) with \(H \subseteq K\). Then there exists an equivariant isomorphism between the invariant groups \((G/H)/(K/H)\) and \(G/K\).

Proof. According to Corollary 3.9, we have that \(K/H <_i G/H\). Thus, \((G/H)/(K/H)\) is a well-defined invariant group (Theorem 3.51). Let us define \(f : G/H \to G/K\), \(f(xH) = xK\) for all \(xH \in G/H\). As in the standard theory of groups we prove that \(f\) is a well-defined surjective homomorphism with \(Ker f = K/H\). Moreover, \(f\) is equivariant because for all \(\pi \in S_A\) and \(xH \in G/H\) we have \(f(\pi * (xH)) = f((\pi \circ x)H) = (\pi \circ x)K = \pi * (xK) = \pi * f(xH)\). According to Theorem 3.53, we obtain an equivariant homomorphism between \((G/H)/(K/H)\) and \(G/K\). \(\square\)

Theorem 3.55 (Third FSM isomorphism theorem). Let \((G, \cdot, \circ)\) be an invariant group, \(H <_i G\) and \(K \leq_i G\). There exists an equivariant isomorphism between the invariant groups \(K/(H \cap K)\) and \((KH)/H\).

Proof. Since \(H\) and \(K\) are invariant subgroups of \(G\), we obtain that \(H \cap K\) is an invariant subgroup of \(G\). Therefore, \(H \cap K\) is an invariant subgroup of \(K\) (Proposition 3.38). A trivial calculation shows us that \(H \cap K < K\). Hence \(K/(H \cap K)\) is
an invariant group. Since \( H \triangleleft G \), we obtain \( HK = KH \). According to Proposition 3.39, it follows that \( KH \) is an invariant group. It is easy to check that \( H \triangleleft KH \), and so \((KH)/H\) is a well-defined invariant group. Let us define \( f : K \to (KH)/H \), \( f(k) = kH \) for all \( k \in K \). As in the general theory of groups we prove that \( f \) is a surjective homomorphism of groups whose kernel is \( \text{Ker} f = H \cap K \). Moreover, \( f \) is equivariant because for all \( \pi \in S_A \) and \( k \in K \) we have \( f(\pi \circ k) = (\pi \circ k)H = \pi \ast (kH) = \pi \ast f(k) \). According to Theorem 3.53, we obtain an equivariant homomorphism between \( K/(H \cap K) \) and \((KH)/H\).

\[ \Box \]

### 3.4.3 Embedding Theorems

**Definition 3.47.** An invariant set \((X, \cdot)\) is a **uniform invariant set** if there exists a finite set \( S \) such that all the elements of \( X \) are supported by \( S \).

For example each invariant finite set of form \( \{a_1, \ldots, a_n\} \) is a uniform invariant set with \( S = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_n) \). A set in which all the elements are equivariant is also an invariant uniform set with \( S = \emptyset \).

**Definition 3.48.** An invariant group \((G, \cdot, \circ)\) is a **uniform invariant group** if \((G, \circ)\) is a uniform invariant set.

**Proposition 3.42.** Let \((X, \cdot)\) be a uniform invariant set. The group \( S_X = \{f : X \to X \mid f \text{ bijective}\} \) is a uniform invariant group.

**Proof.** According to Proposition 2.3, we know that \( X^X \) is an \( S_A \) set with the \( S_A \) action \( \ast : S_A \times X^X \to X^X \) defined by \((\pi \ast f)(x) = \pi \cdot (f(\pi^{-1} \cdot x))\) for all \( \pi \in S_A \), \( f \in X^X \) and \( x \in X \). We prove that each element from \( X^X \) is finitely supported. A function \( f : X \to X \) is finitely supported in the sense of Definition 2.7 if and only if it is finitely supported with respect to the permutation action \( \ast \). Let \( f : X \to X \) be a function. We know that there exists a finite set \( S \) such that all the elements in \( X \) are supported by \( S \). We want to prove that \( S \) supports \( f \). Let \( \pi \in \text{Fix}(S) \). In the view of Proposition 2.4, to prove that \( \pi \ast f = f \) it is sufficient to prove that \( f(\pi \cdot x) = \pi \cdot f(x) \) for each \( x \in X \). However, \( S \) supports each element in \( X \). Since \( \pi \in \text{Fix}(S) \), we have \( \pi \cdot x = x \) and \( \pi \cdot f(x) = f(x) \) for each \( x \in X \). Therefore, \( S \) supports \( f \). It follows that \( X^X \) is an invariant set. We prove that \( S_X \) is an invariant group with the usual composition of functions. It is clear that \((S_X, \circ)\) is a group (where \( \circ \) represents the usual composition of functions). We must prove that for each \( f, g \in S_X \) we have \( \pi \ast (f \circ g) = (\pi \ast f) \circ (\pi \ast g) \). Indeed, for each \( x \in X \), we have \( (\pi \ast (f \circ g))(x) = \pi \cdot (f(\pi^{-1} \cdot x)) \). Also, if we denote \( (\pi \ast f)(y) = y \) we have \( y = \pi \cdot (g(\pi^{-1} \cdot y)) \) and \( ((\pi \ast f) \circ (\pi \ast g))(x) = (\pi \ast f)(y) = \pi \cdot f(\pi^{-1} \cdot y) = \pi \cdot f((\pi^{-1} \circ \pi) \cdot g(\pi^{-1} \cdot x)) = \pi \cdot (f(g(\pi^{-1} \cdot x))). \)

To prove that \( S_X \) is an invariant group it remains to prove that \( S_X \) is an invariant set. For this we must prove that \( \ast_{S_X} \) (where \( \ast_{S_X} \) represents the restriction of the function \( \ast \) to \( S_A \times S_X \)) is an \( S_A \)-action on \( S_X \). All we have to do is to prove that the codomain of the action \( \ast_{S_X} \) is indeed \( S_X \). So we must prove that \( \pi \ast f \in S_X \) for each
\[ \pi \in S_A \] and each \( f \in S_X \). More precisely, we have to prove that whenever \( f : X \to X \) is bijective we have that \( \pi \ast f \) is also bijective for each \( \pi \in S_A \). Let \( \pi \in S_A \) and \( f : X \to X \) be a bijective function. Suppose that \( (\pi \ast f)(x) = (\pi \ast f)(y) \) for some \( x, y \in X \). Then \( \pi \cdot (f(\pi^{-1} \cdot x)) = \pi \cdot (f(\pi^{-1} \cdot y)) \), and so \( (\pi^{-1} \circ \pi) \cdot (f(\pi^{-1} \cdot x)) = (\pi^{-1} \circ \pi) \cdot (f(\pi^{-1} \cdot y)) \). Thus, \( f(\pi^{-1} \cdot x) = f(\pi^{-1} \cdot y) \), and so \( \pi^{-1} \cdot x = \pi^{-1} \cdot y \). Therefore \( x = y \), and \( \pi \ast f \) is one-to-one. Let us prove that \( \pi \ast f \) is onto. Let \( y \in X \) be an arbitrary element. Since \( f \) is onto, we can find an element \( z \in X \) such that \( f(z) = \pi^{-1} \cdot y \). Let \( x = \pi \cdot z \). We have \( (\pi \ast f)(x) = \pi \cdot (f(\pi^{-1} \cdot (\pi \cdot z))) = \pi \cdot (f(z)) = y \). Hence \( \pi \ast f \) is onto.

**Theorem 3.56.** Let \((G, \cdot, \diamond)\) be a uniform invariant group. Then there exists an equivariant isomorphism from \( G \) to an invariant subgroup of \( S_G \).

**Proof.** For each \( g \in G \) we consider the function \( f_g : G \to G \) defined by \( f_g(x) = g \cdot x \). Clearly, \( f_g \) is finitely supported by \( \text{supp}(g) \) for all \( g \in G \). Moreover, \( f_g \in S_G \) for each \( g \in G \). Let \( H = \{f_g \mid g \in G\} \). Clearly, \( H \) is a subgroup of \( S_G \). Moreover, by Lemma 3.6, we have that \( H \) is an invariant subgroup of \( S_G \). Indeed, if \( h \in H \), we have that \( h = f_{g'} \) for some \( g' \in G \). Let \( \pi \in S_A \). We have \( (\pi \ast h)(x) = \pi \circ (f_g(\pi^{-1} \cdot x)) = \pi \circ (g \cdot (\pi^{-1} \cdot x)) = \pi \circ (\pi \cdot (g \cdot x)) = f_{\pi \circ g}(x) \). Hence \( \pi \ast h \in H \).

Let \( T : G \to S_G \) be the function defined by \( T(g) = f_g \) for each \( g \in G \). As in the standard proof of Cayley’s theorem (see [133]) it can be proved (by direct calculation) that \( T \) is an injective group homomorphism whose image is \( H \). It remains to prove that \( T \) is equivariant. It is sufficient to prove that \( T(\pi \circ g) = \pi \ast T(g) \) for each \( g \in G \) and \( \pi \in S_A \) (where by \( \ast \) we denote the \( S_A \)-action on \( S_G \) defined in the proof of Proposition 3.42). However, \( T(\pi \circ g) = f_{\pi \circ g} \) and \( \pi \ast T(g) = \pi \ast f_g \). We have just proved that \( \pi \ast f_g = f_{\pi \circ g} \) for all \( \pi \in S_A \).

We present a form of the Cayley’s theorem for invariant groups which are not necessary uniform. Its proof is similar to the proof of Theorem 3.56; we just make the remark that if \( G \) is an invariant group, then the set of all finitely supported bijections on \( G \) is also an invariant group (the proof is similar to the proof of Proposition 3.42 and uses Proposition 2.1).

**Theorem 3.57 (Cayley’s theorem for invariant groups).** Let \((G, \cdot, \diamond)\) be an invariant group. There exists an equivariant isomorphism from \( G \) to an invariant subgroup of the invariant group of all finitely supported bijections on \( G \).

**Proof.** The required isomorphism is defined as \( T \) in the proof of Theorem 3.56. The definition of \( T \) makes sense because \( T(g) \) is supported by \( \text{supp}(g) \) for each \( g \in G \).

We are now able to give Cayley’s theorem for \( \mathbb{Z}_{\text{ext}}(\Sigma) \) in FSM.

**Corollary 3.10.** Let \( \Sigma \) be a possibly infinite invariant set. There exists an equivariant isomorphism from \( \mathbb{Z}_{\text{ext}}(\Sigma) \) to an invariant subgroup of the invariant group formed by all finitely supported bijections on \( \mathbb{Z}_{\text{ext}}(\Sigma) \).

From the proof of Theorem 3.57, we can present a similar theorem of Cayley-type for invariant monoids.
Theorem 3.58 (Cayley’s theorem for invariant monoids). Let \((X, +, \cdot)\) be an invariant monoid. There exists an equivariant isomorphism between \(X\) and an invariant submonoid of the invariant monoid formed by the finitely supported elements from \(X^X\).

According to Theorem 3.58, we have the following result of Cayley-type in the FSM framework for extended multisets.

Corollary 3.11. Let \(\Sigma\) be a possibly infinite invariant set. There exists an equivariant isomorphism between \(N_{\text{ext}}(\Sigma)\) and an invariant submonoid of the invariant monoid formed by the finitely supported elements from \((N_{\text{ext}}(\Sigma))^\text{ext}\).

Theorem 3.59. Let \((G, \cdot, \circ)\) be a uniform invariant group and \(H \leq G\). The core of the subgroup \(H\) in \(G\) is \(H_G\) defined by \(H_G = \bigcap_{g \in G^g} gHg^{-1}\). The next assertions follow:

1. \(H_G\) is the largest invariant normal subgroup of \(G\) contained in \(H\).
2. If we consider the action of \(G\) on \(\rho_s^H = \{xH \mid x \in G\}\), \(\alpha : G \times \rho_s^H \to \rho_s^H\) defined by \(\alpha(g, xH) = (g \cdot x)H\) for all \(g \in G\) and \(xH \in \rho_s^H\), \(\varphi_\alpha : G \to S_{G/\rho_s^H}\) the permutation representation of \(G\) corresponding to \(\alpha\), then \(\varphi_\alpha\) is equivariant and \(H_G = \ker \varphi_\alpha\).
3. There exists an equivariant isomorphism from \(G/H_G\) to an invariant subgroup of \(S_{G/\rho_s^H}\). In particular, when the index of \(H\) in \(G\) is \(n\) we have that the cardinality of \(G/H_G\) is equal to \(n\), and there exists an equivariant isomorphism from \(G/H_G\) to an invariant subgroup of \(S_n\).

Proof. For \(K \leq G\) and \(g \in G\) we denote by \(K^g\) the subgroup \(gKg^{-1}\) of \(G\). Therefore, \(H_G = \bigcap_{g \in G} H^g\). By easy calculations (see for example [133]) we obtain that \(H_G < G\) and \(H_G\) is the largest normal subgroup of \(G\) contained in \(H\). Also \(\ker \varphi_\alpha = \{g \in G \mid (g \cdot x)H = xH, \forall x \in G\} = \{g \in G \mid g \in H^{-1}, \forall x \in G\} = \bigcap_{x \in G} H^{-1} = H_G\). Since \(G\) is an invariant group, we have that \(G/\rho_s^H\) is an invariant set with the \(S_A\)-action \(\circ : G \times G/\rho_s^H \to G/\rho_s^H\) defined by \(\pi \circ (xH) = (\pi \cdot x)H\) for all \(\pi \in A\) and \(xH \in G/\rho_s^H\) (see the proof of Theorem 3.51). Since all the elements of \(G\) are supported by the same \(S\), it is clear that all the elements of \(G/\rho_s^H\) are supported by the same \(S\). According to Proposition 3.42, we obtain that \((S_{G/\rho_s^H}, \circ, \cdot, \ast)\) is an invariant group. To prove that \(\varphi_\alpha\) is equivariant we have to prove that \(\varphi_\alpha(\pi \circ g) = \pi \circ \varphi_\alpha(g)\) for all \(\pi \in A\) and \(g \in G\). Let \(g \in G\). For all \(xH \in G/\rho_s^H\) we have \(\varphi_\alpha(\pi \circ g)(xH) = (\pi \circ (g \cdot x)H) = \pi \circ ((\pi \cdot (g \cdot (\pi^{-1} \cdot x)))H) = (\pi \circ (g \cdot (\pi^{-1} \cdot x)))H = (\pi \circ (g \cdot \cdot x))H\). Hence \(\varphi_\alpha\) is equivariant. According to Proposition 3.40, we obtain that \(H_G = \ker \varphi_\alpha\) is an invariant subgroup of \(G\). According to Theorem 3.52, we obtain that \(\text{Im} \varphi_\alpha \leq S_{G/\rho_s^H}\). According to Theorem 3.53, we obtain that there exists an equivariant isomorphism between \(G/H_G = G/\ker \varphi_\alpha\) and \(\text{Im} \varphi_\alpha\). \(\square\)
3.4 Groups in Finitely Supported Mathematics

3.4.4 Finitely Supported Subgroups

In this section we present some properties of the family of all finitely supported subgroups of an invariant group in terms of invariant lattices and invariant domains.

Let \((P, \sqsubseteq)\) be a poset. A subset \(U\) of \(P\) is directed if it is non-empty and each pair of elements in \(U\) has an upper bound in \(U\). A poset \((D, \sqsubseteq)\) in which every directed subset has a supremum is called a directed-complete partial order, or dcpo for short. Let \(x\) and \(y\) be elements of a dcpo \((D, \sqsubseteq)\). We say that \(x\) approximates \(y\), and denote this by \(x \ll y\), if for all directed subsets \(U\) of \((D, \sqsubseteq)\) we have that \(y \sqsubseteq \sqcup U\) implies \(x \sqsubseteq u\) for some \(u \in U\). We say that \(x\) is compact if it approximates itself; the set of all compact elements in a dcpo \(D\) is denoted by \(K(D)\). We note that \(x \sqsubseteq y\) whenever \(x \ll y\), and \(x' \ll y'\) whenever \(x' \sqsubseteq x \ll y \sqsubseteq y'.\) We say that a subset \(B\) of a dcpo \((D, \sqsubseteq)\) is a basis for \((D, \sqsubseteq)\), if for every element \(x\) of \((D, \sqsubseteq)\) there exists a directed subset \(U\) of elements in \(B\) approximating \(x\), with \(\sqcup U = x\). The directness of \(U\) shows that whenever \(B\) is a basis for \((D, \sqsubseteq)\), for each element \(x\) in \(D\) we can say that the set of elements in \(B\) approximating \(x\) is directed, and \(x\) is the supremum of the directed set of elements in \(B\) approximating it. Using the definition of approximation and the previous result we conclude that for each dcpo \((D, \sqsubseteq)\) with a basis \(B\) we have that \(K(D) \subseteq B\). A dcpo is called a continuous domain if it has a basis. It is called an algebraic domain if it has a basis of compact elements. More details are in [1].

Let \((G, \cdot)\) be a group. If \(H\) is a subgroup of \(G\) we denote this by \(H \leq G\). If \(S \subseteq G\), we denote by \([S]\) the subgroup of \(G\) generated by \(S\), i.e. the smallest subgroup of \(G\) which contains \(S\). Every element of \([S]\) can be expressed as a finite product of elements of \(S\) and inverses of elements of \(S\). If \(S \subseteq G\) is finite and \(H = [S]\), we call \(H\) a finitely generated subgroup of \(G\). The set \(\mathcal{L}(G)\) of all subgroups of \(G\) ordered by inclusion forms a complete lattice. If \(\langle H_i \rangle_{i \in I}\) is a family of subgroups of \(G\), the infimum of this family is \(\bigcap_{i \in I} H_i\) and the supremum is \([\bigcup_{i \in I} H_i]\). Moreover, according to [1], we have that \((\mathcal{L}(G), \subseteq)\) is an algebraic domain and the compact elements in \((\mathcal{L}(G), \subseteq)\) are precisely those in \(F(\mathcal{L}(G))\), where \(F(\mathcal{L}(G))\) is the set of all finitely generated subgroups of a group \(G\).

We can reformulate some definitions from ZF domain theory in FSM while noting that in FSM only finitely supported objects are allowed.

**Definition 3.49.** An invariant poset \((D, \sqsubseteq, \cdot)\) in which every finitely supported directed subset has a supremum is called an invariant directed-complete partial order, or invariant dcpo for short.

**Definition 3.50.** Let \(x\) and \(y\) be elements of an invariant dcpo \((D, \sqsubseteq, \cdot)\). We say that \(x\) invariant approximates \(y\), and denote this by \(x \ll_{inv} y\), if for all finitely supported directed subsets \(U\) of \((D, \sqsubseteq, \cdot)\) we have that \(y \sqsubseteq \sqcup U\) implies \(x \sqsubseteq u\) for some \(u \in U\). We say that \(x\) is invariant compact if it invariant approximates itself; the set of all invariant compact elements in an invariant dcpo \(D\) is denoted by \(K(D)_{inv}\).

**Definition 3.51.** Let \((D, \sqsubseteq, \cdot)\) be an invariant dcpo.
1. We say that an invariant set $B \subseteq D$ is an invariant basis for $(D, \sqsubseteq, \cdot)$ if for every element $x$ of $(D, \sqsubseteq, \cdot)$ there exists a finitely supported directed subset $U$ of elements in $B$ approximating $x$ with $\sqcup U = x$.

2. $(D, \sqsubseteq, \cdot)$ is called an invariant continuous domain if it has an invariant basis.

3. $(D, \sqsubseteq, \cdot)$ is called an invariant algebraic domain if it has an invariant basis of invariant compact elements.

The following definition generalizes the notion of an invariant subgroup of an invariant group introduced in Definition 3.46.

**Definition 3.52.** Let $(G, \cdot, \circ)$ be an invariant group. A finitely supported subgroup of $G$ is a subgroup of $G$ which is finitely supported as an element of $\wp(G)$.

According to Definition 3.46, any invariant subgroup of an invariant group $G$ is a finitely supported subgroup of $G$ with empty support. Obviously, there may exist finitely supported subgroups of $G$ which are not invariant subgroups of $G$ in the sense of Definition 3.46.

If $(G, \cdot, \circ)$ is an invariant group, we denote by $\mathcal{L}(G)_{inv}$ the family of all finitely supported subgroups of $G$ ordered by inclusion.

**Lemma 3.8.** Let $(G, \cdot, \circ)$ be an invariant group and $F$ a finitely supported subset of $G$. Then $[F]$ is a finitely supported subgroup of $G$.

**Proof.** We claim that $[F]$ is supported by $\text{supp}(F)$. Indeed, let us consider $\pi \in \text{Fix}(\text{supp}(F))$. Let $x_1^{e_1} \cdot x_2^{e_2} \cdot ... \cdot x_n^{e_n}, x_i \in F, e_i = \pm 1, i = 1, ..., n$ be an arbitrary element from $[F]$. Since $\pi \in \text{Fix}(\text{supp}(F))$, we have $\pi \circ x_i \in F, \forall i \in \{1, ..., n\}$. Therefore, because the internal law on $G$ is equivariant, we have $\pi \circ (x_1^{e_1} \cdot x_2^{e_2} \cdot ... \cdot x_n^{e_n}) = (\pi \circ x_1^{e_1}) \cdot (\pi \circ x_2^{e_2}) \cdot ... \cdot (\pi \circ x_n^{e_n}) = (\pi \circ x_1)^{e_1} \cdot (\pi \circ x_2)^{e_2} \cdot ... \cdot (\pi \circ x_n)^{e_n} \in [F]$. Therefore, $\pi \ast [F] = [F]$, where $\ast$ is the $S_A$-action on $\wp(G)$ defined as in Subsection 2.4.1, and so $\text{supp}(F)$ supports $[F]$. $\Box$

**Corollary 3.12.** Let $(G, \cdot, \circ)$ be an invariant group and $F$ a finite subset of $G$. Then $[F]$ is a finitely supported subgroup of $G$.

**Proof.** Let $F = \{x_1, ..., x_n\}$ be a finite subset of $G$. Then $\text{supp}(x_1) \cup ... \cup \text{supp}(x_n)$ supports $F$. Thus, $F$ is finitely supported, and the result follows from Lemma 3.8. $\Box$

**Theorem 3.60.** Let $(G, \cdot, \circ)$ be an invariant group. Then $(\mathcal{L}(G)_{inv}, \sqsubseteq, \ast)$ is an invariant complete lattice, where $\sqsubseteq$ represents the usual inclusion relation on $\wp(G)$ and $\ast$ is the $S_A$-action on $\wp(G)$ defined as in Subsection 2.4.1.

**Proof.** We know that $\ast$ is the $S_A$-action on $\wp(G)$ defined as in Subsection 2.4.1. We claim that the restriction of $\ast$ to $\mathcal{L}(G)_{inv}$ is an $S_A$-action on $\mathcal{L}(G)_{inv}$, that is, the codomain of the restricted function $\ast|_{\mathcal{L}(G)_{inv}}$ is also $\mathcal{L}(G)_{inv}$. We have to prove that for any $\pi \in S_A$ we have that $\pi \ast H$ is a finitely supported subgroup of $G$ whenever $H$ is a finitely supported subgroup of $G$. Fix some $\pi \in S_A$ and $H \leq G$, $H$ finitely supported as a subset of $G$. Let $\pi \circ h_1$ and $\pi \circ h_2, h_1, h_2 \in H$ be two arbitrary elements...
Corollary 3.13. Let $(G, \cdot, \circ)$ be an invariant group. Then $(\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)$ is an invariant (pointed) dcpo and an invariant cppo.

According to Theorem 3.46, we have the following result.

Corollary 3.14. Let $(G, \cdot, \circ)$ be an invariant group. Each finitely supported continuous function $f : \mathcal{L}(G)_{\text{inv}} \rightarrow \mathcal{L}(G)_{\text{inv}}$ possesses a least fixed point $\text{fix}(f) = \bigcup_{n \in \mathbb{N}} \{e\}$, where $e$ is the identity element in $G$. Moreover, $\text{supp}(\text{fix}(f)) \subseteq \text{supp}(f)$.

Moreover, according to Theorem 3.34, we have the following Tarski-type result.

Corollary 3.15. Let $(G, \cdot, \circ)$ be an invariant group and let $f : \mathcal{L}(G)_{\text{inv}} \rightarrow \mathcal{L}(G)_{\text{inv}}$ be an equivariant, order-preserving function over $\mathcal{L}(G)_{\text{inv}}$. The set of all fixed points of the function $f$ form another invariant complete lattice.

Lemma 3.9. If $(H_i)_{i \in I}$ is a finitely supported directed family of finitely supported subgroups of $G$, then $\bigcup_{i \in I} H_i$ is a finitely supported subgroup of $G$, and $[\bigcup_{i \in I} H_i] = \bigcup_{i \in I} H_i$.

Proof. According to the proof of Theorem 3.60, because $(H_i)_{i \in I}$ is a finitely supported family of finitely supported subgroups of $G$, we have that $\bigcup_{i \in I} H_i$ is finitely supported.
supported in $\mathcal{P}(G)$. Now, let $x, y \in \bigcup H_i$. There are $i, j \in I$ such that $x \in H_i$ and $y \in H_j$. Because of the directness of $(H_i)_{i \in I}$ we can find $k \in I$ such that $H_k$ is an upper bound of both $H_i$ and $H_j$. This means that $x, y \in H_k$ and hence $xy^{-1} \in H_k \subseteq \bigcup H_i$.

We obtain that $\bigcup H_i$ is a finitely supported subgroup of $G$. \hfill \Box

**Proposition 3.43.** Let $(G, \cdot, \circ)$ be an invariant group. Each finitely generated subgroup of $G$ is invariant compact in $(\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)$.

**Proof.** Let $H \leq G$ be a finitely generated subgroup of $G$. Then $H = [F]$ where $F$ is a finite subset of $G$. According to Corollary 3.12, we have that $H$ is a finitely supported subgroup of $G$. This means $H \in \mathcal{L}(G)_{\text{inv}}$. Let $(H_i)_{i \in I}$ be a finitely supported directed family of finitely supported subgroups of $G$ with $H \subseteq \bigcup_{i \in I} H_i$.

According to Lemma 3.9, we have $H \subseteq \bigcup_{i \in I} H_i$, and so $F \subseteq H \subseteq \bigcup_{i \in I} H_i$. However, we remark that if a finite set $X$ is covered by a finitely supported directed family of finitely supported subsets $(X_i)_{i \in I}$, then $X$ will always be contained in some $X_i$. This is because, according to Theorem 2.20, the definitions of (1)-finiteness and (3)-finiteness are equivalent in FSM. Therefore, there exists $j \in I$ such that $F \subseteq H_j$. However, $[F] = \bigcap_{H \leq H'} F \subseteq H^j$, and hence $[F] \subseteq H_j$. This means exactly $H \leq_{\text{inv}} H$. \hfill \Box

**Lemma 3.10.** Let $(G, \cdot, \circ)$ be an invariant group. Let $\pi \in S_A$ and $F$ a finite subset of $G$. Then $\pi \ast [F] = [\pi \ast F]$, where $\ast$ is the $S_A$-action on $\mathcal{P}(G)$ defined as in Subsection 2.4.1.

**Proof.** According to Corollary 3.12, we have that $[F]$ is a finitely supported subgroup of $G$, and so the statement of the lemma makes sense in FSM. Let $x \in [F]$. Then $x = x_1^{e_1} \cdot x_2^{e_2} \cdots \cdot x_n^{e_n}$, $x_i \in F$, $e_i = \pm 1$, $i = 1, \ldots, n$. Therefore, because the internal law on $G$ is equivariant, we have $\pi \circ x = \pi \circ (x_1^{e_1} \cdot x_2^{e_2} \cdots \cdot x_n^{e_n}) = (\pi \circ x_1^{e_1}) \cdot (\pi \circ x_2^{e_2}) \cdots \cdot (\pi \circ x_n^{e_n}) = (\pi \circ x_1)^{e_1} \cdot (\pi \circ x_2)^{e_2} \cdots \cdot (\pi \circ x_n)^{e_n} \in [\pi \ast F]$. We get $\pi \ast [F] \subseteq [\pi \ast F]$. The reverse inclusion follows analogously. Thus, $\pi \ast [F] = [\pi \ast F]$. \hfill \Box

**Corollary 3.16.** Let $(G, \cdot, \circ)$ be an invariant group and let $F(\mathcal{L}(G))$ be the set of all finitely generated subgroups of a group $G$. Then $F(\mathcal{L}(G)) \subseteq \mathcal{L}(G)_{\text{inv}}$ and $F(\mathcal{L}(G))$ is also an invariant set.

**Proof.** According to Corollary 3.12, every finitely generated subgroup of $G$ is a finitely supported subgroup of $G$. Thus, $F(\mathcal{L}(G)) \subseteq \mathcal{L}(G)_{\text{inv}}$. In order to prove that $F(\mathcal{L}(G))$ is an invariant set it remains to prove that $\pi \ast [F]$ is finitely generated whenever $\pi \in S_A$ and $[F]$ is a finitely generated subgroup of $G$. According to Lemma 3.10, we have $\pi \ast [F] = [\pi \ast F]$. Since $F$ is finite, then $\pi \ast F$ is also finite, and so $\pi \ast [F]$ is finitely generated. \hfill \Box

**Proposition 3.44.** Let $(G, \cdot, \circ)$ be an invariant group and let $H$ be a finitely supported subgroup of $G$. Then the subgroups generated by the finite subsets of $H$ form a finitely supported directed family. Moreover, $H$ is the union of the subgroups generated by the finite subsets of $H$. 


Proof. Let \( A_H = \{ [F] \mid F \subseteq H \text{ and } F \text{ is finite} \} \). We have to prove that \( A_H \) is a finitely supported directed family and \( H = \bigcup_{H' \in A_H} H' \). First we prove that \( A_H \) is finitely supported. We claim that \( \text{supp}(H) \) supports \( A_H \). Indeed, let us consider \( \pi \in \text{Fix}(\text{supp}(H)) \). Let \( F' \) be an arbitrary finite subset of \( H \). According to Lemma 3.10, we have \( \pi \ast [F'] = [\pi \ast F'] \), where \( \ast \) is the \( S_A \)-action on \( \emptyset(G) \) defined as in Subsection 2.4.1. However, \( \pi \ast H = H \) because \( \pi \in \text{Fix}(\text{supp}(H)) \). Since \( F' \subseteq H \), from the definition of \( \ast \) we have \( \pi \ast F' \subseteq \pi \ast H = H \). Obviously \( \pi \ast F' \) is finite, and so \([\pi \ast F'] \subseteq A_H \). Thus, \( \pi \ast [F'] \subseteq A_H \), that is, \( \text{supp}(H) \) supports \( A_H \).

Let \([F_1] \in A_H \) and \([F_2] \in A_H \). Then \([F_1 \cup F_2] \in A_H \). Also \([F_1] = \bigcap_{H' \leq G} H' \). We know that \( F_1 \subseteq [F_1 \cup F_2] \) and so \([F_1] \subseteq [F_1 \cup F_2] \). Analogously \([F_2] \subseteq [F_1 \cup F_2] \). We obtained that \( A_H \) is directed.

Now let \( h \in H \). Then \( h \in \{ [h] \} \) and \( \{ [h] \} \in A_H \). Therefore, \( H \subseteq \bigcup_{H' \in A_H} H' \). For the reverse inclusion let \( F \) be a finite subset of \( H \). Since \([F] = \bigcap_{H' \leq G} H' \), we get \([F] \subseteq H \) and \( \bigcup_{H' \in A_H} H' \subseteq H \). \( \square \)

**Theorem 3.61.** Let \((G, \cdot, \cdot)\) be an invariant group. Then \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\) is an invariant continuous domain and an invariant basis in \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\) is precisely \( F(\mathcal{L}(G)) \).

Proof. By Corollary 3.16, we have that \( F(\mathcal{L}(G)) \) is an invariant set. For every finitely supported \( H \) of \( G \), we consider \( A_H = \{ [F] \mid F \subseteq H \text{ and } F \text{ is finite} \} \). Clearly, \( A_H \subseteq F(\mathcal{L}(G)) \). According to Proposition 3.44, we know that \( A_H \) is finitely supported and directed, and \( H = \bigcup_{H' \in A_H} H' \). According to Proposition 3.43, we know that whenever \([F] \in A_H \) we have \([F] \ll_{\text{inv}} [F] \subseteq H \) and hence (after a trivial calculation) \([F] \ll_{\text{inv}} H \). Using the definition of an invariant basis in an invariant dcpo (Definition 3.51) we obtain that \( F(\mathcal{L}(G)) \) is an invariant basis in \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\). \( \square \)

**Theorem 3.62.** Let \((G, \cdot, \cdot)\) be an invariant group. Then \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\) is an invariant algebraic domain and the family of all invariant compact elements in \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\) is precisely \( F(\mathcal{L}(G)) \).

Proof. Let \( H \) be an invariant compact element in \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\). Then \( H \ll_{\text{inv}} H \). The set \( A_H \) defined as in the proof of Proposition 3.44 is finitely supported and directed, and \( H = \bigcup_{K \in A_H} K \). Since \( H \ll_{\text{inv}} H \), there exists \( H' \in A_H \) such that \( H \subseteq H' \).

However, because \( H' \in A_H \) there exists a finite set \( F \subseteq H \) such that \( H' = [F] \). Since \( F \subseteq H \), we have \([F] \subseteq H \). Therefore, \( H' \subseteq H \), and so \( H' = H \). We obtain that \( H \in F(\mathcal{L}(G)) \).

Conversely, by Proposition 3.43, any finitely generated subgroup of \( G \) is invariant compact. Thus, a finitely supported subgroup of \( G \) is invariant compact if and only if it is finitely generated.

Since by Theorem 3.61, \( F(\mathcal{L}(G)) \) is an invariant basis in \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\), we obtain that \((\mathcal{L}(G)_{\text{inv}}, \subseteq, \ast)\) is an invariant algebraic domain. \( \square \)
3.5 General Comments

FM set theory is a more suitable framework for experimental sciences than ZF set theory. Therefore, translating ZF properties of several algebraic structures into such a framework deserves special attention. Rather than working with an alternative set theory we work in FSM, and present our results in terms of invariant sets.

Classical multisets over finite alphabets are extended in Section 3.1 to the framework of invariant sets. We define “extended multisets” over possibly infinite alphabets, presenting also some properties of this new concept. The analogy between the results obtained in FSM and those obtained according to the ZF axioms of set theory is emphasized by the results presented in Section 3.1. In Theorem 3.4 we proved that the set of all extended multisets over an invariant set $\Sigma$ is a free abelian invariant monoid, and it satisfies the universality property expressed in Theorem 3.5. The free monoid over $\Sigma$ is also an invariant monoid according to Theorem 3.6, and it satisfies the universality property presented in Theorem 3.7. By repeatedly applying these universality properties, a connection between the set of all extended multisets over $\Sigma$ and the free monoid over $\Sigma$ is emphasized first in the ZF approach, and second in the FSM approach, in terms of finitely supported homomorphisms. Several FSM order properties of multisets and extended multisets are presented in Proposition 3.5 and Theorem 3.12. The framework for studying multisets is again extended in Section 3.1.3 by the informal replacement of “equivariant” with “finitely supported”, that is, we consider a new class of multisets defined over finitely supported subsets of invariant sets instead of the class of those multisets defined on invariant sets. Several properties of the extended multisets of rank 1 are presented in Section 3.1.3.

The classical theory of invariant sets over a fixed set $A$ of atoms is generalized in [45] to a new theory of invariant sets over arbitrary unfixed sets of data values. The notion of ‘$S_A$-set’ is replaced by the notion of ‘set endowed with an action of a subgroup of the symmetric group of $D$’ for an arbitrary set of data values $D$, and the notion of ‘finite set’ is replaced by the notion of ‘set with a finite number of orbits according to the previous group action (orbit-finite set)’. The theory of automata has been studied in this framework [45]. According to definitions in [45], the set $A$ of atoms is a single-orbit set. However, the set $N_\text{ext}(A)$ has an infinite number of orbits because if two functions from $N_\text{ext}(A)$ are in the same orbit, then their corresponding algebraic supports must have the same cardinality. Therefore, we are able to develop an FSM theory of multisets even when the alphabet is possibly infinite and the set of all multisets over the related alphabet is not finite or orbit-finite. Informally, our approach extends the framework from ‘finite/orbit-finite’ to ‘infinite/orbit-infinite but with finite algebraic support’. However, a theory of invariant multisets over orbit-finite alphabets could be investigated. Presenting this in detail is future work. Bojanczyk introduces a notion of invariant (nominal) monoid over arbitrary data symmetries [42] in order to prove that a language of data words is definable in first-order logic if and only if its syntactic monoid is aperiodic. We have a slightly different perspective. The notion of invariant monoid introduced in Definition 3.7 makes sense only when the set of atoms is fixed, and invariant
monoids are used in order to obtain FSM properties of multisets and to connect several such FSM properties in terms of finitely supported homomorphisms. The notion of invariant monoid presented in Definition 3.7 is similar to the notion of invariant group analyzed in Section 3.4. Therefore, the correspondence, isomorphism and embedding theorems presented in Section 3.4 for invariant groups can be naturally rephrased for invariant monoids. Bojanczyk uses alternative definitions for invariant algebraic structures in his generalized framework of G-sets [45], in order to study languages of data words. We present the invariant algebraic structures in the classical framework of invariant sets in order to prove that several classical ZF properties of algebraic structures have analogues in FSM. Therefore, we focus on an algebraic study of invariant structures. Presenting isomorphism, embedding, fixed point, correspondence, decomposing and invariance-preserving theorems was not the object of Bojanczyk’s papers, and represent the original part of Chapter 3.

In Section 3.2 we define and study “generalized multisets” both in the ZF framework and in FSM. In Subsection 3.2.1 several algebraic properties of generalized multisets are presented. The central idea of this subsection is to prove that \( Z(\Sigma) \) is a finitely generated, lattice-ordered, free abelian group\(^3\). From this property of \( Z(\Sigma) \) and the general theory of groups, we get new properties of generalized multisets (see especially Theorems 3.17, 3.22 and 3.23). Some other order properties of \( Z(\Sigma) \) could also be obtained from the indicated references by particularizing to \( Z(\Sigma) \) some results from the general theory of l-groups. We also prove that \( Z(\Sigma) \) can be organized as a totally ordered group and we obtain some ordering properties for the free group on \( \Sigma \), \( F(\Sigma) \) (see Theorem 3.24). These properties of generalized multisets are discussed in some alternative mathematics such as Reverse Mathematics (see Subsection 3.2.1.3) and FSM (see Subsection 3.2.2). In Proposition 3.11 we proved that the set of all extended generalized multisets over \( \Sigma \) is an invariant set. Moreover, the set of all extended generalized multisets over \( \Sigma \) is a free abelian invariant group (Theorem 3.26), and it satisfies the universality property expressed in Theorem 3.27. The free group over \( \Sigma \) is also an invariant group according to Theorem 3.28, and it satisfies the universality property presented in Theorem 3.29. These results are also connected in FSM. An FSM embedding theorem of Cayley-type is proved for the set of extended generalized multisets over \( \Sigma \) using the results in Section 3.4 (Corollary 3.10).

Invariant posets and domains are studied in Section 3.3. An FSM theory for partially ordered sets was first developed by Pitts and Shinwell [141] in order to describe a denotational semantics for a functional programming language incorporating facilities for manipulating syntax involving names and binding operations. However, the main result of Subsection 3.3.1, a Tarski-type theorem concerning invariant complete lattices (Theorem 3.34), and the main results in Subsection 3.3.2 and Subsection 3.3.4 belong to the authors. Event structures are introduced in [114] as abstract representations of the behaviour of safe Petri nets. They describe a concurrent system by means of a set of events, representing action occurrences, and for every two events it is specified whether one of them is a prerequisite for the other.

\(^3\) Note that \( Z(\Sigma) \) is not a free l-group in the sense of Definition 2.1 from [158].
whether they exclude each other, or whether they may happen concurrently. Invariant event structures were described in [8] using the results from Section 3.3. The solution of the Scott recursive domain equation \( D \cong (D \rightarrow D) \) in the FSM approach is presented in Subsection 3.3.7.

Pawlak’s general theory of rough sets studies in the ZF framework the approximations of subsets of some finite sets. In Subsection 3.3.3 we define and study in FSM the approximations of finitely supported subsets of some possibly infinite invariant sets. In order to realize our goal we translate the algebraic structures of Galois connections into FSM, and we present their properties in terms of finitely supported objects. Invariant Galois connections are presented in Subsection 3.3.2. Using the results in Subsection 3.3.1 and Subsection 3.3.2 we are able to present invariant Pawlak’s approximations in terms of invariant Galois connections (Theorem 3.37). In the ZF framework, fixed points of Galois connections are important because definable sets may be viewed as fixed points of rough approximation mappings [94]. In FSM, according to Theorem 3.38, the set of all definable subsets of an invariant set \( U \) form an invariant complete Boolean sublattice of \( \mathcal{P}_{fs}(U) \). One benefit of using Pawlak’s approximation method on invariant sets is that we are able to define and study the approximations of some finitely supported subsets of a possibly infinite invariant set, while Pawlak [118] studied only the approximations of some finite subsets of a finite set. Informally, we can generalize the Pawlak’s approximation framework from “finite” to “infinite with finite support”. A second benefit is that we can prove that the theory of Pawlak approximations makes sense even when we work in a different framework of set theory.

In Subsection 3.3.4 we study the abstract interpretations of programming languages in the framework of invariant sets. FSM abstract interpretations are studied by means of invariant correctness relations, invariant representation functions and invariant Galois connections. A relationship between invariant correctness relations and invariant representation functions is presented in Theorem 3.39. According to Theorem 3.40, the invariant representation functions can be used in order to define invariant Galois connections. The techniques of widening and narrowing are used in Subsection 3.3.5 in order to approximate the least fixed points of certain finitely supported transition functions on invariant spaces of properties. By Subsection 3.3.5, the calculability results in the classical ZF theory of abstract interpretation also hold in the framework of invariant sets. Therefore, the theory of abstract interpretation is consistent in FSM.

Invariant groups are defined as groups which are also invariant sets and whose internal laws are equivariant. Several algebraic properties of invariant groups are presented in Subsection 3.4.1. In Subsection 3.4.2 the classical correspondence and isomorphism theorems from ZF group theory are translated into FSM in terms of equivariant homomorphisms. In Subsection 3.4.3 uniform invariant groups are defined, and several invariant embedding theorems valid for this class of groups are presented. The finitely supported subgroups of an invariant group are studied in terms of invariant lattices and invariant domains in Subsection 3.4.4. Invariant groups are, actually, the natural extension of invariant monoids. However, the presence of inverse elements in a group allows us to think about the study of reversibility
in terms of invariant sets. In this book we present an algebraic framework for such a future development. The wreath product and one of its generalizations are used in the algebraic theory of automata in order to prove the Krohn-Rhodes theorem which states that any deterministic automaton is a homomorphic image of a cascade of some simple automata which realize either resets or permutations [101]. According to Theorem 3.50, the regular wreath product of two invariant groups is also invariant. The cascade product of two (invariant) automata can be studied in a similar way. We conjecture that a similar decomposition theorem for a class of invariant automata can be presented in the framework of invariant sets in terms of invariant wreath products.

Since every ZF set together with its discrete $S_A$-action is an invariant set, we conclude that the results in the classical theory of algebraic structures can be obtained by particularizing the results in this chapter.

### 3.6 Comments on the Methods Used in This Chapter

We finish this chapter with a remark regarding the methods we used to translate ZF results into FSM. The reader familiar with algebraic structures and FSM techniques might expect extending algebraic structures to invariant algebraic structures to be trivial, but in fact it is not as easy as one might at first expect because in FSM only finitely supported objects are allowed. Therefore, all the notions and results have to be presented in terms of finitely supported objects. This can create some unexpected problems. First several $S_A$-actions had to be defined in order to build an invariant structure on some algebraic structures like free monoids (Theorem 3.6), free groups (Theorem 3.28), factor monoids (Proposition 3.4), factor groups (Theorem 3.51) and symmetric groups (Proposition 3.42). After these $S_A$-actions were defined we had to check whether the classical ZF result can be naturally translated into FSM only by replacing “algebraic structure” with “finitely supported/invariant algebraic structure”.

The translation of a ZF result into the world of invariant sets is not trivial and always deserves special attention. This is because, given an invariant set $X$, there could exist some subsets of $X$ (for example the simultaneously infinite and co-finite subsets of the set $A$) which fail to be finitely supported. We present some examples of this in the following lines.

We know that there exist models of ZF without choice that satisfy the statement “Every set can be totally ordered” that is known as “the ordering principle”. More details about such models are in [92], where Howard-Rubin’s first model N38 and Cohen’s first model M1 are mentioned. However, we claim that the statement “For every invariant set $X$ there exists a finitely supported total order relation on $X$” is inconsistent in FSM. Indeed, suppose that there exists a finitely supported total order $<$ on the invariant set $A$. Let $a, b, c \notin \text{supp}(<)$ with $a < b$. Since $(ac) \in \text{Fix}(\text{supp}(<))$, we have $(ac)(a) < (ac)(b)$, so $c < b$. However, we also have $(ab), (bc) \in \text{Fix}(\text{supp}(<))$, and so $((ab) \circ (bc))(a) < ((ab) \circ (bc))(b)$,
that is, $b < c$. We get a contradiction, and so the translation of the ordering principle into FSM realized by replacing “structure” with “finitely supported structure” yields a false statement. Moreover, as proved in Subsection 2.7, all the ZF choice principles presented in [88] are inconsistent in FSM, even if they are all independent from the axioms of ZF set theory. Another example of a mathematical result that fails in FSM is the Stone representation theorem for Boolean lattices (claiming that every Boolean lattice is isomorphic to the dual algebra of its associated Stone space). According to Subsection 5.2 from [123], Stone duality fails in the framework of invariant sets because its proof would require a choice principle, namely the ultrafilter theorem, and this theorem is proved to be inconsistent in FSM (see Proposition 5.2.2 from [123] or Section 2.7 from this book). Other results which fail in the FSM setting, such as determinization of finite automata, or equivalence of two-way and one-way finite automata, are presented in [45].

According to [74], there exists a meta-theoretic principle called “the equivariance property” stating that the validity of a formula in the language of FM set theory is preserved by applying a permutation to all its free variables (see Proposition 2.11). Note that the meta-theoretic principle presented above does not always yield appropriate or useful FSM concepts. This is because FSM is generally defined within the ZF framework, whilst the mentioned “equivariance property” holds in the FM cumulative universe (or in the ZFA framework) described in [74]. We cannot directly apply a result which is valid for particular formulas in the FM or ZFA languages in order to prove a ZF property. However, in the ZF framework there exists a related “equivariance/finite support principle” described by using higher-order logic (see Theorem 3.5 in [126] or Theorem 2.5 from this book) which is adequate for the theory of invariant sets. It is worth noting that we chose not to use this principle in order to prove that some structures are finitely supported. One reason is that we want to present our results without involving any notion regarding higher-order logic. Another reason is that sometimes we need to effectively construct the support, and it is not enough to prove only that a certain structure is finitely supported. Let us take a look to Subsection 3.3.5. The equivariance/finite support principle could ensure that each element of the form $l_n^\phi$ or $f_n^m$ is finitely supported. However, we cannot prove directly by involving the form of the finite support principle presented in [126] that all elements $l_n^\phi$ are uniformly supported (by the same set of atoms) and all elements $f_n^m$ are uniformly supported; such a statement requires the precise construction of the support. Other examples in which the equivariance/finite support principle cannot be properly used are represented by Theorem 3.7, Theorem 3.27 and Theorem 3.29. This principle could ensure, after some refinements, that the function $\psi$ in the statements of these theorems is finitely supported. However, we cannot conclude from the equivariance/finite support principle in the form presented in [126] that any set supporting $\phi$ also supports $\psi$, that is, $\text{supp}(\psi) \subseteq \text{supp}(\phi)$. In the related theorems the authors were able to prove a more precise characterization for the support of some structures which could not be obtained by a direct application of the equivariance/finite support principle in the form from [126]. Thus, in these results we did not prove only that some structures are finitely supported, but we also found a relationship between the supports of the
related structures. However, looking at the direct method of constructing the supports in the proofs of the related theorems, we could provide a refinement (stronger form) of the equivariance/finite support principle stating, informally, that for any finite set $S$ of atoms, anything that is definable from $S$-supported structures using $S$-supported constructions is $S$-supported. This statement can be proved by refining the proof of the equivariance/finite support principle from [126]. However, it is worth noting that the related refinement of the equivariance/finite support principle is not carried out in [126] in this form. This stronger form of the finite support principle could be applied in the proofs of the results from this book in order to prove that some structures are uniformly supported and in order to prove some relationship results between several supports. Let us take a look at the proof of Lemma 3.3, for example. The stronger form of the finite support principle would lead to the conclusion that the sequence $(l_n^\phi \mid n < \omega)$ is finitely supported, because both $(l_n \mid n < \omega)$ and $\phi$ were supported by the same $supp(\phi) \cup supp((l_n \mid n < \omega))$. However, the formal involvement of the stronger form of the finite support principle interferes with our direct proof.

Since, in applying the equivariance/finite support principle, one must take into account all the parameters upon which a particular construction depends, we believe the formal involvement of the equivariance/finite support principle, i.e. the precise verification whether the conditions for applying the equivariance/finite support principle are properly satisfied, is sometimes at least as difficult as a direct proof. Moreover, our direct proof method does not require advanced knowledge of (higher-order) logic, and helps the non-expert reader to become familiar with the involved FSM techniques.

### 3.7 Conclusion

Our goal is to develop a mathematics for experimental sciences which deals with a more relaxed notion of finiteness. We call such a mathematics ‘Finitely Supported Mathematics’, or FSM for short; it represents a first step in managing the notion of infinite. Informally, in FSM we can model infinite structures after a finite number of observations. More precisely, we intend to restate some parts of algebra by replacing ‘(infinite) sets’ with ‘invariant sets’. This allows us to model some infinite structures by using their finite supports. In order to sustain our viewpoint, we need some results from the axiomatic theory of FM sets presented in [74]. Rather than using a non-standard set theory, we could alternatively work with invariant sets, which are defined within ZF as usual sets endowed with some group actions satisfying a finite support requirement. The properties of invariant sets are similar to those presented in [127], with the caveat that we assume invariant sets to be defined over possibly non-countable sets of atoms. Our book presents the basic steps required in order to provide an extension of the theory of invariant sets to a theory of invariant algebraic structures. Although the initial purpose of defining invariant sets was to formulate a semantics for syntax with variable binding, we consider that such sets can also
be used from an algebraic perspective in order to characterize infinite structures modulo finite supports, and thus in order to provide more information about infinite objects.

The category of invariant sets has a very rich structure (e.g. it is equivalent to the Schanuel topos), and so the definitions of many structures classically given in the usual category of sets can be reformulated within the invariant sets framework. A natural question is which classical theorems about these structures hold internally in the world of invariant sets. Until now (or, more precisely, until we are able to solve the open problem presented below) there does not exist a standard/formal algorithm to translate an arbitrary classical ZF result into FSM. This is because there may exist some subsets of an invariant set which fail to be finitely supported, and thus there may exist some ZF results that fail in the universe of invariant sets. Related examples regarding the previous statement are presented in Section 3.6. Therefore, reformulating the ZF theorems into FSM has to be done for each case separately. For example, the theory of monoids is studied in FSM in Section 3.1, the theory of posets and domains is reformulated within invariant sets in Section 3.3, and the theory of groups is rephrased in FSM in Section 3.4. In order to prove that a structure is finitely supported, one could use either the finite support principle from [126] (e.g. Theorem 2.5) or the more “constructive” method described in this book. To employ the so called “constructive method” means that we anticipate a possible candidate for a support and we prove that this candidate is indeed a support. In this book we agree to use a direct method for constructing the supports of some structures. This is because the general principles of equivariance and finite support are hard to apply formally, and in practice it is often easier and less error-prone to check equivariance by hand rather than try to formalize proofs in higher-order logic.

**An Open Problem**

The main task in order to define FSM is to prove that certain subsets of an invariant set are finitely supported. We already know that given an invariant set $X$, there could exist some subsets of $X$ which fail to be finitely supported. Some related examples are presented in [127] and [156]. However, all these examples are described by using choice principles or consequences of choice principles (like the assertion that the set $A$ can be non-amorphous in ZF or ZFA) in order to construct some structures which later fail to be finitely supported. In Section 2.7 we proved that all the choice principles presented in [88] are inconsistent in FSM. We have not yet found any example of a non-finitely supported subset of an invariant set defined/constructed without using a choice principle from [88] or a consequence of a form of choice (such as the construction of an infinite and cofinite subset of an infinite set). Therefore, the question regarding the validity of the following assertions naturally appears:

- If we consider ZF set theory (or ZFA set theory) without any choice principle, then is every subset of an invariant set finitely supported?
- For what kind of atoms does the previous question have an affirmative answer?
If we get an affirmative answer (even for a particular set of atoms), then the mathematics developed in ZF (or ZFA) set theory without any choice principle would be somehow equivalent to FSM, namely we could model any infinite structure by using its finite support.
Chapter 4
Extended Fraenkel-Mostowski Set Theory

Abstract The finite support axiom of Fraenkel-Mostowski set theory is very strong. We study the consequences of replacing this strong axiom with a weaker one. In this chapter we generalize Fraenkel-Mostowski set theory by giving a new set of axioms which defines Extended Fraenkel-Mostowski set theory. In Extended Fraenkel-Mostowski set theory, instead of the finite support axiom we require that each subset of the set of atoms is either finite or cofinite. We study several algebraic, order and topological properties of Extended Fraenkel-Mostowski sets.

4.1 Axioms of Extended Fraenkel-Mostowski Set Theory

Let \( P_A \) be the set of all bijections of \( A ; S_A \) is a proper subgroup of \( P_A \). We extend the definitions in Section 2.3 by replacing \( S_A \) with \( P_A \).

Definition 4.1. Let \( X \) be a ZF set. A \( P_A \)-action on \( X \) is a function \( \cdot : P_A \times X \rightarrow X \) having the properties that \( Id \cdot x = x \) and \( \pi \cdot (\pi' \cdot x) = (\pi \circ \pi') \cdot x \) for all \( \pi, \pi' \in P_A \) and \( x \in X \).

Definition 4.2. Let \( X \) be a \( P_A \)-set and \( x \in X \). We say that \( S \subseteq A \) supports \( x \) if for each \( \pi \in \text{Fix}(S) \cap S_A \) we have \( \pi \cdot x = x \). If \( \text{Fix}(S) \cap S_A \) is non-empty, then it has a least element which also supports \( x \). We call this element the support of \( x \), and we denote it by \( \text{supp}(x) \).

The following theorem can be proved in a similar way to Theorem 2.4 because in this section our definition of the notion of “set supporting an element” also involves only finitary permutations (Definition 4.2).

Theorem 4.1. Let \( X \) be a \( P_A \)-set and for each \( x \in X \) let us define \( \mathcal{F}_x = \{ S \subseteq A \mid S \text{ finite, } S \text{ supports } x \} \). If \( \mathcal{F}_x \) is non-empty, then it has a least element which also supports \( x \). We call this element the support of \( x \), and we denote it by \( \text{supp}(x) \).
**Definition 4.4.** i) Let $X$ be a ZFA set. A $P_A$-interchange function over $X$ is a function $\cdot : P_A \times X \to X$ defined inductively by $\pi \cdot a = \pi(a)$ for all atoms $a \in A$, and by $\pi \cdot x = \{\pi \cdot y \mid y \in x\}$ otherwise. Moreover, it satisfies the following axiom: for each $x \in X$, there is a finite non-empty set $S \subset A$ such that for each $\pi \in Fix(S) \cap S_A$ we have $\pi \cdot x = x$.

ii) A $P_A$-IFM set is a pair $(X, \cdot)$, where $X$ is a ZFA set, and $\cdot : P_A \times X \to X$ is a $P_A$-interchange function over $X$. We simply use $X$ whenever no confusion arises.

**Remark 4.1.** Since $P_A$ is a group, the $P_A$-interchange function $\cdot : P_A \times X \to X$ is an action of the group $P_A$ on the set $X$ because we have $Id \cdot x = x$ and $\pi \cdot \pi' \cdot x = (\pi \circ \pi') \cdot x$ for all $\pi, \pi' \in P_A$. Therefore, we can see a $P_A$-IFM set $(X, \cdot)$ as a set provided by an action of $P_A$ on $X$.

The reader might ask why we chose to define the invariant sets (IFM sets) in Section 2.3 as sets equipped with an $S_A$-action and not as sets equipped with a $P_A$-action. Well, we do not change the field at all if we replace $S_A$ with $P_A$ in FSM (or in the FM cumulative universe). This is because in FSM (and in the FM cumulative universe) only finitely supported objects are allowed. In a similar way to Example 2.1(3), for each $\sigma \in P_A$, we have that $S_\sigma = \{a \in A \mid \sigma(a) \neq a\}$ is the least set of atoms supporting $\sigma$ in the sense of Definition 4.2. According to the finite support requirement, in FSM (and in the FM cumulative universe) $S_\sigma$ has to be finite for each $\sigma \in P_A$. Thus, in FSM (and in the FM cumulative universe) only finitary permutations of atoms are allowed. In Extended Fraenkel-Mostowski (EFM) set theory the finite support requirement is eliminated. Therefore, even non-finitary permutations are allowed in the EFM universe. When we extend FM set theory by replacing the finite support axiom with a weaker axiom, it is natural to replace $S_A$ with $P_A$ in the new definitions and results.

We can generalize the notions defined in Definition 4.4.

**Definition 4.5.** i) Let $X$ be a ZFA set. An extended interchange function over $X$ is a function $\cdot : P_A \times X \to X$ defined inductively by $\pi \cdot a = \pi(a)$ for all atoms $a \in A$, and by $\pi \cdot x = \{\pi \cdot y \mid y \in x\}$ otherwise. Moreover, each subset of $A$ is either finite or cofinite.

ii) An EFM set is a pair $(X, \cdot)$, where $X$ is a ZFA set, and $\cdot : P_A \times X \to X$ is an extended interchange function on $X$. We simply use $X$ whenever no confusion arises.

iii) Let $G$ be a subgroup of $P_A$. We say that a group action $\cdot : G \times X \to X$ is defined as the extended interchange function if $\cdot$ is defined inductively by $\pi \cdot a = \pi(a)$ for all atoms $a \in A$, and by $\pi \cdot x = \{\pi \cdot y \mid y \in x\}$ otherwise, for all $\pi \in G$.

iv) A $G$-renaming is an orbit of an (arbitrary) atom under the action $\cdot : G \times A \to A$ defined as the extended interchange function.

**Remark 4.2.** Since $P_A$ is a group, the extended interchange function $\cdot : P_A \times X \to X$ is an action of the group $P_A$ on the set $X$; we have $Id \cdot x = x$ and $\pi \cdot \pi' \cdot x = (\pi \circ \pi') \cdot x$ for all $\pi, \pi' \in P_A$. Therefore, we can think of an EFM set $(X, \cdot)$ as being like a set provided by an action of $P_A$ on $X$. 
It is worth noting that we use the same notation · for both the $P_A$-interchange function and the extended interchange function. It will be proved later that a $P_A$-interchange function can be also represented as an extended interchange function.

As presented in Example 2.3, in the FM framework each subset of $A$ is either finite or cofinite because of the finite support requirement. We replace the finite support requirement with this property of the structure of $A$.

**Definition 4.6.** The following axioms provide a complete characterization of Extended Fraenkel-Mostowski set theory:

1. $\forall x. (\exists y. y \in x) \Rightarrow x \notin A$ (only non-atoms can have elements)
2. $\forall x, y. (x \notin A \land y \notin A \land \forall z. (z \in x \iff z \in y)) \Rightarrow x = y$ (axiom of extensionality)
3. $\forall x. \exists y. z = \{x, y\}$ (axiom of pairing)
4. $\forall x. \exists y. z = \{z \mid z \subseteq x\}$ (axiom of powerset)
5. $\forall x. \forall y. \notin A \land \{z \mid z \in w \land w \in x\}$ (axiom of union)
6. $\forall x. \exists y. \{z \mid z \in x\}$, for each functional formula $f(z)$ (axiom of replacement)
7. $\forall x. \exists y. \{z \mid z \in x \land p(z)\}$, for each formula $p(z)$ (axiom of separation)
8. $(\forall x. (\forall y. x \land y) \Rightarrow p(x)) \Rightarrow \forall x. p(x)$ (induction principle)
9. $\exists x. (\emptyset \in x \land (\forall y. x \Rightarrow y \cup \{y\} \in x))$ (axiom of infinity)
10. $A$ is not finite
11. Each subset of $A$ is either finite or cofinite (axiom of the structure of $A$)

A model of EFM set theory is represented by the model $\nu(A)$ of ZFA set theory, where $A$ is assumed to be an infinite amorphous set of atoms. More precisely, we define:

- $\mu_0(A) = \emptyset$;
- $\mu_{\alpha+1}(A) = A + \emptyset(\mu_\alpha(U))$, where $+$ denotes the disjoint union of sets defined in Example 2.1(7);
- $\Gamma_{\alpha+1}(A) = \mu_{\alpha+1}(A) \setminus T_0$, where $T_0$ is formed by those ZFA subsets of $A$ which are simultaneously infinite and cofinite;
- $\Gamma_{\lambda}(A) = \bigcup_{\alpha < \lambda} (\nu_\alpha(\mu_\alpha(A) \setminus T_0)) (\lambda$ a limit ordinal),

Let $\Gamma(A)$ be the union of all $\Gamma_\alpha(A)$. Then $\Gamma(A)$ is a model of EFM set theory.

**Remark 4.3.** Axiom 11’ of EFM set theory is a direct consequence of Axiom 11 of FM set theory. Thus, EFM set theory is a natural extension of FM set theory. A $P_A$-interchange function can be presented as an extended interchange function, and a $P_A$-IFM set can be presented as an EFM set.

There is no visible difference between the notions of interchange function ($P_A$-interchange function) and extended interchange function, except there is a restriction on the type. In FM set theory the notions of interchange function, $P_A$-interchange function and extended interchange function are identical because only finitary permutations are allowed in the FM universe.
4.2 Inconsistency of the Axiom of Choice

**Theorem 4.2.** The choice principles $\text{Fin}$ and $\text{AC(fin)}$ are inconsistent with the axioms of EFM set theory.

*Proof.* According to [105], we know that $\text{Fin}$ implies “Every infinite set $X$ has an infinite subset $Y$ such that $X \setminus Y$ is also infinite”. According to [51], the following implication holds: $\text{AC(fin)}$ implies “Every infinite set $X$ has an infinite subset $Y$ such that $X \setminus Y$ is also infinite”. These results remain valid in EFM set theory. The presence of atoms in the EFM framework does not change their ZF proof, and the finite support property is no longer required in EFM set theory. According to axiom 11’ in EFM set theory, for each subset $X$ of the infinite set $A$ we have that either $X$ is finite or $A \setminus X$ is finite. Therefore, the statement “Every infinite set $X$ has an infinite subset $Y$ such that $X \setminus Y$ is also infinite” is false in the EFM framework. Thus, the choice principles $\text{Fin}$ and $\text{AC(fin)}$ fail in EFM set theory. The inconsistency of $\text{Fin}$ with the axioms of EFM set theory can also be proved directly from axiom 11’. Suppose that $\text{Fin}$ is a valid statement in the EFM framework. Then we can find an injection $f : \mathbb{N} \to A$. Obviously $f(2\mathbb{N})$ and $f(2\mathbb{N} + 1)$ are disjoint, infinite subsets of $A$. Therefore, $f(2\mathbb{N})$ is infinite and cofinite, and this contradicts the structure of $A$. Thus, $\text{Fin}$ fails in the EFM framework. $\Box$

**Remark 4.4.** Note that the proof of Theorem 4.2 is consistent with the EFM axioms. However, such a proof cannot be made in FSM because in the FSM universe only finitely supported objects are allowed. So, the mentioned implications in the proof of Theorem 4.2 are not necessary valid in FSM unless we are able to reformulate them in terms of finitely supported objects. This is the reason why we do not present Theorem 2.12 and Theorem 2.13 as consequences of Theorem 4.2. More details are in Remark 2.6.

According to Theorem 2.1 (which is also consistent with the EFM axioms), since $\text{AC(fin)}$ and $\text{Fin}$ are inconsistent with the axioms of EFM set theory, the choice principles $\text{AC, ZL, DC, CC, PCC, PIT, UFT, OP, KW, RKW,}$ and $\text{OEP}$ presented in Section 2.1 are inconsistent with the axioms of EFM set theory.

We make the remark that, although the axiom of choice is inconsistent with both the FM and the EFM axioms, a weaker form of the axiom of choice (where the choice is made from finite families) is valid both in FSM and in EFM.

**Remark 4.5.** The axiom of choice states that, for each family $\mathcal{F}$ of non-empty disjoint sets, we can find a system of representatives (which is a set that contains exactly one element from each set in $\mathcal{F}$). If $\mathcal{F}$ is a finite family of disjoint non-empty sets, this statement is a consequence of Axioms 1-9 (and not a form of the axiom of choice). Indeed, if $\mathcal{F}$ contains only one non-empty set $U$, then we can find an element $x_0 \in U$ (because $U$ is non-empty). According to the axiom of pairing, we obtain the set $\{x_0\}$ which is a set of representatives for $\mathcal{F}$. By the induction principle, we can obtain a set of representatives for each finite family $\mathcal{F}$ of disjoint non-empty sets (see [135] for details).
The previous remark is applied, for example, in the proof of Theorem 4.4 or in the proof of Proposition 4.6.

4.3 Algebraic Properties of EFM Sets

Since the sets in the EFM framework (or in the FM framework, respectively) are pairs \((X, \cdot)\) where \(X\) is a ZFA set and \(\cdot\) is an extended interchange function over \(X\) (or \(\cdot\) is an interchange function over \(X\), respectively), we can also say that the properties of extended interchange functions (interchange functions) provide properties of EFM sets (FM sets).

Our goal is to present some results which finally allow us to say that the domain of the interchange functions (\(P_A\)-interchange functions) and the domain of the extended interchange functions have some similar algebraic properties. Several general properties of permutation groups used for proving these results can be found in [53] or [133].

**Theorem 4.3.** In the EFM framework \(P_A\) is a torsion group.

**Proof.** We prove that \(P_A\) is a torsion group, i.e. every element of \(P_A\) has finite order. First we prove that the cycles of an arbitrary \(\sigma \in P_A\) are finite. Moreover, there is an \(m \in \mathbb{N}\) such that all but finitely many cycles of \(\sigma\) have length \(m\). Let us suppose that \(\sigma\) has an infinite cycle. If we assume that \(\sigma\) has at least two infinite cycles, then the set of points of one of these cycles is infinite and cofinite. However, every subset of \(A\) is finite or cofinite, and this means that every cycle of \(\sigma\) is finite. If we suppose now that \(\sigma\) has only one infinite cycle, we obtain that \(\sigma \circ \sigma\) is a permutation with at least two infinite cycles, and so we get a contradiction. Now, for every \(n \in \mathbb{N}\), the set of points in the cycles of \(\sigma\) which have length \(n\) is also finite or cofinite. If there is \(n\) such that this set is cofinite, then the proof is finished. If not, then there is an infinite number of different cycle lengths. We can define a partition of the set of cycle lengths into two infinite sets \(X\) and \(Y\). Then the set of points from cycles with length in \(X\) is infinite and cofinite, and so we get a subset of \(A\) (the set of points from cycles with length in \(X\)) which is neither finite nor cofinite. Again we contradict the relation \(\wp(A) = \wp_{\text{fin}}(A) \cup \wp_{\text{cofin}}(A)\). We obtained that all the cycles of \(\sigma\) are finite, and have a finite number of cycle lengths. According to Theorem 5.1.2 in [84], the order of \(\sigma\) is the least common multiple of these cycle lengths. Thus, \(P_A\) is a torsion group.

**Remark 4.6.** Since the set of cycle lengths is a subset of \(\mathbb{N}\) (built by using the axiom of infinity), we could define a partition of the set of cycle lengths into two infinite sets \(X\) and \(Y\). The construction of \(\mathbb{N}\) is not in contradiction with the axioms of the EFM set theory. However, the set \(A\) of atoms cannot be partitioned into two infinite subsets \(A_1\) and \(A_2\).

**Theorem 4.4.** In the EFM framework each subgroup of \(P_A\) which is finitely generated is also finite.
Proof. We prove that, if \( G \leq P_A \) is a finitely generated group, then \( G \) is finite. Let \( \sigma_1, \sigma_2, \ldots, \sigma_m \in P_A \) and \( G = \langle \sigma_1, \ldots, \sigma_m \rangle \). A \( G \)-renaming is the orbit of an element \( \alpha \in A \) under the canonical action of \( G \) on \( A \) defined as in Definition 4.5. We prove that there is an \( r \) (depending on \( m \)) such that all but finitely many \( G \)-renamings (under the canonical action of renaming on atoms defined by the extended interchange function) have size \( r \). Let us assume that there is an infinite \( G \)-renaming under the canonical action of \( G \) on \( A \) defined by \( (\sigma, \alpha) \mapsto \sigma(\alpha) \). As a \( G \)-renaming is the orbit of an element \( \alpha \in A \), we claim that this orbit contains a countable infinite subset. We define a word with \( k \) letters in \( \sigma_1, \sigma_2, \ldots, \sigma_m \) to be a finite composition of \( k \) permutations and inverses from the set \( \{ \sigma_1, \sigma_2, \ldots, \sigma_m \} \). This terminology comes from the theory of free groups. Of course, the set of words with \( k \) letters is finite for each \( k \). We consider an infinite sequence of words in \( \sigma_1, \sigma_2, \ldots, \sigma_m \). If there is \( a \in A \) with an infinite orbit, we can define the image \( \{a_1, a_2, \ldots, a_m\} \) of \( a \) under the words of the sequence by \( a_1 = \sigma_1(a), \ldots, a_m = \sigma_m(a) \). Let \( a_{m+1} = \sigma_{m+1}(a) \), where \( \sigma_{m+1} \) is the first word in the sequence such that \( \sigma_{m+1}(a) \notin \{a_1, a_2, \ldots, a_m\} \). Such a \( \sigma_{m+1} \) exists because we suppose that the orbit of \( a \) is infinite. Indeed, we can define a method of covering the sequence of words in \( \sigma_1, \sigma_2, \ldots, \sigma_m \) in the following way: first we cover the words with two letters (in an alphabetically ordered way, that is, in the same way as we “read a dictionary”, because the set of letters is finite, and so well ordered; note that each finite set can be well ordered, and in order to prove this we do not need the axiom of choice), then we cover the words with three letters, and so on. We pick the first word we find with the required property that the image of \( a \) under it is not a member of \( \{a_1, a_2, \ldots, a_m\} \). We present a constructive method to chose the first element in the sequence with the required property. The method of covering the sequence presented before could induce a well order relation on that sequence if we consider only the distinct words in the sequence (note that if we form all the possible words with the letters \( \sigma_1, \sigma_2, \ldots, \sigma_m \) we could have words in \( \sigma_1, \sigma_2, \ldots, \sigma_m \) with different numbers of letters but which are equal); this order is called “lexicographic order”. With \( a_{m+1} \) already found we repeat the procedure described before to find \( a_{m+2} \) and so on. Thus, we obtain a countable subset of \( A \) denoted by \( B \). This contradicts the fact that all subsets of \( A \) are finite or cofinite because \( B \) has both infinite and cofinite subsets. If a finite number (greater than one) of \( G \)-renaming sizes occur infinitely, then we contradict the special property of \( A \) that \( \wp(A) = \wp_{\fin}(A) \cup \wp_{\cofin}(A) \). Indeed, let us suppose we have an infinite number of \( G \)-renamings with size \( k \) and an infinite number of \( G \)-renamings with size \( l \). Since the \( G \)-renamings which are different are also disjoint, we conclude that elements in the \( G \)-renamings with size \( k \) form a set which is both infinite and cofinite. If the \( G \)-renamings are arbitrarily large, we again obtain a contradiction. The proof of this fact is similar to that of Theorem 4.3: we use a partition of the \( G \)-renaming sizes into two infinite sets \( X \) and \( Y \), and see that the set of elements with \( G \)-renaming sizes in \( X \) is infinite and cofinite. We conclude that all but finitely many \( G \)-renamings have size \( r \). Thus, there are infinitely many \( G \)-renamings, and all but finitely many of these \( G \)-renamings have size \( r \) (otherwise, if we assume that there are only a finite number of \( G \)-renamings, because each \( G \)-renaming is finite, it follows that \( A \) is finite which is a contradiction).
Let us suppose that $G$ is infinite. We define an equivalence relation on the set of $G$-renamings saying that two $G$-renamings are equivalent iff the actions of $G$ on them are isomorphic. Since $G$ is finitely generated, it follows that there is only a finite number of homomorphisms from $G$ to $S_r$, and so there is only a finite number of equivalence classes (we can identify an action with its associated representation by permutations). It follows that one equivalence class (denoted by $\mathcal{O}$) is infinite; otherwise, if all the equivalence classes are finite, because there are only finitely many equivalence classes, then there is only a finite number of $G$-renamings, which is a contradiction.

Let $X_0$ be a $G$-renaming that is a representative of $\mathcal{O}$. The action of $G$ on $X_0$ can be seen as a homomorphism $f$ from $G$ to $S_r$. In fact this action can be viewed as the associated representation by permutations $\psi : G \to S(X_0)$ defined by $\psi(\sigma)(x) = \sigma(x)$. Since $|X_0| = r$, there is an isomorphism $\phi : S(X_0) \to S_r$, and $f = \phi \circ \psi$. If $\sigma \in \text{Ker } f$, then $\sigma$ fixes all the elements in $X_0$, and so $\sigma$ fixes all the elements whose $G$-renamings are in $\mathcal{O}$. Definition 4.19 of [133] is useful to show what isomorphic actions look like. The number of elements of $A$ fixed by $\sigma$ is infinite, and because $\varrho(A) = \varrho_{\text{fin }}(A) \cup \varrho_{\text{cofin }}(A)$, the number of elements of $A$ not fixed by $\sigma$ is finite. Therefore, $\text{Ker } f$ is formed by permutations which keeps fixed all but finitely many atoms.

We also have that $S_A$ is locally finite. Indeed, let $\pi_1, \ldots, \pi_k \in S_A$ such that $\pi_1$ permutes the atoms from a finite subset of $A$ named $U_1, \ldots, \pi_k$ permutes the atoms from a finite subset of $A$ named $U_k$. Let $U = U_1 \cup \ldots \cup U_k$. Then each of $\pi_1, \ldots, \pi_k$ is a permutation of $U$. If $u$ is the finite cardinality of $U$, then we obtain that $|\{\pi_1, \ldots, \pi_k\}| \leq S(U) \cong S_u$, and, of course, $|\{\pi_1, \ldots, \pi_k\}|$ is finite.

Now, since $\text{Ker } f \leq S_A$ and $S_A$ is locally finite, we have that $\text{Ker } f$ is locally finite (see [133]). There is also an isomorphism from $G/\text{Ker } f$ to $S_r$; the proof is similar to the proof of the fundamental isomorphism theorem for groups, and it does not use the axiom of choice. Since $\text{Ker } f$ is locally finite and $G/\text{Ker } f$ is finite, it follows that $G$ is also locally finite (this result is proved in [133] for the general case: if for a group $H$ there is $K \triangleleft H$ such that both $K$ and $H/K$ are locally finite, then $H$ is locally finite; moreover, if $H/K$ is finite, the axiom of choice is not used). Since $G$ is finitely generated, we have that $G$ is finite, and this completes the proof.

Remark 4.7. The validity of the last paragraph in the proof of Theorem 4.4 also follows from a result claiming that for a finitely generated group $G$, every subgroup of finite index in $G$ is finitely generated; the proof of this result does not use the axiom of choice (see [133]). Indeed, using the notations from the previous theorem, we get that $\text{Ker } f$ is a subgroup of finite index in $G$. Then $\text{Ker } f$ is finitely generated. Since $\text{Ker } f$ is also a locally finite group (it is a subgroup of the locally finite group $S_A$), then $\text{Ker } f$ is finite. Since $\text{Ker } f$ and $G/\text{Ker } f$ are both finite, it follows that $G$ is finite; the proof is similar to the proof of Lagrange Theorem. According to Remark 4.5, we can choose a system of representatives for the set of left cosets modulo $\text{Ker } f$ since $G/\text{Ker } f$ is finite.

A general result in ZF group theory says that a torsion group which is at the same time soluble and finitely generated is also a finite group. Another result says that
a torsion group which is in the same time nilpotent and finitely generated is also a finite group (see [130]). The result presented in Theorem 4.4 is stronger; we need neither solubility nor nilpotency.

Since in the axiomatic description of EFM set theory we assumed that $\wp(A) = \wp_{fin}(A) \cup \wp_{cofin}(A)$, Theorems 4.3 and 4.4 are not valid in a general theory of atoms. In fact, we can prove Theorem 4.3 and Theorem 4.4 only in EFM and in FM settings.

We give a result which presents some algebraic connections between the domain of the extended interchange function and the domain of the interchange function.

**Theorem 4.5.** The properties of $P_A$ described in Theorem 4.3 and Theorem 4.4 are valid in both EFM and FSM.

**Proof.** The result follows because $P_A$ coincides with $S_A$ in the FM framework. \(\Box\)

In the following proposition we present a collection of some known results from group theory providing certain characterizations of the extended interchange function in terms of transitive groups. Such results can be proved without employing any form of choice.

**Definition 4.7.** A group $G \leq P_A$ is called transitive if each atom can be obtained from another atom after a renaming under a permutation in $G$ (i.e. the canonical action $\cdot : G \times A \to A$ has only one orbit).

**Proposition 4.1.** Let $G \leq S_A$.

1. If $G$ is transitive, then the commutator subgroup $D(G)$ is also transitive.
2. Suppose that $H \triangleleft G$ with $H$ transitive. Then $D(G) \leq H$.
3. If $G$ is transitive, then $D(G) = D(D(G))$.
4. If $G$ is transitive, then $G$ is not soluble [159].
5. If $G$ is transitive, then for each $a \in A$ the subgroup $IREN(a) = \{\pi \in G | \pi(a) = a\}$ is not soluble [30].
6. If $G$ is transitive, and $B$ a finite subset of $A$, then there is $\sigma \in G$ such that $\sigma(B) \cap B = \emptyset$ [112].
7. Let us consider the additional requirements that $G \leq P_A$ with the property that $G$ is transitive, and there is no $B \subseteq A$ such that either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ for each $\sigma \in G$. If $G$ contains a non-identity permutation of $S_A$, then $G$ must contain the group of even permutations in $S_A$ [53].

For the last part of this section we consider an additional condition on $A$. We denote by $FPA$ the partitions of $A$ in which all the parts are finite. If $(A_i)_i \in FPA$, then there is a unique natural number $|\left(\left(\right)\right)|$ such that all but finitely many parts of $(A_i)_i$ have the cardinality $|\left(\left(\right)\right)|$, and the cardinality $|\left(\left(\right)\right)|$ is called the cardinality of the partition $(A_i)_i$. We can prove this in a similar way to Theorem 4.3 where all but finitely many cycles of a permutation have the same length. We assume that among the partitions in $FPA$ we are able to choose a partition with maximum cardinality (which can be as large as needed). We call this cardinality the “dimension of $A$”, and a partition with maximum cardinality is called a “maximal partition”. We introduce
the following order relation on $FPA$: $(A_i)_{i \in I} \leq (B_j)_{j \in J}$ iff $\forall j \in J \exists I_j \subseteq I$ such that $B_j = \bigcup_{i \in I_j} A_i$.

Two partitions $(A_i)_{i \in I}$ and $(B_j)_{j \in J}$ are equivalent (denoted by $(A_i)_{i \in I} \sim (B_j)_{j \in J}$) if whenever there is $B \subseteq A$, $B$ infinite and $B = \bigcup_{i \in I} A_i$, then for $C \subseteq B$ we have “there exists $i \in I$ such that $C = A_i$ iff there is $j \in J$ such that $C = B_j$”.

**Proposition 4.2.** ($FPA, \leq$) is a complete lattice, and the equivalence relation $\sim$ over $FPA$ defined before is a congruence.

**Proposition 4.3 ([154]).** There is a one-to-one function from the subgroup lattice $P_A/S_A$ to the lattice of equivalence classes of partitions of $A$.

**Proof.** Let $H \leq P_A/S_A$. From the general theory of bounded amorphous sets, we have that $P_A/S_A$ is finite [154]. Let $\sigma_1, \sigma_2, \ldots, \sigma_m \in P_A$ be left coset representatives for $S_A$. Let $(A_i)_{i \in I}$ be a maximal partition of $A$. Then for each $j \in \{1,2,\ldots,m\}$ we have that $\sigma_j$ keeps fixed the equivalence class of $(A_i)_{i \in I}$. Thus, we can assume that all of them keep $(A_i)_{i \in I}$ fixed. A result from classical set theory says that if $(A_i)_{i \in I} \in FPA$, then there is $(B_j)_{j \in J} \subseteq FPA$ such that $(A_i)_{i \in I} \sim (B_j)_{j \in J}$ and $(B_j)_{j \in J}$ is formed only from members with cardinality $|B_j|_{j \in J}$ and members of cardinality 1.

We can say that $\sigma_1, \ldots, \sigma_m$ keep fixed all but finitely many elements of the maximal partition $(A_i)_{i \in I}$. Let $A_j$ be a part of this partition which is fixed by $\sigma_1, \ldots, \sigma_m$, and $|A_j| = |(A_i)_{i \in I}| = r$. We use the notation $A_j = \{1,\ldots,r\}$. Now we consider a function $f$ defined on $P_A$ having values in $S_r$ with the property that for each $\sigma \in P_A$, $f(\sigma)$ is the induced permutation in $S_r$ for the representative of an equivalence class of $\sigma$ modulo $S_A$. It is not difficult to prove that $f$ is a group homomorphism, and $\text{Ker } f = S_A$. This homomorphism does not depend on the choice of representatives of the equivalence classes modulo $S_A$ because, by renumbering the points of $A_j$, we can exchange any image with a conjugate in $S_r$. Since in every element from $P_A$ all but finitely many cycles have the same length, the image of the homomorphism defined before is represented by permutations in which all cycles have the same length. We can say that the finitely generated group $\{\sigma_1, \ldots, \sigma_m\}$ keeps the partition $(A_i)_{i \in I}$ fixed, and $\{(\sigma_1, \ldots, \sigma_m)\}$ acts semiregularly on all but finitely many parts of $(A_i)_{i \in I}$.

The group $H_1$ generated by the representatives of left cosets in $H$ has $H$-orbits of cardinality $|H|$ in these parts of $(A_i)_{i \in I}$, and so defines a partition whose cardinality is $|H|$.

In the following we prove that the related function is one-to-one (injective). Let us assume that $H$ and $K$ provide equivalent partitions. We denote by $\{[H,K]\}$ the subgroup generated by $H$ and $K$; thus, $H \leq \{[H,K]\}$. Since $H$ and $\{[H,K]\}$ provide equivalent partitions, it follows that $|H| = |\{[H,K]\}|$, and so $H = \{[H,K]\}$. We also have $K = \{[H,K]\}$, and so we conclude that $H = K$. □

The reader can note that an additional condition on $A$ (namely the existence of the maximal partition) is used to prove this result. However, this condition does not restrict the generality too much because the maximum cardinality can be as large as we need. Even without this condition, in [154] it is proved in a similar way that there is a one-to-one function from the set of finitely generated subgroups of $P_A/S_A$ to the set of equivalence classes of the partitions of $A$. 
4.4 Topological Properties of EFM Sets

This section makes a connection between classical group theory and domain theory. For each group, its subgroup lattice is an algebraic domain with respect to the standard inclusion of subgroups. A basis for this domain is represented precisely by the finitely generated subgroups [1]. Some results in classical order theory are particularized to this domain and several properties of various classes of groups are obtained. We also make a connection between the topology and group theory by defining the Scott topology on the subgroup lattice of a group. A basis for this topology is expressed in terms of finitely generated subgroups (Theorem 4.8). Continuous functions defined with respect to the Scott topology also have interesting properties (Theorem 4.11 and Theorem 4.12). Finally several new order and topological properties of EFM sets are obtained.

4.4.1 Subgroup Lattices as Domains

According to Subsection 3.4.4, because every ZF set is a trivial invariant set, we obtain the following result (which is a classical result known from [1]).

**Theorem 4.6.** Let $G$ be a group.

- $(\mathcal{L}(G), \subseteq)$ is a continuous domain and a basis in $(\mathcal{L}(G), \subseteq)$ is precisely $F(\mathcal{L}(G))$.
- $(\mathcal{L}(G), \subseteq)$ is an algebraic domain and the compact elements in $(\mathcal{L}(G), \subseteq)$ are precisely those in $F(\mathcal{L}(G))$.

In the general theory of domains the next interpolation property is valid (see [77]):

Let $x \ll y$ in a continuous domain $(D, \sqsubseteq)$ with basis $B$. Then there exists an element $b \in B$ such that $x \ll b \ll y$.

So, if $(D, \sqsubseteq)$ is an algebraic domain and $x \ll y$, we can find a compact element $c$ such that $x \ll c \ll y$. For the particular case of algebraic domains this result can be easily proved. Indeed, let $x \ll y$. Because $D$ is algebraic we know that $y$ is the directed supremum of the compact elements approximating it. According to the definition of the approximation relation, there exists $c \in K(D)$ such that $x \sqsubseteq c \ll y$. Because $c \ll c$ we get $x \ll c \ll y$.

The following result can be easily proved (see [1]).

**Theorem 4.7.** Let $G$ be a group and $H, K$ be two elements in $(\mathcal{L}(G), \subseteq)$ such that $H \ll K$. There exists a finitely generated subgroup of $G$ denoted by $L$ with $H \ll L \ll K$. 
4.4.2 Scott Topology over the Subgroup Lattice of a Group

A topology on a space $X$ is a system of subsets of $X$ (called open sets), which is closed under finite intersections and infinite unions. The complements of open sets are called closed sets [50]. For a dcpo $(D, \sqsubseteq)$ there are many possible choices of topology to transform $D$ into a topological space. There are the well-known Scott topology and Lawson topology. These were described in [77] for the general case of dcpos. Here we particularize to groups some topological results in the general theory of dcpos and domains. Our goal is to obtain some new properties of groups, and, particularly, some new properties of $P_\lambda$.

Let $(D, \sqsubseteq)$ be a dcpo. A subset $U$ is called Scott-closed if it is a lower set and is closed under suprema of directed subsets. A principal ideal (i.e. an ideal of form $\downarrow x$ where $\downarrow x = \{y \in D \mid y \sqsubseteq x\}$) is always a Scott-closed set. Complements of closed sets are called Scott-open. A Scott-open set is an upper set $O$ with the property that every directed set whose supremum belongs to $O$ has a non-empty intersection with $O$.

**Definition 4.8.** Let $(\mathcal{L}(G), \subseteq)$ be the subgroup lattice of $G$. A subset $(H_i)_{i \in I}$ of elements in $\mathcal{L}(G)$ is called Scott-closed if the following conditions are satisfied:

1. For each $i \in I$ and $K \leq G$, $K \subseteq H_i$ implies there exists $j \in I$ such that $K = H_j$.
2. If $(K_j)_{j \in J} \subseteq (H_i)_{i \in I}$ is a directed family of subgroups of $G$, then $\bigcup_{j \in J} K_j \subseteq (H_i)_{i \in I}$.

**Definition 4.9.** Let $(\mathcal{L}(G), \subseteq)$ be the subgroup lattice of $G$. A subset $(H_i)_{i \in I}$ of elements in $\mathcal{L}(G)$ is called Scott-open if the following conditions are satisfied:

1. For each $i \in I$ and $K \leq G$, $K \supseteq H_i$ implies there exists $j \in I$ such that $K = H_j$.
2. If $(K_j)_{j \in J} \subseteq (H_i)_{i \in I}$ is a directed family of subgroups of $G$ with $\bigcup_{j \in J} K_j \subseteq (H_i)_{i \in I}$, then there are $j \in J$ and $i \in I$ such that $K_j = H_i$.

We already know that $(\mathcal{L}(G), \subseteq)$ is an algebraic domain. From Corollary II-1.15 in [77], we can give the following result.

**Theorem 4.8.** The Scott topology on $\mathcal{L}(G)$ has a basis formed from the sets $\uparrow H = \{K \leq G \mid K \supseteq H\}$ where $H \in F(\mathcal{L}(G))$.

Moreover, if $(D, \sqsubseteq)$ is a continuous domain with basis $B$, we can prove that each open set $O$ in $D$ can be expressed as the union $O = \bigcup_{x \in O \cap B} \{y \in D \mid y \gg x\}$ [1].

**Corollary 4.1.** Let $(H_i)_{i \in I}$ be an open set in $\mathcal{L}(G)$. Then for each $j \in I$ there exists $k \in I$ such that $H_k$ is finitely generated and $H_j \supseteq H_k$.

A set in $(\mathcal{L}(G), \subseteq)$ is Scott-compact if it is topologically compact with respect to the Scott topology. A set in $(\mathcal{L}(G), \subseteq)$ is saturated if it is the intersection of some open sets in $(\mathcal{L}(G), \subseteq)$. Using properties of Sober spaces we can prove that in an algebraic domain a set is Scott-open iff it is Scott-compacted and saturated (see [77]).

**Theorem 4.9.** Let $(H_i)_{i \in I}$ be a set of elements in $\mathcal{L}(G)$. Then $(H_i)_{i \in I}$ is Scott-open if and only if $(H_i)_{i \in I}$ is Scott-compacted and saturated.
**Definition 4.10.** A function $f : \mathcal{L}(G) \rightarrow \mathcal{L}(G)$ is called *Scott-continuous* if and only if it is topologically continuous with respect to the Scott topology over $\mathcal{L}(G)$.

**Theorem 4.10.** A function $f : \mathcal{L}(G) \rightarrow \mathcal{L}(G)$ is Scott-continuous if and only if $f$ is monotone and for each directed family $(H_i)_{i \in I}$ of subgroups of $G$ we have $f(\bigcup_{i \in I} H_i) = \bigcup_{i \in I} f(H_i)$.

**Proof.** Let $f : \mathcal{L}(G) \rightarrow \mathcal{L}(G)$ be a Scott-continuous function. We show the monotonicity of $f$. Let $H, K \leq G$ with $H \subseteq K$. The set $\downarrow f(K) = \{ U \leq G \mid U \subseteq f(K) \}$ is a principal ideal, and hence it is a Scott-closed set. Since $f$ is topologically continuous, we have that $f^{-1}(\downarrow f(K))$ is Scott-closed, and so it is a lower set. Since $K \in f^{-1}(\downarrow f(K))$ and $H \subseteq K$, we have $H \in f^{-1}(\downarrow f(K))$. This means $f(H) \subseteq f(K)$ and $f$ is monotone. Let $(H_i)_{i \in I}$ be a directed family of subgroups of $G$. The set $A = \downarrow (\bigcup_{i \in I} f(H_i))$ is Scott-closed and hence $f^{-1}(A)$ is Scott-closed. Since $(H_i)_{i \in I} \subseteq f^{-1}(A)$, it follows that $\bigcup_{i \in I} H_i \in f^{-1}(A)$. This means $f\left(\bigcup_{i \in I} H_i\right) \subseteq \bigcup_{i \in I} f(H_i)$. The converse inclusion follows from the monotonicity of $f$.

Let us suppose now that $f$ is monotone and for each directed family $(H_i)_{i \in I}$ of subgroups of $G$ we have $f(\bigcup_{i \in I} H_i) = \bigcup_{i \in I} f(H_i)$. We show that $f$ is topologically continuous. Let $O$ be an open subset in $\mathcal{L}(G)$. Clearly, $O$ is an upper set and then $f^{-1}(O)$ is an upper set because $f$ is monotone. Let $(H_i)_{i \in I}$ be a directed family of subgroups of $G$ whose supremum $H = \bigcup_{i \in I} H_i$ belongs to $f^{-1}(O)$. This means $f(\bigcup_{i \in I} H_i) = \bigcup_{i \in I} f(H_i) \in O$. Because $O$ is Scott-open we can find $j \in I$ such that $f(H_j) \in O$, that is, $H_j \in f^{-1}(O)$. We proved that $f^{-1}(O)$ is Scott-open and $f$ is Scott-continuous.

**Theorem 4.11.** A function $f : \mathcal{L}(G) \rightarrow \mathcal{L}(G)$ is Scott-continuous if and only if for each $H \leq G$ and each $K \leq G$ finitely generated with $K \ll f(H)$ there exists $L \leq G$ finitely generated with $L \ll H$ such that “$L \subseteq U$ implies $K \subseteq f(U)$” for each subgroup $U$ of $G$.

**Proof.** We denote by $F(\mathcal{L}(G))_H$ the set of all finitely generated subgroups of $G$ approximating $H$. From Theorem 4.6, we know that $F(\mathcal{L}(G))$ is a bases in $\mathcal{L}(G)$. From the general theory of basis, we have that $F(\mathcal{L}(G))_H$ is directed and each subgroup $H$ of $G$ can be expressed as $H = \bigcup_{H' \in F(\mathcal{L}(G))_H} H'$.

Let us suppose that the function $f : \mathcal{L}(G) \rightarrow \mathcal{L}(G)$ is Scott-continuous and $H \leq G$. According to Theorem 4.10, we have $f(H) = \bigcup_{H' \in F(\mathcal{L}(G))_H} f(H')$. If $K \leq G$ is finitely generated with $K \ll f(H)$ there exists $L \in F(\mathcal{L}(G))_H$ such that $K \subseteq f(L)$. If $U$ is another subgroup of $G$ such that $L \subseteq U$, we also have $K \subseteq f(L) \subseteq f(U)$ because $f$ is monotone by Theorem 4.10.

It remains to prove the converse implication. We start by making the remark that $F(\mathcal{L}(G))_H \subseteq \{ L \mid L \subseteq K \}$ implies, by taking the supremum, that $H \subseteq K$. This implication is true for all subgroups $H$ and $K$ of $G$. 

Let us prove first that \( f \) is monotone. Let \( H_1, H_2 \leq G \) with \( H_1 \subseteq H_2 \). We suppose that \( f(H_1) \not\subseteq f(H_2) \). This means that there exists a finitely generated subgroup \( K \) of \( G \) with \( K \not\ll f(H_1) \) but \( K \not\ll f(H_2) \). For \( K \), there exists a finitely generated subgroup \( L \) of \( G \) with \( L \ll H_1 \) for which we have the implication: \( L \subseteq U \) implies \( K \subseteq f(U) \) for each subgroup \( U \) of \( G \). However, \( L \subseteq H_2 \), and we must have \( K \subseteq f(H_2) \). We get a contradiction with the choice of \( K \), and hence \( f \) is monotone.

Let \( (H_i)_{i \in I} \) be a directed family of subsets of \( G \). We denote by \( H \) the supremum of this family, i.e. \( H = \bigcup_{i \in I} H_i \). Because \( f \) is monotone, we have \( \bigcup_{i \in I} f(H_i) \subseteq f(H) \).

We suppose that \( f(H) \not\subseteq \bigcup_{i \in I} f(H_i) \). This means there exists a finitely generated subgroup \( K \ll f(H) \) with \( K \not\subseteq \bigcup_{i \in I} f(H_i) \). For this \( K \) we can find a finitely generated subgroup \( L \) of \( G \) with \( L \ll H \) for which we have the implication: \( L \subseteq U \) implies \( K \subseteq f(U) \) for each subgroup \( U \) of \( G \). However, \( H = \bigcup_{i \in I} H_i \). From the definition of the approximation relation, we have that there exists \( i \in I \) such that \( L \subseteq H_i \). We now obtain \( \bigcup_{i \in I} f(H_i) \supseteq f(H_j) \supseteq f(L) \supseteq K \). We get a contradiction because we chose \( K \not\subseteq \bigcup_{i \in I} f(H_i) \). Now, we have \( f(\bigcup_{i \in I} H_i) = \bigcup_{i \in I} f(H_i) \), and by Theorem 4.10 we obtain that \( f \) is Scott-continuous.

From the general theory of domains, we know that each continuous domain \((D, \sqsubseteq)\) with basis \( B \) is canonically isomorphic to \( \text{Id}(B, \ll) \), where \( \text{Id}(B, \ll) \) is the ideal completion of \( B \), i.e. the set of all ideals (directed lower sets) of \((B, \ll)\) ordered by inclusion. The required isomorphism is given by \( f : \text{Id}(B, \ll) \rightarrow D \) defined by \( f(A) = \sqcup A \) for each ideal \( A \) in \((B, \ll)\), and \( g : D \rightarrow \text{Id}(B, \ll) \) which maps each \( x \) in \( D \) into the directed set of elements in \( B \) approximating \( x \).

Also, for each dcpo \( E \) and for each monotone map \( h : B \rightarrow E \) we can find a continuous function \( \tilde{h} : \text{Id}(B, \ll) \rightarrow E \) defined by \( \tilde{h}(A) = \sqcup h(A) \). The continuity of \( h \) follows by applying the associativity of suprema and Theorem 4.10. Each continuous function \( \alpha \) from \( D \) to another dcpo \( E \) can be expressed as \( \alpha = \alpha|_B \circ g \) because of the definition of the basis \( B \). However, \( g : D \rightarrow \text{Id}(B, \ll) \) is completely determined only by \( D \) and \( B \). Also, \( \alpha|_B : \text{Id}(B, \ll) \rightarrow E \) is completely determined by \( \alpha : D \rightarrow E \) which is the restriction of \( \alpha \) to \( B \). Therefore, each continuous function from the domain \( D \) to the dcpo \( E \) is completely determined by its restriction to the basis \( B \) of \( D \). A complete calculation is presented in [1] and [77]. We can give the following result.

**Theorem 4.12.** A continuous function \( f : \mathcal{L}(G) \rightarrow \mathcal{L}(G) \) is completely determined by its values on the finitely generated subgroups of \( G \).

Several fixed-point theorems in general order theory remain valid for the domain \((\mathcal{L}(G), \subseteq)\). Tarski’s fixed-point theorem states that, whenever \( L \) is a complete lattice and \( f : L \rightarrow L \) is a monotone map, we have that \( \text{fix}(f) = \{ x \in L \mid x = f(x) \} \) is non-empty. Moreover, \( \text{fix}(f) \) forms another complete lattice (Theorem 0-2.3 in [77]). We particularize this theorem to \((\mathcal{L}(G), \subseteq)\) which is a complete lattice.
Theorem 4.13. Each monotone function \( f : \mathcal{L}(G) \to \mathcal{L}(G) \) has a fixed point. The least of them is given by \( \cap \{ H \leq G \mid f(H) \subseteq H \} \), and the largest by \( \cup \{ H \leq G \mid H \subseteq f(H) \} \).

In the case of continuous functions things are more clear. We have a uniform canonical method for constructing the fixed points of a continuous function on a pointed dcpo (i.e. a dcpo with a least element). From Proposition II-2.4 in [77], we know that, whenever \((D, \sqsubseteq, \bot)\) is a pointed dcpo (the least element of \(D\) is denoted by \(\bot\)) and \(f : D \to D\) is a continuous function, there is a least fixed point of \(f\) which is given by \( \text{fix}(f) = \sup \{ f^n(\bot) \mid n \in \mathbb{N} \} \). Moreover, from Theorem 2.1.19 in [1], the map \( \text{fix} : [D \to D] \to D \), \( f \mapsto \text{fix}(f) \) is also continuous.

Theorem 4.14. Each continuous function \( f : \mathcal{L}(G) \to \mathcal{L}(G) \) has a least fixed point. It is given by \( \bigcup_{n \in \mathbb{N}} f^n(\{e\}) \) where \( e \) is the identity element in \( G \).

4.4.3 Topological Properties of the Group of Permutations of Atoms in EFM Set Theory

The results in previous subsections are presented in the general case when \( G \) is an arbitrary group. A particular class of groups is represented by the locally finite groups, which are groups all of whose finitely generated subgroups are also finite. Therefore, if \( G \) is a locally finite group, then a subgroup \( H \) of \( G \) is finitely generated if and only if \( H \) is finite. The results presented in previous subsections can be particularized to locally finite groups by replacing “finitely generated” with “finite”.

Let \( G \) be a locally finite group. We have that \( \mathcal{L}(G) \) is an algebraic domain, and the smallest basis in \( \mathcal{L}(G) \) (i.e. the set of all compact elements in \( \mathcal{L}(G) \)) is formed precisely from the finite subgroups of \( G \). The Scott topology on \( \mathcal{L}(G) \) has a basis formed from the sets \( \uparrow H = \{ K \leq G \mid K \supseteq H \} \) where the subgroups \( H \) are precisely the finite subgroups of \( G \). A continuous function \( f : \mathcal{L}(G) \to \mathcal{L}(G) \) is completely determined by its values on the finite subgroups of \( G \). A function \( f : \mathcal{L}(G) \to \mathcal{L}(G) \) is Scott-continuous if and only if for each \( H \leq G \) and each \( K \leq G \) finite with \( K \ll f(H) \) there exists \( L \leq G \) finite with \( L \ll H \) such that “\( L \subseteq U \) implies \( K \subseteq f(U) \)” for each subgroup \( U \) of \( G \). Whenever \( H \ll K \) in \( \mathcal{L}(G) \) we can interpolate a finite subgroup of \( G \) between \( H \) and \( K \). All these results are valid whenever \( G \) is a locally finite group. There are some important classes of locally finite groups for which the results presented before look quite interesting. Some examples of locally finite groups (for which the previous results are valid) are infinite direct sums of finite groups [130], Hamiltonian groups, i.e. the non-abelian groups all of whose subgroups are normal [130], and torsion solvable groups [61]. For these particular classes of groups we obtain interesting results using the general order theory for groups and the local finiteness property. For example: if \( G \) is a torsion solvable group, then the Scott topology on \( \mathcal{L}(G) \) has a basis formed from the sets \( \uparrow H = \{ K \leq G \mid K \supseteq H \} \) where the subgroups \( H \) are precisely the finite subgroups.
of $G$; if $G$ is a Hamiltonian group, then a continuous function $f : \mathcal{L}(G) \to \mathcal{L}(G)$ is completely determined by its values on the finite subgroups of $G$.

An important locally finite group, namely $P_A$, is presented in Section 4.3. First we make the remark that none of the results presented in this section, except Theorem 4.9, uses any form of choice in its proof. The definitions and results presented in this section, except Theorem 4.9, are also valid if we employ the axioms of EFM set theory instead of the axioms of the usual ZF set theory. The indexing of several families of subgroups in this section was done only for ease of expression; it does not play a special role. So, to avoid any logical contradiction in EFM we can present these families without using indexes; some examples of how we can express the results in this section without using indexes are Theorem 4.17 and Theorem 4.19. From Theorem 4.4, we know that $P_A$ is locally finite, which means that the set of finitely generated subgroups of $P_A$ is identical with the set of finite subgroups of $P_A$. Since the results presented in this section, except Theorem 4.9, keep the same proofs (which do not use AC) if we work with the EFM axioms, we can present several properties of $P_A$ in EFM.

From Theorem 4.6 and Theorem 4.4 we obtain the following result.

**Theorem 4.15.** $\mathcal{L}(P_A)$ is an algebraic domain and the smallest basis in $\mathcal{L}(P_A)$ (i.e. the set of all compact elements in $\mathcal{L}(P_A)$) is formed precisely from the finite subgroups of $P_A$.

Theorem 4.8 and Theorem 4.4 provide a description of a topological basis for the Scott topology over $\mathcal{L}(P_A)$.

**Theorem 4.16.** The Scott topology on $\mathcal{L}(P_A)$ has a basis formed from the sets $\uparrow H = \{K \leq P_A | K \supseteq H\}$ where the subgroups $H$ are precisely the finite subgroups of $P_A$.

From Corollary 4.1 and Theorem 4.4, we also get the following result.

**Theorem 4.17.** Let $\mathcal{F}$ be an open set in $\mathcal{L}(P_A)$ (i.e. an open family of subgroups with respect to the Scott topology). Then for each subgroup $H$ of $P_A$ which belongs to $\mathcal{F}$, there exists a finite subgroup $K$ of $P_A$ with the property that $K \in \mathcal{F}$ and $H \supseteq K$.

From Theorem 4.12, we know that a continuous function on a subgroup lattice is completely determined by its behaviour on a basis. In this way, because of Theorem 4.4, we obtain the following.

**Theorem 4.18.** A continuous function $f : \mathcal{L}(P_A) \to \mathcal{L}(P_A)$ is completely determined by its values on the finite subgroups of $P_A$.

Theorem 4.10 can be easily translated into the EFM framework. We obtain the following theorem.

**Theorem 4.19.** A function $f : \mathcal{L}(P_A) \to \mathcal{L}(P_A)$ is Scott-continuous if and only if $f$ is monotone and for each directed family $\mathcal{F}$ of subgroups of $G$ we have $f(\bigcup_{H \in \mathcal{F}} H) = \bigcup_{H \in \mathcal{F}} f(H)$. 
From Theorem 4.11 and Theorem 4.4, we get a continuity criterion.

**Theorem 4.20.** A function $f : \mathcal{L}(P_A) \to \mathcal{L}(P_A)$ is Scott-continuous if and only if for each $H \leq P_A$ and each $K \leq P_A$ finite with $K \ll f(H)$ there exists $L \leq P_A$ finite with $L \ll H$ such that “$L \subseteq U$ implies $K \subseteq f(U)$” for each subgroup $U$ of $P_A$.

An interpolation property in $\mathcal{L}(P_A)$ follows from Proposition 4.7 and Theorem 4.4.

**Theorem 4.21.** Whenever $H \ll K$ in $\mathcal{L}(P_A)$ we can interpolate a finite subgroup of $P_A$ between $H$ and $K$.

A fixed-point theorem in the domain $\mathcal{L}(P_A)$ is obtained from Theorem 4.14 and Theorem 4.4.

**Theorem 4.22.** Each continuous function $f : \mathcal{L}(P_A) \to \mathcal{L}(P_A)$ has a least fixed point. It is given by $\bigcup_{n \in \mathbb{N}} f^n(\{id_A\})$ where $id_A$ is the identity map on $A$.

In FSM, we have already proved that the subgroup lattice $\mathcal{L}(G)$, formed by the finitely supported subgroups of an invariant group $G$ is an invariant complete lattice and an invariant algebraic domain (see Subsection 3.4.4). In particular, according to Example 3.3, we have that $\mathcal{L}(S_A)$ formed by the finitely supported subgroups of $S_A$ is an invariant complete lattice and an invariant algebraic domain. Since in FM axiomatic set theory (and in FSM) the group $P_A$ coincides with $S_A$, and because every finite subset of an invariant set is finitely supported, it is easy to prove (similarly to Subsection 3.4.4) that the theorems in this subsection are consistent in FSM (if we reformulate them in terms of finitely supported objects). The complete calculations are left to the reader.

### 4.5 Renamings in the Extended Fraenkel-Mostowski Framework

In this section we analyze how some classical results of nominal logic are changed (or not) when we work in the EFM framework instead of the FM framework. We naturally extend some notions and results of nominal logic, and, together with some mathematical properties obtained in Section 4.3 and some additional combinatorial results (which remain valid in an axiomatic set theory where the axiom of choice is disallowed), we are able to give some new properties of permutative renamings. We deal with renamings induced by permutations, and not with renamings induced by substitutions and substitution actions. In fact, a link between these viewpoints is given by the fact that for a $\lambda$-calculus expression $t$ and two atoms $a$ and $b$, we have $\{b|a\}t = \alpha (ba) \cdot t$ for $b \notin fn(t)$. According to Theorem 2.3, the $\alpha$-equivalence in the $\lambda$-calculus can be described in terms of permutative renamings without it being necessary to define which are the free variables of a term.

**Definition 4.11.** Let $x$ be an element of an EFM set $X$. A **permutative renaming** of $x$ is an element of the form $\pi \cdot x$, where $\pi \in P_A$ and $\cdot : P_A \times X \to X$ is an extended interchange function on $X$. 
The same definition can be used to characterize the permutative renamings of elements of an FM set. If $x$ is an element of an FM set $X$, then a permutative renaming of $x$ is an element of the form $\pi \cdot x$, where $\pi \in P_A$ and $\cdot : P_A \times X \to X$ is an interchange function ($P_A$-interchange function) on $X$. It is worth noting that in FM, the notions of interchange function and $P_A$-interchange function have the same meaning because only finitary permutations are allowed in the FM universe.

In classical FM set theory, permutations are obtained by composing finitely many transpositions [74]. In this section, since we eliminate the finite support property from the FM axioms, we work in the general case where $P_A$ is the set of all bijections of $A$, $X$ is an EFM set and the extended interchange function is defined on $P_A$ not only on $S_A$ (like in [72, 74]). A permutative renaming in our approach is of the form $\pi \cdot x$, where $\pi \in P_A$. The notion of permutative renaming defined in [72] is a particular case of the notion of permutative renaming defined by Definition 4.11.

From now on, permutative renamings are simply called renamings. Let $G$ be a subgroup of $P_A$.

**Definition 4.12.**

1. The representation of $P_A$ by permutations of the EFM set $X$ is a group homomorphism $\varphi : P_A \to S_X$ defined by $\varphi(\pi)(x) = \pi \cdot x$, where $S_X$ is the symmetric group on $X$.

2. Let $x$ and $y$ be elements of an EFM set $X$.
   
   a. $x$ and $y$ are called equivalent, denoted by $x \sim y$, whenever we can obtain one from the other by a renaming;
   
   b. $x$ and $y$ are called equivalent under permutations in $G$, denoted by $x \sim_G y$, whenever we can obtain one from the other by a renaming under a permutation in $G$ (i.e. there is $\pi \in G$ such that $y = \pi \cdot x$).

3. Let $X$ be an EFM set.
   
   a. $\text{REN}(x) = \{ \pi \cdot x \mid \pi \in P_A \}$ is the set of all renamings of $x$; we also say that $\text{REN}(x)$ is a class of renamings in $X$.
   
   b. $\text{REN}_G(x) = \{ \pi \cdot x \mid \pi \in G \}$ is the set of all renamings of $x$ under the permutations in $G$; we also say that $\text{REN}_G(x)$ is a class of renamings in $X$ under permutations in $G$. A renaming of an (arbitrary) atom under the permutations in $G$ is called a $G$-renaming.

4. Let $X$ be an EFM set.
   
   a. $\text{IREN}(x) = \{ \pi \in P_A \mid \pi \cdot x = x \}$ is the set of permutations for which we obtain a fixed renaming of $x$ (a renaming which keeps $x$ unchanged).
   
   b. $\text{IREN}_G(x) = \{ \pi \in G \mid \pi \cdot x = x \}$ is the set of permutations in $G$ for which we obtain a fixed renaming of $x$.

5. Let $X$ be an EFM set.
   
   a. An element $x \in X$ for which $\text{IREN}(x) = P_A$ is called fixed on all renamings. The set of elements in $X$ which are fixed on all renamings is denoted by $\text{IRN}(X)$. 

b. An element $x \in X$ for which $IREN_G(x) = G$ is called **fixed on renamings under permutations in $G$**. The set of elements in $X$ which are fixed on renamings under permutations in $G$ is denoted by $IRN_G(X)$.

Let $X$ be an EFM set, and $G \leq P_A$. We have the following results which we present without proofs.

**Proposition 4.4.**

1. $\sim_G$ is an equivalence relation on $X$.
2. $REN_G(x)$ is the equivalence class of $x$ modulo $\sim_G$ which is the orbit of the element $x$ under the action $\cdot : G \times X \rightarrow X$ defined as the extended interchange function.
3. In terms of group theory, $IREN(x)$ is the stabilizer of $x$ under the extended interchange function, and $IREN_G(x)$ is the stabilizer of $x$ under the action $\cdot : G \times X \rightarrow X$ defined as the extended interchange function. A trivial consequence is that $IREN_G(x) \leq G$.

**Remark 4.8.** If $G$ is a finite subgroup of $P_A$, we denote by $\pi IREN_G(x)$ the left cosets modulo $IREN_G(x)$. A function $\psi : \{ \pi IREN_G(x) | \pi \in G \} \rightarrow REN_G(x)$ defined by $\psi(\pi IREN_G(x)) = \pi \cdot x$ is well defined, and it is a bijection. Thus, $|REN_G(x)| = [G : IREN_G(x)]$.

**Proposition 4.5.** Let $G$ be a finite subgroup of $P_A$ and $X$ a finite EFM set. Let $S'$ be a system of representatives for classes of renamings in $X$ under permutations in $G$, with at least two elements; such a system $S'$ exists because $X$ is finite, and the axiom of choice is not required (see Remark 4.5). Then, by using the class equation in group theory,

$$|X| = |IRN_G(X)| + \sum_{x \in S'} |REN_G(x)| =$$

$$|IRN_G(X)| + \sum_{x \in S'} |G : IREN_G(x)| =$$

$$= |IRN_G(X)| + \sum_{x \in S'} \frac{|G|}{|IREN_G(x)|}.$$

Let $IREN(\pi)$ be the set of $x \in X$ fixed under $\pi$, i.e. $IREN(\pi) = \{ x \in X | \pi \cdot x = x \}$. Let $G \leq P_A$ be a finite group of permutations. Then we can find the number of orbits under the extended interchange function for finite EFM sets.

**Proposition 4.6.** Let $X$ be a finite EFM set. If $G \leq P_A$ is finite, the number $k$ of classes of renamings in $X$ under the permutations in $G$ (i.e. the number $k$ of orbits in $X$ under the action $\cdot : G \times X \rightarrow X$ defined as the extended interchange function) is

$$k = \frac{1}{|G|} \sum_{\pi \in G} |IREN(\pi)|.$$
Proof. Let $M = \{(\pi, x) \in G \times X \mid \pi \cdot x = x\}$. We express $|M|$ in two ways.

We can build sets of representatives for finite families by using axioms 1-9 (see Remark 4.5). We have $(\pi, x) \in M$ iff $\pi \in IREN_G(x)$, so $M$ is the disjoint union of the sets $IREN_G(x) \times \{x\}$ ($x \in X$). Since $X$ is finite, there is only a finite number of such sets. Using Lagrange’s Theorem for finite groups and Remark 4.8,

$$|M| = \sum_{x \in X} |IREN_G(x)| = \sum_{x \in X} \frac{|G|}{|G : IREN_G(x)|} = \sum_{x \in X} \frac{|G|}{|IREN_G(x)|}. \quad (4.1)$$

According to Proposition 4.4, the classes of renamings in $X$ are orbits in $X$ under the action $\cdot : G \times X \rightarrow X$ defined as an extended interchange function. If these orbits are $X_1, X_2, \ldots, X_k$, then they form a partition of $X$. According to relation 4.1, we have

$$|M| = \sum_{i=1}^{k} \sum_{x \in X_i} \frac{|G|}{|IREN_G(x)|} = \sum_{i=1}^{k} \sum_{x \in X_i} \frac{|G|}{X_i} = \sum_{i=1}^{k} |G| = k \cdot |G|. \quad (4.2)$$

On the other hand, for a given $\pi \in G$, $(\pi, x) \in M$ iff $x \in IREN(\pi)$. Thus, $M$ is the disjoint union of the sets $\{\pi\} \times IREN(\pi)$ ($\pi \in G$). Finally,

$$|M| = \sum_{\pi \in G} |IREN(\pi)|. \quad (4.3)$$

From relations 4.2 and 4.3, we obtain the identity:

$$k = \frac{1}{|G|} \sum_{\pi \in G} |IREN(\pi)|.$$

All these identities do not use the axiom of choice. Since $G$ and $X$ are finite, all the results used in our proofs are counting problems, and so they can be obtained from the axioms of EFM set theory, especially by using the induction principle (which is valid in EFM set theory).

Remark 4.9. If $X$ is a finite FM set, $S$ supports each $x \in X$ and $G \leq P_A$ is finite, then the number $k$ of classes of renamings in $X$ under the permutations in $G$ (i.e. the number $k$ of orbits in $X$ under the action $\cdot : G \times X \rightarrow X$) is

$$k = \frac{1}{|G|} \sum_{\pi \in G} |IREN(\pi)| = \frac{1}{|G|} \left( \sum_{\pi \in G} |IREN(\pi)| + \sum_{\pi \in G} |IREN(\pi)| \right) =$$

$$= \frac{1}{|G|}(|Fix(S)||X| + \sum_{\pi \in G} |IREN(\pi)|) = \frac{|Fix(S)||X|}{|G|} + \sum_{\pi \in G} \frac{|IREN(\pi)|}{|G|}.$$

The following two properties of permutative renamings follow immediately from Theorem 4.3 and Theorem 4.4, respectively. According to the following results, we emphasize that, even if we use only axiom 11’ and the notion of extended interchange function to define the permutative renamings, these have similar properties
to the permutative renamings defined in [72] where the authors use axiom 11 (i.e.
the finite support property) and the notion of interchange function.

**Theorem 4.23.** Let \( x \) be an element of an arbitrary EFM set \( X \), and \( \pi \) an arbitrary permutation of atoms in \( A \). We can generate only a finite number of renamings of \( x \) by applying the extended interchange function to \( x \) and to each permutation obtained by composing \( \pi \) and \( \pi^{-1} \) multiple times (a permutation obtained by composing \( \pi \) and \( \pi^{-1} \) multiple times is of the form \( \pi^k \) for an arbitrary \( k \in \mathbb{Z} \)).

**Theorem 4.24.** Let \( x \) be an element of an arbitrary EFM set \( X \). If we consider a finite number of permutations, then we can generate only a finite number of renamings of \( x \) by applying the extended interchange function to \( x \) and to each composition of these permutations and their inverses.

**Corollary 4.2.** Let \( X \) be a finite EFM set, and let us consider a group \( G \) generated by \( \{\pi_1, \pi_2, \ldots, \pi_m\} \) where \( \pi_1, \pi_2, \ldots, \pi_m \in P_A \). Then the number \( k \) of classes of renamings in \( X \) under the permutations in \( G \) is

\[
k = \frac{1}{|G|} \sum_{\pi \in G} |IREN(\pi)|.
\]

**Proof.** The result follows from Proposition 4.6. According to Theorem 4.4, it follows that \( G \) is finite, and so Proposition 4.6 can be applied. \( \square \)

According to Theorem 4.5, we can say that Theorems 4.23 and 4.24 and Corollary 4.2 are also valid in FM set theory and in FSM.

### 4.6 Comments

The main goal of describing EFM set theory is to prove that some properties of \( P_A \) which are valid in the FM framework remain valid if, instead of axiom 11 in the description of FM set theory, we introduce the weaker axiom 11’ in the description of EFM set theory. For the proof of some important properties of \( P_A \) (for example Theorems 4.3 and 4.4) we do not necessarily need to assume that for each element in an FM set there is a finite non-empty set supporting it as we did in the axiomatic description of FM set theory. To prove these properties of \( P_A \), instead of axiom 11, we use only a consequence of it (i.e. axiom 11’) which says that each subset of \( A \) is either finite or cofinite. This axiom is actually equivalent only to the assertion that every set of atoms (and not necessarily every arbitrary set) is finitely supported.

In Section 4.3 we prove that the domain of the extended interchange function defined in the EFM framework (see Definition 4.5) and the domain of the interchange function defined in the FM framework (see Definition 2.10) have similar algebraic properties. In Section 4.4 we present several order and topological properties of the group \( P_A \) which are expressed in terms of finite subgroups. These properties are related to the similar results obtained in FSM in Subsection 3.4.4. In Section 4.5 we
prove that some properties of renamings which are valid in the FM framework (for example Theorems 4.23 and 4.24 and Corollary 4.2) remain valid in the EFM framework. The main results in this chapter were published by us in [7], [12] and [16].

We do not say that EFM set theory is better than FM set theory. The finite support property has important benefits (some of them are presented for example in Chapters 3 and 5). However, we want to emphasize that we can relax the set of axioms of FM set theory and the effect is that, for the group of all bijections of atoms, we obtain similar algebraic order and topological properties in both the FM and EFM frameworks.
Chapter 5
Process Calculi in Finitely Supported Mathematics

Abstract The aim of this chapter is to present a set of compact transition rules (transition rules without side conditions) for the monadic version of the fusion calculus (update calculus). These transition rules are expressed using the quantifier $\forall$ and the freshness quantifier $\forall$. Using some results presented in the second chapter of this book, we are able to compare the new semantics of the monadic fusion calculus with its related known semantics.

5.1 Introduction and Methods

In this chapter, we provide an algorithm to describe an FSM semantics for a certain process calculus. To save space, we show how this algorithm works for the particular example of the monadic fusion calculus. However, the algorithm can be successfully applied in the same way to other process calculi such as the $\pi$-calculus [9] or the $\pi I$-calculus [5, 11]. A short presentation of some FSM semantics for these process calculi is made in Section 5.4.

The $\pi$-calculus [137] was designed to be a foundation for concurrent computation, in the same way as the $\lambda$-calculus is a foundation for sequential computation. Communication between processes in the $\pi$-calculus is realized by communication channels. Programs in the $\pi$-calculus are systems of parallel processes that synchronize via message-passing handshakes on named channels. A benefit of the $\pi$-calculus is that the channels may be restricted (only certain processes may communicate on them). When a process sends a restricted name as a message to a process outside the scope of the restriction, the scope is said to extrude, that is, it enlarges to embrace the process receiving the channel. The communication possibilities of a process may change over time; a process may learn the names of new channels via scope extrusion. Thus, a channel is a transferable capability for communication. The $\pi I$-calculus (or simply $\pi I$) was introduced by Sangiorgi in [136]; it is a variant of the $\pi$-calculus in which free outputs are disallowed.
The fusion calculus has emerged as a good foundation model for distributed computation paradigms such as web services and service-oriented architectures. The monadic fusion calculus (also called the update calculus) was presented for the first time in [116]. It contains the monadic $\pi$-calculus as a proper subcalculus (as is proved in Section 2.3 from [116]), and thus inherits all its expressive power. Therefore, everything that can be done in the monadic $\pi$-calculus can be done in the update calculus without added complications. However, the update calculus has only one binding operator, whereas the $\pi$-calculus has two (binding of input variables and restriction of communication channels). Furthermore, there is a complete symmetry between input and output actions in the update calculus, which does not occur in the $\pi$-calculus. This is due to the fact that, in the $\pi$-calculus, input entails a binding while output does not.

We employ FSM results to obtain an FSM semantics of the update calculus. We use the freshness quantifier $\mathcal{N}$, which provides the possibility of removing the free variables (which are represented by the notion of finite support) from the scope of a rule: $\mathcal{N}x$ means that $x$ can be fresh for other parts of an expression. For example, $\forall x . \mathcal{N}y . \forall z . expression$ is true iff $\forall x, y, z . (y \text{ is fresh for } x) \Rightarrow (expression)$. We prove several FSM properties of the binding operator of the monadic fusion calculus (namely scope) which allow us to make a comparison between the FSM semantics of this process calculus and the other known semantics defined before.

The central idea of this chapter is to use atoms to represent variable symbols and FSM abstraction to represent the binding operator. A mixing of $\forall$ and $\mathcal{N}$ is used to replace the side conditions in the transition rules of the monadic fusion calculus. Finally, we prove that the new semantics of the monadic fusion calculus and its original semantics presented in [116] are equivalent. Several results of this type were also obtained in [9] and [5, 11] for the $\pi$-calculus, and for the $\piI$-calculus, respectively. In [9] the authors proved that the FSM semantics and the late semantics of the $\pi$-calculus are completely equivalent. Analogously, the FSM semantics and the original semantics of the $\piI$-calculus presented in [136] have the same expressive power. The main results from [9] and [11] are presented in Section 5.4 without proofs. However, for a complete presentation we recommend the related references with the remark that in these references we used the term ‘nominal’ instead of ‘FSM’.

### 5.2 A Case Study: The Monadic Fusion Calculus

The monadic version of the fusion calculus (also called the update calculus) was presented in [116]. It contains the monadic $\pi$-calculus as a proper subcalculus. However, there are some differences between the update calculus and the monadic $\pi$-calculus. In the update calculus the input action does not bind names. The effect of an interaction is that the output and the input names become identified in what is called an update. There are two differences between updates and $\pi$-calculus interactions: the effect of an update is not necessarily local but regulated by the use of a
scope operator, and updates are symmetric with respect to the input-output polarities. The only binding operator in the update calculus is called scope and is denoted by \((x)P\), meaning that \(x\) is local in \(P\). In a sense, it is a common denominator of input binding and restriction in the \(\pi\)-calculus. Restriction implies that no name will ever replace bound names, while input binding requires that the bound name is immediately replaced by something received along the communication channel. Scope neither forbids nor forces a replace; it merely states the extent of the name.

We assume an infinite set of names ranging over \(u,v,...,x,y,...\). As in the \(\pi\)-calculus, names are used to represent communication channels, values and placeholders for channels and values. Processes are defined by

\[ P,Q ::= 0 \mid z[x].P \mid z[x].P \mid P + Q \mid P|Q \mid (x)P. \]

The empty process is denoted by \(0\). The output-guarded process \(z[x].P\) sends an object \(x\) along a channel \(z\) and then, after the output is completed, continues as \(P\). The input-guarded process \(z[x].P\) receives an object along the channel \(z\), and replaces \(x\) with that object; after the input is completed, it continues as \(P\). Contrary to the \(\pi\)-calculus, \(x\) is not bound in \(z[x].P\). As in the \(\pi\)-calculus, \(P + Q\) represents nondeterministic choice and \(P \mid Q\) represents parallel composition (that is, components \(P\) and \(Q\) can proceed independently and can interact via shared channels). The scope \((x)P\) limits the scope of \(x\) to \(P\); scopes can be used to delimit the extent of updates (that is, update effects with respect to \(x\) are limited to \(P\)). The name \(x\) is said to be bound in \((x)P\). The free names \(fn(P)\) are the names with a non-bound occurrence in \(P\).

**Definition 5.1.** (\(\alpha\)-convertibility)

1. If a name \(y\) does not occur in the process \(P\), then \(P\{y|z\}\) is the process obtained by replacing each free occurrence of \(z\) in \(P\) by \(y\).
2. A change of bound names in a process \(P\) is the replacement of a subterm \((x)Q\) of \(P\) by \((y)Q\{y|x\}\), where \(y\) does not occur in \(Q\).
3. Two processes \(P\) and \(Q\) are \(\alpha\)-convertible (and this is denoted by \(P \equiv_{\alpha} Q\)) if \(Q\) can be obtained from \(P\) by a finite number of changes of bound names.

It is easy to note that \(\alpha\)-convertibility in the update calculus is similar to the \(\alpha\)-equivalence in the \(\lambda\)-calculus. In FSM we are able to prove mathematically (as in Example 2.4) that \(\alpha\)-convertible processes are identical, whilst in [116] this fact was assumed by an informal agreement.

The actions of the update calculus are defined by

\[ \gamma ::= z[x] \mid z[x] \mid [x/z] \mid 1 \mid (x)z[x] \mid (x)z[x]. \]

An output action \(z[x]\) is similar to the free output in the \(\pi\)-calculus; \(z[x]\) means “send the object \(x\) along the channel \(z\)”. An input action \(z[x]\) means “receive an object along the channel \(z\) and replace \(x\) with that object”. Contrary to the situation in the \(\pi\)-calculus, this action does not bind \(x\), which means that the scope of \(x\) is not bound by the action. The update action \([x/z]\) (which does not appear in the \(\pi\)-calculus) indicates the replacement of all \(z\) by \(x\). An action \([x/x]\) is called “inert” and is denoted by \(1\) (because the choice of \(x\) in \([x/x]\) is not important).
The actions $z[x], z[x]$ and $[x/z]$ are called free actions, and are generically denoted by $\alpha$. The object $x$ of all these actions (except 1 which has no object) is free in these actions. Free actions have no bound names. A transition labelled with a free action is denoted by $P \xrightarrow{\alpha} Q$.

The actions $(x)z[x]$ and $(x)z[x]$ are called bound actions, and the name $x$ is bound in these actions. A transition labelled with an action (either free or bound) is denoted by $P \xrightarrow{\gamma} Q$. The meaning of a bound action is simply that the object is emitted out of its scope, and must therefore not be confused with any name from the environment.

We denote by $n(\gamma), fn(\gamma)$ and $bn(\gamma)$ all the names, free names and bound names occurring in $\gamma$, respectively. By definition, $n(1) = 0$.

<table>
<thead>
<tr>
<th>$\gamma$</th>
<th>$n(\gamma)$</th>
<th>$fn(\gamma)$</th>
<th>$bn(\gamma)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$z[x]$</td>
<td>${x, z}$</td>
<td>${x, z}$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$z[x]$</td>
<td>${x, z}$</td>
<td>${x, z}$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$[x/z]$</td>
<td>${x, z}$</td>
<td>${x, z}$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$1$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$(x)z[x]$</td>
<td>${x, z}$</td>
<td>${z}$</td>
<td>${x}$</td>
</tr>
<tr>
<td>$(x)z[x]$</td>
<td>${x, z}$</td>
<td>${z}$</td>
<td>${x}$</td>
</tr>
</tbody>
</table>

A structural congruence relation can be defined over the set of processes. To define a structural congruence, we need the notions of context and congruence. A minor auxiliary definition is required for sums: an occurrence of 0 in a process is degenerate if it is either the left or right term in a sum $P + Q$, and non-degenerate otherwise. Informally, a context differs from a process only in having a hole $[\cdot]$ in it. A context is regarded as a syntactic entity that transforms processes into processes.

**Definition 5.2.** A context is obtained when the hole $[\cdot]$ replaces a non-degenerate occurrence of 0 in a process. If $C$ is a context and $P$ a process, we write $C[P]$ for the process obtained by replacing the hole $[\cdot]$ in $C$ by $P$.

This replacement is literal, and so names free in $P$ may become bound in $C[P]$.

An equivalence relation $\mathcal{R}$ on processes is a congruence if $(P, Q) \in \mathcal{R}$ implies $(C[P], C[Q]) \in \mathcal{R}$ for every context $C$.

**Definition 5.3.** The relation $\equiv$ over the set of processes is called a structural congruence and it is defined as the smallest congruence which satisfies:

- $P \equiv Q$ if $P \equiv \alpha Q$
- $P + 0 \equiv P$, $P + Q \equiv Q + P$
- $(P + Q) + R \equiv P + (Q + R)$
- $P \mid 0 \equiv P$, $P \mid Q \equiv Q \mid P$
- $(P \mid Q) \mid R \equiv P \mid (Q \mid R)$
- $(x)0 \equiv 0$, $(x)(y)P \equiv (y)(x)P$
- $(x)(P + Q) \equiv (x)P + (x)Q$
- $(x)(P \mid Q) \equiv P \mid (x)Q$ if $x \not\in fn(P)$. 

Definition 5.4. The following labelled transition rules define the Parrow-Victor (PV) semantics of the update calculus:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Transition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OUT</strong></td>
<td>$z[x].P \xrightarrow{uc} P$</td>
</tr>
<tr>
<td></td>
<td>$P \xrightarrow{uc} P'$</td>
</tr>
<tr>
<td><strong>SUM</strong></td>
<td>$P + Q \xrightarrow{uc} P'$</td>
</tr>
<tr>
<td></td>
<td>$P \xrightarrow{uc} P'$</td>
</tr>
<tr>
<td><strong>PAR</strong></td>
<td>$P</td>
</tr>
<tr>
<td></td>
<td>$P \xrightarrow{uc} P'$</td>
</tr>
</tbody>
</table>

**INP**

$z[x].P \xrightarrow{uc} P$

$P \xrightarrow{uc} P'$

**CONG**

$P = P', Q = Q'$, $P \xrightarrow{\gamma} Q$

$P' \xrightarrow{\gamma} Q'$

**COM**

$P [\gamma/v] P'$

$P \xrightarrow{uc} P'$

$P | Q \xrightarrow{uc} P' | Q'$

**O-PASS**

$P \xrightarrow{uc} P'$

$z \neq x, y$

**I-PASS**

$P \xrightarrow{uc} P'$

$z \neq x, y$

**U-PASS**

$P \xrightarrow{uc} P'$

$z \neq x, y; x \neq y$

**1-PASS**

$P \xrightarrow{uc} P'$

$z \neq x$

**SCOPE**

$P \xrightarrow{uc} P'$

$y \neq z$

**I-OPEN**

$P \xrightarrow{uc} P'$

$z \neq x$

A transition of the form $P \xrightarrow{\gamma} P'$ symbolizes the transition of $P$ into $P'$ in the PV semantics of the update calculus labelled with an action (either free or bound). A transition of the form $P \xrightarrow{\alpha} P'$ symbolizes the transition of $P$ into $P'$ in the PV semantics of the update calculus labelled with a free action.

No premise in any transition rule of this PV semantics, except the premise of CONG, contains bound actions. In this operational semantics, the only rules for generating bound actions are CONG, O-PASS and I-PASS. In [116], the rules O-PASS and I-PASS were presented compressed as a single general rule for output and input named OPEN. Also in [116], instead of the rules O-PASS, I-PASS, U-PASS and 1-PASS there is a single rule PASS:

$P \xrightarrow{uc} P'$

$z \notin n(\alpha)$ which includes all our subcases. In fact, we split the rule PASS for every possible form of $\alpha$. 
The rules $U\text{-PASS}$ and $1\text{-PASS}$ have the form presented in Definition 5.4 because when $\alpha$ is the inert action $1 = [x/x]$, the names of $\alpha$ are $\emptyset$ and not $x$. However, our presentation is actually the same as the one given in [116], and only helps us later in presenting the FSM semantics of the update calculus.

The operational semantics of the monadic $\pi$-calculus [137] differs from that of the update calculus in the following way: there are no free input prefixes in the $\pi$-calculus, instead there is a bound input prefix written as $x(y).P$, where $x(y).P$ waits until a name is received along $x$, substitutes it for the bound variable $y$ and continues as $P$. In $x(y).P$, the name $y$ binds free occurrences of $y$ in $P$. For the binding of a name in a process $x(y).P$, the free occurrences of $y$ in $P$ indicate the places where the name received via $x$ will be substituted when the process acts. The input transition in the $\pi$-calculus is given by the rule $\text{INP}_\pi$:

$$\frac{}{x(y).P \xrightarrow{\pi}(y)[y] \rightarrow P}$$

There is no scoping operator in the $\pi$-calculus, but a related restriction operator $\text{new } x$, inheriting the rules $\text{PASS}$ and $\text{OPEN}$. There is no $\text{SCOPE}$ rule because the update actions are not present in the $\pi$-calculus. The interaction rule is

$$\text{COM}_\pi : \frac{P \xrightarrow{\pi}(y)[y], Q \xrightarrow{\pi} Q', x(z) \rightarrow Q'}{P \mid Q \xrightarrow{\pi} P' \{z[y]\} \mid Q'}$$

In the $\pi$-calculus, the action $x[y]$ is written as $x(y)$, the action $(y)x[y]$ is written as $x(y)$, and the action $(y)[y]$ is written as $x[y]$. The action $1$ is denoted by $\tau$ in the $\pi$-calculus. The $\pi$-calculus is isomorphic to a subcalculus of the update calculus formed by requiring that all input prefixes $z[x].P$ occur immediately under a scope $(x)$ of the object in the input prefix. This subcalculus is called the $\text{up}_{\pi}$-calculus. The isomorphism $\leftrightarrow$ between the $\text{up}_{\pi}$-calculus and the $\pi$-calculus is the homomorphism extension of the following two equivalences:

$$(x)z[x].P \leftrightarrow z(x).P,$$

and

$$(z)P \leftrightarrow \text{new } zP \quad \text{whenever } P \text{ is not a free input prefix}.$$
ZFA. Clearly, $A$ can be organized as an IFM set with the $S_A$-action defined in Example 2.1(1). Using the same arguments as in Example 2.4, we can say that the set of the fusion calculus terms forms an IFM set, and the set of fusion calculus terms modulo $\alpha$-conversion also forms an IFM set and an FM set. We can define the abstraction between a variable and a fusion calculus term in the sense of Definition 2.16. The variable $x$ is bound in the expression $(x)P$. In the FSM approach we use the notion of abstraction, and write this expression as $[x]P$. Thus, we can see bindings represented by the scope operator as abstractions defined in FSM (i.e. abstractive elements in the sense of Definition 2.16).

Remark 5.1. We recall that in the FSM approach there are no bound names. The “binding” made by the scope operator is related to Definition 2.16. However, the notion of FSM abstraction means that, when applying $[z]P$, we eliminate $z$ from $\text{supp}(P)$ which intuitively is a “binding of $\text{supp}(z)$ in $P$” (we know that $\text{supp}([z]P) = \text{supp}(P) - \{z\}$, and the support of a process $P$ is precisely the set of free names of $P$). From now on, for intuitive reasons, we will use the term bindings to denote these FSM abstractions generated by the scope operator.

In view of Remark 5.1 we can give the following definition.

Definition 5.5. Processes in the FSM fusion calculus are defined by the following grammar:

$$P, Q ::= 0 | z\lfloor x \rfloor . P | z\lceil x \rceil . P | P + Q | P \mid Q | [x]P.$$

Definition 5.6. Actions of the FSM fusion calculus are given by:

$$\gamma ::= z\lfloor x \rfloor | z\lceil x \rceil | [x/z] | 1 | [x]z\lfloor x \rfloor | [x]z\lceil x \rceil.$$

As in the PV semantics of the fusion calculus, $z\lfloor x \rfloor$, $z\lceil x \rceil$ and $[x/z]$ are the free actions and are generally denoted by $\alpha$. A transition labelled with a free action is denoted by $P \xrightarrow{\alpha} Q$ in the FSM semantics of the fusion calculus.

The actions $[x]z\lfloor x \rfloor$ and $[x]z\lceil x \rceil$ are called bound actions. In fact the bound actions $[x]z\lfloor x \rfloor$ and $[x]z\lceil x \rceil$ are actually the same as $(x)z\lfloor x \rfloor$ and $(x)z\lceil x \rceil$, respectively, but are denoted differently because we want to emphasize that we work in the framework of invariant sets. In fact “$[x]z\lfloor x \rfloor$” and “$[x]z\lceil x \rceil$” is an abuse of notation. We do not say that $x$ binds only in the action. The name $x$ in the actions $[x]z\lfloor x \rfloor$ and $[x]z\lceil x \rceil$ also binds into the derivate. Whenever we present a bound action of form $[x]z\lfloor x \rfloor$ we have an abstraction (in the sense of Definition 2.16) between the atom $x$ and Cartesian pair $(z\lfloor x \rfloor, \text{derivate})$, and analogously for $[x]z\lceil x \rceil$. A transition labelled with an action (either free or bound) is denoted by $P \xrightarrow{\gamma} Q$ in the FSM semantics of the fusion calculus.

We write $n(\gamma)$, $fn(\gamma)$ and $bn(\gamma)$ to mean all the names, free names and bound names respectively occurring in $\gamma$. By definition, $n(1) = \emptyset$. Since no such function as function as $bn$ is defined in the framework of invariant sets, we have:
A solution to present an FSM semantics for the fusion calculus is to rewrite the transition rules in the usual (PV) semantics of the fusion calculus highlighting the action each time. A common notation such as $bn$ cannot be used.

Using Proposition 2.16 we obtain a property of the binding operator in the fusion calculus.

**Proposition 5.1.** If $[x]P = [y]Q$, then one of the following statements is true:

- $x = y$ and $P = Q$.
- $x \neq y$ and $x \# Q$ and $P = (xy) \cdot Q$.

However, when $x \# Q$ we have $(xy) \cdot Q = Q \{x[y]\}$ [74]. From Proposition 5.1, it is clear that two processes in the fusion calculus coincide if and only if they are $\alpha$-convertible (we do not need to assume this by convention); we can prove this by induction on the structure of processes using Proposition 5.1.

**Definition 5.7.** The FSM structural congruence in the fusion calculus is the smallest equivalence relation (denoted by $\equiv_n$) on the set of processes closed under the rules:

1. Processes which are obtained from one another by an $\alpha$-conversion are congruent; in fact they are identified in FSM;
2. $\forall P, Q, R. \ P + 0 \equiv_n P, P + Q \equiv_n Q + P, (P + Q) + R \equiv_n P + (Q + R)$;
3. $\forall P, Q, R, P \ | \ 0 \equiv_n P, P \ | \ Q \equiv_n Q \ | \ P, (P \ | \ Q) \ | \ R \equiv_n P \ | \ (Q \ | \ R)$;
4. $\forall x, y, P, Q. \ [x]0 \equiv_n 0, [x][y]P \equiv_n [y][x]P, [x](P + Q) \equiv_n [x]P + [x]Q$;
5. $\forall P, Q, x. \ [x](P \ | \ Q) \equiv_n P \ | \ [x]Q$.

Note that the FSM structural congruence is not the equality relation in the framework of invariant sets. Clearly, equal processes are congruent. The converse is not valid. For example $[x][y]P = [y][x]P$ if and only if $x, y$ are fresh for $P$ (according to Proposition 2.16). However, we assume $[x][y]P \equiv_n [y][x]P$ for all $x, y$ and $P$. In fact, a rule of the form $\lceil x \rceil yP \equiv_n \lceil y \rceil xP$ only if $x, y$ are fresh for $P$ would be trivial because such a rule would be implied by rule number 1, which already states that $\alpha$-equivalent processes are congruent. Rule number 4 for FSM structural congruence does not contradict Proposition 2.16 because the FSM structural congruence and the equality are different equivalence relations.

We make the distinction between global binding (realized by quantifiers) and local binding (realized by the scope operator) in a rule (formula) from the FSM fusion calculus. If a variable appears bound once locally and another time globally in the same transition rule, this does not represent a logical contradiction. The binding provided by the scope operator (in the sense of Remark 5.1) is seen as a local binding.
only for the following process (for example in the expression $[x]P$, $x$ binds the free occurrences of $x$ only in $P$) and the binding made by the quantifiers $\forall$ and $\exists$ is seen as a global binding, for the entire rule (formula). So, in some rules it is possible to have expressions of the form $\forall x, \ldots, f_1([x]P, \ldots)$ and $\exists x, \ldots, f_2([x]P, \ldots)$. This does not mean that $x$ is bound twice in the same expression. We make the distinction between local binding (which is the binding only for the following process made by the scope operator) and global binding (which is the binding for the entire expression made by quantifiers). $\forall x, \ldots, f_1([x]P, \ldots)$ expresses that $f_1([x]P, \ldots)$ is valid and its validity does not depend on $x$. Also, $\exists x, \ldots, f_2([x]P, \ldots)$ means that $f_2([x]P, \ldots)$ is valid for all but finitely many $x$ (eventually the formula is valid iff $x$ is fresh for an expression or for a process). For example, the expression $\forall z, \exists x, \forall P, P', P z [x] \rightarrow_{nuc} P'$, where $\cdot \rightarrow_{nuc} \cdot$ we denote a transition in the FSM semantics of the fusion calculus, is correctly written even though we might be tempted to say that $x$ is bound twice. The variables $x$ and $z$ are globally bound once. The second binding, made by the scope operator, is a local one, and it is restricted to the process $P$ (or respectively to the action $[x]z[x]$). So, to say that

$$\forall z, \exists x, \forall P, P', P z [x] \rightarrow_{nuc} P'$$

is the same as saying that

$$P z [x] \rightarrow_{nuc} P'$$

if $x$ satisfies a cofiniteness condition (we will later prove that this condition is: $x$ is fresh for $z$).

**Definition 5.8.** The following labelled transition rules define the *FSM semantics* of the (monadic version of) the fusion calculus. A transition of the form $P \stackrel{\gamma}{\rightarrow} Q$ (where $\gamma$ is the action) in the FSM semantics of the monadic fusion calculus is denoted by $P \rightarrow_{nuc}^{\gamma} Q$.

1. $\forall x, z, P, z [x] \rightarrow_{nuc}^{[x]} P$
2. $\forall x, z, P, z [x] \rightarrow_{nuc}^{[x]} P$
3. $\forall \alpha, P, Q, P', P' \rightarrow_{nuc}^{\alpha} P'$
4. $\forall P, Q, P', Q', \gamma, P \equiv_n P', Q \equiv_n Q', P \rightarrow_{nuc}^{\gamma} Q$
5. \( \forall P, P', Q, \alpha. \frac{P | Q}{\alpha \mapsto P' | Q} \)
6. \( \forall x, y, z, P, P', Q, Q'. \frac{P \mid Q}{\alpha \mapsto P' \mid Q'} \)
7. \( \forall x, z, P, P'. \frac{P | \alpha \mapsto P'}{\alpha \mapsto [z]P \mid [z]P'} \)
8. \( \forall x, y, z, P, P'. \frac{P \mid [z]P}{\alpha \mapsto P' \mid [z]P'} \)
9. \( \forall x, y, z, P, P'. \frac{P \mid [z]P}{\alpha \mapsto P' \mid [z]P'} \)
10. \( \forall x, y, z, P, P'. \frac{P \mid [z]P}{\alpha \mapsto [z]P' \mid [z]P'} \)
11. \( \forall y, z, P, P'. \frac{P \mid [y]P}{\alpha \mapsto P' \mid [y]P'} \)
12. \( \forall x, y, z, P, P'. \frac{P \mid [x]P}{\alpha \mapsto P' \mid [x]P'} \)
13. \( \forall x, y, z, P, P'. \frac{P \mid [x]P}{\alpha \mapsto P' \mid [x]P'} \)

We are able to provide a mathematical proof of the equivalence of the PV and FSM semantics of the fusion calculus. First we define a set of transition rules in the form presented by Parrow and Victor [116] (assuming some cofiniteness conditions in the hypotheses of the rules). Next we prove that these rules are in fact identical to those in the FSM semantics of the fusion calculus.

**Definition 5.9.** A basic transition rule in the FSM semantics of (the monadic version of) the fusion calculus is in a **PV-FSM form (or in a PVn form, for short)** if it coincides with one of the following rules:

\[
\text{OUT}_{PV} : \quad [x]P \xrightarrow{\alpha \mapsto [x]P'} \quad \text{INP}_{PV} : \quad [x]P \xrightarrow{\alpha \mapsto [x]P'}
\]
We give some lemmas allowing us to prove that each transition rule in the FSM semantics of the fusion calculus can be presented in a PV-FSM form. Later we prove a result showing that the PV and the FSM semantics of the fusion calculus provide the same transitions.

The following lemma is trivial.

**Lemma 5.1.** 1. Rule number 1 in the FSM semantics of the fusion calculus is identical to rule OUTPV \( n \).
2. Rule 2 in the FSM semantics of the fusion calculus is identical to rule INPPV \( n \).
3. Rule 3 in the FSM semantics of the fusion calculus is identical to rule SUMPV \( n \).
4. Rule 4 in the FSM semantics of the fusion calculus is identical to rule CONGPV \( n \).
5. Rule 5 in the FSM semantics of the fusion calculus is identical to rule PARPV \( n \).
6. Rule 6 in the FSM semantics of the fusion calculus is identical to rule COMPV \( n \).
7. Rule 10 in the FSM semantics of the fusion calculus is identical to 1-PASSPV \( n \).

In view of Proposition 2.12 and Proposition 2.13, we are now able to provide the following results.

**Lemma 5.2.** Rule O-PASSPV \( n \) of Definition 5.9 is identical to rule number 7 in the FSM semantics of the fusion calculus.
Proof. Let \( p \) be the formula \( ∀P,P'.(P \xrightarrow{x,y}_{\text{nuc}} P' \text{ implies } \{z\}P \xrightarrow{x,y}_{\text{nuc}} \{z\}P') \) in the logic of FM. The free variables of \( p \) are contained in the set \( \{x,y,z\} \). Indeed, the set of free variables of \( p \) is formed only by \( x,y \) because \( P,P' \) are bound by the quantifier \( ∀ \), and \( z \) is bound by the scope operator; if we assume the free variables of \( p \) to be only the variables of \( p \) which are globally unbound, then these free variables of \( p \) would be \( x,y,z \) and again these are contained in the set \( \{x,y,z\} \). Now, because of Proposition 2.12 and Proposition ref4.4-11, we obtain the equivalence result \( ∀z.(z\#\{x,y\} \text{ implies } p) \) if and only if \( \mathcal{N}z.p \). Since \( x \) and \( y \) were arbitrarily chosen, we can say that rule \( O-PASSPv_n \) of Definition 5.9 is identical to rule number 7 in the FSM semantics of the fusion calculus.

\[\square\]

**Lemma 5.3.** Rule \( I-PASSPv_n \) of Definition 5.9 is identical to rule number 8 in the FSM semantics of the fusion calculus.

Proof. Let \( p \) be the formula \( ∀P,P'.(P \xrightarrow{x,y}_{\text{nuc}} P' \text{ implies } \{z\}P \xrightarrow{x,y}_{\text{nuc}} \{z\}P') \) in the logic of FM. The free variables of \( p \) are contained in the set \( \{x,y,z\} \). Indeed, the set of free variables of \( p \) is formed only by \( x,y \) because \( P,P' \) are bound by the quantifier \( ∀ \), and \( z \) is bound by the scope operator; if we assume the free variables of \( p \) to be only the variables of \( p \) which are globally unbound, then these free variables of \( p \) would be \( x,y,z \) and again these are contained in the set \( \{x,y,z\} \). Now, according to Proposition 2.12 and Proposition 2.13, we obtain the equivalence result \( ∀z.(z\#\{x,y\} \text{ implies } p) \) if and only if \( \mathcal{N}z.p \). Since \( x \) and \( y \) were arbitrarily chosen, we can say that rule \( I-PASSPv_n \) of Definition 5.9 is identical to rule number 8 in the FSM semantics of the fusion calculus.

\[\square\]

**Lemma 5.4.** Rule \( U-PASSPv_n \) of Definition 5.9 is identical to rule number 9 in the FSM semantics of the fusion calculus.

Proof. Let \( p \) be the formula \( ∀P,P'.(P \xrightarrow{x,y}_{\text{nuc}} P' \text{ implies } \{z\}P \xrightarrow{x,y}_{\text{nuc}} \{z\}P') \) in the logic of FM, and \( q \) be the formula \( \mathcal{N}z.∀P,P'.(P \xrightarrow{x,y}_{\text{nuc}} P' \text{ implies } \{z\}P \xrightarrow{x,y}_{\text{nuc}} \{z\}P') \) in the logic of FM (which is precisely \( \mathcal{N}z.p \)). The free variables of \( q \) are contained in the set \( \{x,y\} \). Indeed, the set of free variables of \( q \) is formed only by \( x,y \) because \( P,P' \) are bound by the quantifier \( ∀ \), and \( z \) is bound by the freshness quantifier; if we assume the free variables of \( q \) to be only the variables of \( q \) which are globally unbound, then these free variables of \( q \) would be \( x,y \) and again these are contained in the set \( \{x,y\} \). Now, because of Proposition 2.12 and Proposition 2.13, we obtain the equivalence result \( ∀y.(y\#x \text{ implies } q) \) if and only if \( \mathcal{N}y.q \). The free variables of \( p \) are contained in the set \( \{x,y,z\} \). Indeed, the set of free variables of \( p \) is formed only by \( x,y \) because \( P,P' \) are bound by the quantifier \( ∀ \), and \( z \) is bound by the scope operator; if we assume the free variables of \( p \) to be only the variables of \( p \) which are globally unbound, then these free variables of \( p \) would be \( x,y,z \) and again these are contained in the set \( \{x,y,z\} \). Now, according to Proposition 2.12 and Proposition 2.13, we obtain the equivalence result \( ∀z.(z\#\{x,y\} \text{ implies } p) \) if and only if \( \mathcal{N}z.p \).
5.3 FSM Semantics of the Fusion Calculus

Let us suppose that rule $U$-PASS$_{PV}$ of Definition 5.9 is valid. Let $y \# x$ be arbitrarily chosen (fixed). From $U$-PASS$_{PV}$, we know that “$\forall z.(z \# y \rightarrow y \# x)$” is valid; moreover, “$\forall z.(z \# y \rightarrow y \# x)$” is valid even when $x = y$ because of rule 1-PASS$_{PV}$. This means $\forall z.p$ is valid and hence $q$ is valid. So the implication “$\forall y.(y \# x \rightarrow y \# x)$” is valid and hence $\forall y.q$ is valid. Since $x$ was arbitrarily chosen, we can say that rule $U$-PASS$_{PV}$ of Definition 5.9 implies rule number 9 in the FSM semantics of the fusion calculus.

Conversely, let us choose an arbitrary atom $x$. Let us suppose that $\forall y.\forall z.p$ is valid, which means $\forall y.q$ is valid. Let $y \# x$ and $z \# y, x$. We must prove the validity of the proposition $p$: “$\forall P, P'.(P \xrightarrow{\text{nuc}} P' \text{ implies } [z]P \xrightarrow{\text{nuc}} [z]P')$”. Since $y \# x$, we have that $q$ is valid, which means $\forall z.p$ is valid. Since $z \# \{x, y\}$, it follows that $p$ is valid, and hence $U$-PASS$_{PV}$ is a valid rule.

\textbf{Lemma 5.5.} Rule SCOPE$_{PV}$ of Definition 5.9 is identical to rule number 11 in the FSM semantics of the fusion calculus.

\textbf{Proof.} Let $p$ be the formula “$\forall P, P'.(P \xrightarrow{\text{nuc}} P' \text{ implies } [z]P \xrightarrow{\text{nuc}} [z]P')$” in the logic of FM, where $n([y/z]) = fn([y/z])$. The free variables of $p$ are contained in the set $\{y,z\}$. Indeed, the set of free variables of $p$ is formed only by $y$ because $P, P'$ are bound by the quantifier $\forall$, and $z$ is bound by the scope operator; if we assume the free variables of $p$ to be only the variables of $p$ which are globally unbound, then these free variables of $p$ would be $y, z$ and again these are contained in the set $\{y,z\}$. Now, because of Proposition 2.12 and Proposition 2.13, we obtain the equivalence result “$\forall z.(z \# y \rightarrow y \# x)$” if and only if $\forall z.p$”. Since $y$ was arbitrarily chosen, we can say that rule SCOPE$_{PV}$ of Definition 5.9 is identical to rule number 11 in the FSM semantics of the fusion calculus.

\textbf{Lemma 5.6.} Rule O-OPEN$_{PV}$ of Definition 5.9 is identical to rule number 12 in the FSM semantics of the fusion calculus.

\textbf{Proof.} Let $p$ be the formula “$\forall P, P'.(P \xrightarrow{\text{nuc}} P' \text{ implies } [x]P \xrightarrow{\text{nuc}} [x]P')$” in the logic of FM, where $n([z/x]) = fn([z/x])$ and $n([x/z]) = \{z\}$. The free variables of $p$ are contained in the set $\{x,z\}$. Indeed, the set of free variables of $p$ is formed only by $z$ because $P, P'$ are bound by the quantifier $\forall$, and $x$ is bound by the scope operator; if we assume the free variables of $p$ to be only the variables of $p$ which are globally unbound, then these free variables of $p$ would be $x, z$ and again these are contained in the set $\{x,z\}$. Now, because of Proposition 2.12 and Proposition 2.13, we obtain the equivalence result “$\forall x.(x \# z \rightarrow x \# z)$” if and only if $\forall x.p$”. Since $z$ was arbitrarily chosen, we can say that rule O-OPEN$_{PV}$ of Definition 5.9 is identical to rule number 12 in the FSM semantics of the fusion calculus.

\textbf{Lemma 5.7.} Rule I-OPEN$_{PV}$ of Definition 5.9 is identical to rule number 13 in the FSM semantics of the fusion calculus.

\textbf{Proof.} Let $p$ be the formula “$\forall P, P'.(P \xrightarrow{\text{nuc}} P' \text{ implies } [x]P \xrightarrow{\text{nuc}} [x]P')$” in the logic of FM, where $n([z/x]) = fn([z/x])$ and $n([x/z]) = \{z\}$. The free variables of $p$ are
contained in the set \( \{ x, z \} \). Indeed, the set of free variables of \( p \) is formed only by \( z \) because \( P, P' \) are bound by the quantifier \( \forall \), and \( x \) is bound by the scope operator; if we assume the free variables of \( p \) to be only the variables of \( p \) unbound globally, then these free variables of \( p \) would be \( x, z \) and again these are contained in the set \( \{ x, z \} \). Now, according to Proposition 2.12 and Proposition 2.13, we obtain the equivalence result “\( \forall x. (x \# z \implies p) \) if and only if \( \forall x. p' \)”. Since \( z \) was arbitrarily chosen, we can say that rule I-OPEN\(_{PV,n} \) of Definition 5.9 is identical to rule number 13 in the FSM semantics of the fusion calculus. \( \square \)

From Lemmas 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 and 5.7, we are able to say that each transition rule in Definition 5.8 can be expressed in a PV-FSM form. This leads to the following corollary.

**Corollary 5.1.** The PV-FSM transition rules of Definition 5.9 also represent the FSM semantics of the (monadic version of) the fusion calculus.

**Definition 5.10.** A basic structural congruence rule in the FSM fusion calculus is in a PV-FSM form if it coincides with one of the following rules:

1. Processes which are obtained from one another by an \( \alpha \)-conversion are congruent; in fact they are identified in the framework of invariant sets;
2. \( P + 0 \equiv_n P, P + Q \equiv_n Q + P, (P + Q) + R \equiv_n P + (Q + R) \);
3. \( P \mid 0 \equiv_n P, P \mid Q \equiv_n Q \mid P, (P \mid Q) \mid R \equiv_n P \mid (Q \mid R) \);
4. \( [x]0 \equiv_n 0 \), \( [x][y]P \equiv_n [y][x]P, [x](P + Q) \equiv_n [x]P + [x]Q \);
5. \( [x](P \mid Q) \equiv_n P \mid [x]Q \) if \( x \# P \).

**Lemma 5.8.** Rule number 5 of Definition 5.7 is identical to rule number 5 of Definition 5.10.

**Proof.** Let \( p \) be the formula “\( \forall Q, [x](P \mid Q) \equiv_n P \mid [x]Q' \)” in the logic of FM. The free variables of \( p \) are contained in the set \( \{ x, P \} \). Indeed, the set of free variables of \( p \) is formed only by \( P \) (precisely only by the set of free names of \( P \), which is included in \( P \)) because \( Q \) is bound by the quantifier \( \forall \), and \( x \) is bound by the scope operator; if we assume the free variables of \( p \) to be only the variables of \( p \) which are globally unbound, then these free variables of \( p \) would be \( x, P \) and again these are contained in the set \( \{ x, P \} \). Now, because of Proposition 2.12 and Proposition 2.13, we obtain the equivalence result “\( \forall x. (x \# P \implies p) \) if and only if \( \forall x. p' \)”. Since \( P \) was arbitrarily chosen, we can say that rule number 5 of Definition 5.7 is identical to rule number 5 of Definition 5.10. \( \square \)

From Lemma 5.8, we are able to say that each structural congruence rule in Definition 5.7 can be expressed in a PV-FSM form. This leads to the following corollary.

**Corollary 5.2.** The PV-FSM structural congruence rules of Definition 5.10 are identical to the FSM structural congruence rules in Definition 5.7.
Now we can make a comparison between the PV semantics of the fusion calculus and the FSM semantics of the fusion calculus. First we remind the reader how we can prove, in the general theory, the equivalence of two semantics of the fusion calculus. To prove that two semantics of the fusion calculus, namely \( u_1 \) (where a transition is denoted by \( \rightarrow_1 \)), an action is denoted by \( \gamma_1 \) and a prefix is denoted by \( p_1 \)) and \( u_2 \) (where a transition is denoted by \( \rightarrow_2 \), an action is denoted by \( \gamma_2 \) and a prefix is denoted by \( p_2 \)), are “equivalent” or “have the same expressive power”, we must be able to define an encoding (morphism) \( \varphi : u_1 \rightarrow u_2 \) with a special property between the syntactic constructions, and to find a way to prove that everything that can be expressed with the transition rules in \( u_1 \) can also be expressed with the transition rules in \( u_2 \) as an image under the morphism \( \varphi \), and vice versa.

A practical way to do this is to define the morphism \( \varphi \) inductively by the following rules:

1. \( \varphi(0) = 0 \).
2. \( \varphi(p_1^i)_{P_1} = p_2^i \varphi(P_1) \), for each prefix \( p_1^i \) and each process \( P_1 \), where \( \{ p_1^i \} \) are the prefixes in \( u_1 \) and each of the prefixes \( p_1^i \) has a corresponding prefix \( p_2^i \) in \( u_2 \).
3. \( \varphi(P_1 | Q_1) = \varphi(P_1) \varphi(Q_1) \), for each \( P_1, Q_1 \).
4. \( \varphi((x)P_1) = \varphi(P_1) \), for each \( x, P_1 \), where \( (x)P \) is a general notation for the binding of \( x \) in \( P \) in various semantics ((x)P could be the binding realized by the scope operator in the PV semantics or, respectively, the FSM abstraction in the FSM semantics).

With \( \varphi \) defined in this way we must prove that \( \varphi \) is surjective and its kernel is precisely the \( \alpha \)-equivalence on \( u_1 \). To prove that \( u_1 \) and \( u_2 \) are equivalent semantics of the fusion calculus we must show the following implications (the classical procedure is by induction on the depth of the deduction tree):

- For each \( P_1, Q_1, \gamma_1 \) in \( u_1 \) we have that \( P_1 \xrightarrow{\gamma_1} Q_1 \) implies \( \varphi(P_1) \xrightarrow{\gamma_2} \varphi(Q_1) \), where \( \gamma_2 \) corresponds to \( \gamma_1 \) in \( u_2 \) (for example if \( u_1 \) is the PV semantics of the fusion calculus and \( u_2 \) is the FSM semantics of the fusion calculus, then: if \( \gamma_1 = x[y] \) then \( \gamma_2 = x[y] \), if \( \gamma_1 = x[y] \) then \( \gamma_2 = x[y] \), if \( \gamma_1 = [x/y] \) then \( \gamma_2 = [x/y] \), if \( \gamma_1 = (x)x[y] \) then \( \gamma_2 = (x)x[y] \), and if \( \gamma_1 = (x)x[y] \) then \( \gamma_2 = (x)x[y] \)).
- For each \( P_2, Q_2, \gamma_2 \) in \( u_2 \), choosing fresh names for the bound atoms in \( P_2 \) and \( Q_2 \) such that \( P_2 = \varphi(P_1) \) and \( Q_2 = \varphi(Q_1) \), we have that \( P_2 \xrightarrow{\gamma_2} Q_2 \) implies \( P_1 \xrightarrow{\gamma_1} Q_1 \), where \( \gamma_1 \) corresponds to \( \gamma_2 \) in \( u_1 \) (for example if \( u_2 \) is the FSM semantics of the fusion calculus and \( u_1 \) is the PV semantics of the fusion calculus then: if \( \gamma_2 = x[y] \) then \( \gamma_1 = x[y] \), if \( \gamma_2 = x[y] \) then \( \gamma_1 = x[y] \), if \( \gamma_2 = [x/y] \) then \( \gamma_1 = [x/y] \), if \( \gamma_2 = [x/y] \) then \( \gamma_1 = [x/y] \), if \( \gamma_2 = (x)x[y] \) then \( \gamma_1 = (x)x[y] \), and if \( \gamma_2 = (x)x[y] \) then \( \gamma_1 = (x)x[y] \)).

In our case, for the fusion calculus, things are very clear. Both in the PV semantics and in the FSM semantics of the fusion calculus, the syntax of processes and the basic actions are actually the same (see Definitions 5.5 and 5.6 and Remark 5.1). So, it is not necessary to define explicitly a morphism \( \varphi \) between the PV semantics of the fusion calculus and the FSM semantics of the fusion calculus as in the general theory. We can assume \( \varphi \) to be a morphism which leaves the processes and the actions in both semantics unchanged (with the remark that the terms obtained after
an $\alpha$-conversion are identified in the framework of invariant sets, and the bindings in the framework of invariant sets are in the sense of Definition 2.16) and whose kernel is the $\alpha$-equivalence on the PV semantics of the (monadic version of the) fusion calculus.

Such a $\phi$ is inductively induced by the FSM abstraction. The main property of $\phi$ is that for any process $P$ in $u_1$ (when $u_1$ is the PV semantics of the fusion calculus) we have $z \not\in fn(P)$ iff $z \not\# \phi(P)$ (easy to prove by induction on the syntax of $\phi$). These properties of $\phi$ allow us to adopt the convention of eliminating $\phi$ in the proof of the following theorem ($\phi$ is seen as an inclusion for ease of expression).

A connection between the PV structural congruence and the FSM structural congruence is given in the following theorem.

**Theorem 5.2.** For any two processes $P$ and $Q$ we have the following equivalence:

$$P \equiv Q \text{ if and only if } P \equiv_n Q.$$  

**Proof.** For the FSM structural congruence in the fusion calculus we consider the set of structural congruence rules presented in Definition 5.10 instead of the structural congruence rules presented in Definition 5.7. By Corollary 5.2, these two sets of rules coincide. Each structural congruence of the form $P \equiv_n Q$ is obtained by repeatedly applying the structural congruence rules in Definition 5.10. We have to prove a double implication. The first part will be proved by induction on the depth of the deduction tree of $\equiv$, the second by induction on the depth of the deduction tree of $\equiv_n$. To save space we do not write out the induction hypotheses in complete formality. We analyze only one case. The rest of them are trivial. First we prove that $P \equiv Q$ implies $P \equiv_n Q$ (in fact $P \equiv Q$ implies $\phi(P) \equiv_n \phi(Q)$; however, we can eliminate $\phi$ and write $\phi(P)$ as $P$ with the remark that the terms obtained after an $\alpha$-conversion are identified, and the bindings in the framework of invariant sets are in the sense of Definition 2.16).

We analyze the case of the last rule in Definition 5.3. Suppose $(x)(P \mid Q) \equiv P \mid (x)Q$ with $x \not\in fn(P)$. Then, because $fn(P) = supp(P)$ (Example 2.4), we have $x \not\# P$ and hence $[x](P \mid Q) \equiv [x]P$.

Conversely we prove that $P \equiv_n Q$ implies $P \equiv Q$. We analyze only the case of rule number 5 in Definition 5.10. Suppose $[x](P \mid Q) \equiv P \mid [x]Q$ with $x \not\# P$. Then, because $fn(P) = supp(P)$ (Example 2.4) we have $x \not\in fn(P)$ and hence $(x)(P \mid Q) \equiv P \mid (x)Q$. 

**Remark 5.2.** If we apply the general theory step by step, in the proof of Theorem 5.2 we obtain (by induction) that $P \equiv_n Q$ implies $P' \equiv Q'$ where $P = \phi(P')$ and $Q = \phi(Q')$ for fresh choices of bound names in $P$ and respectively in $Q$. Since $\phi$ leaves the processes and the actions in both semantics unchanged, we have that $P = \phi(P)$ and $Q = \phi(Q)$. Now, because the kernel of $\phi$ is precisely the $\alpha$-equivalence in PV, it follows that $P \equiv_\alpha P'$ and $Q \equiv_\alpha Q'$, and hence $P \equiv Q$.

The main result in this section is the following theorem which provides the connection between the PV and the FSM semantics of the fusion calculus.
**Theorem 5.3.** For any two processes $P$ and $Q$ and any action $\gamma$ we have:

$$P \xrightarrow{\gamma}_{uc} Q \text{ if and only if } P \xrightarrow{\gamma}_{nuc} Q.$$  

**Proof.** For the FSM semantics of the fusion calculus we consider the set of transition rules presented in Definition 5.9 instead of the transition rules presented in Definition 5.1. By Corollary 5.1, these two sets of transition rules coincide. Each transition of the form $P \xrightarrow{\gamma}_{nuc} Q$ is obtained by repeatedly applying the basic transition rules in Definition 5.9. We have to prove a double implication. The first part will be proved by induction on the depth of the deduction tree of $uc$, the second by induction on the depth of the deduction tree of $nuc$. To save space we do not write out the induction hypotheses in complete formality. We analyze only a few cases. The rest of them are very similar or trivial. First we prove that $P \xrightarrow{\gamma}_{uc} Q$ implies $P \xrightarrow{\gamma}_{nuc} Q$.

Case $U$-PASS. Suppose $P \xrightarrow{x/y}_{uc} P'$ where $z \neq x, y; x \neq y$. Then $(z)P \xrightarrow{x/y}_{uc} (z)P'$.

By the induction hypothesis, we have $P \xrightarrow{x/y}_{nuc} P'$. Since $\text{supp}(\{x,y\}) = \{x,y\}$ and $\text{supp}(\{x\}) = \{x\}$, we have that $z \neq x, y$ is equivalent to $z \notin \text{supp}(\{x,y\})$ which is $z \# x, y$, and $y \neq x$ is equivalent to $y \notin \text{supp}(\{x\})$ which is $y \# x$. We can apply rule $U$-PASS$_{PVn}$ and we get $[z]P \xrightarrow{x/y}_{nuc} [z]P'$.

Case SCOPE. Suppose $P \xrightarrow{y/z}_{uc} P'$ where $y \neq z$. Then $(z)P \xrightarrow{1}_{uc} P'\{y|z\}$. By the induction hypothesis, we have $P \xrightarrow{y/z}_{nuc} P'$. Since $\text{supp}(\{y\}) = \{y\}$, we have that $z \neq y$ is equivalent to $z \notin \text{supp}(\{y\})$ which is $z \# y$. We can apply rule SCOPE$_{PVn}$ and we get $[z]P \xrightarrow{1}_{nuc} P'\{y|z\}$.

Case $O$-OPEN. Suppose $P \xrightarrow{z|x}_{uc} P'$ where $z \neq x$. Then $(x)P \xrightarrow{z|x}_{uc} P'$. By the induction hypothesis, we have $P \xrightarrow{z|x}_{nuc} P'$. Since $\text{supp}(\{z\}) = \{z\}$, we have that $x \neq z$ is equivalent to $x \notin \text{supp}(\{z\})$ which is $x \# z$. We can apply rule $O$-OPEN$_{PVn}$ and we get $[x]P \xrightarrow{z|x}_{nuc} P'$.

We prove $P \xrightarrow{\gamma}_{nuc} Q$ implies $P \xrightarrow{\gamma}_{uc} Q$.

Case $U$-PASS$_{PVn}$. Suppose $P \xrightarrow{x/y}_{nuc} P'$ where $z \# x, y; y \# x$. Then $[z]P \xrightarrow{x/y}_{nuc} [z]P'$.

By the induction hypothesis, we have $P \xrightarrow{x/y}_{uc} P'$. Since $\text{supp}(\{x,y\}) = \{x,y\}$ and $\text{supp}(\{x\}) = \{x\}$, we have that $z \# x, y$ is equivalent to $z \notin \text{supp}(\{x,y\})$ which is $z \neq x, y$, and $y \# x$ is equivalent to $y \notin \text{supp}(\{x\})$ which is $y \neq x$. We can apply rule $U$-PASS and we get $(z)P \xrightarrow{x/y}_{uc} (z)P'$.

Case SCOPE$_{PVn}$. Suppose $P \xrightarrow{y/z}_{nuc} P'$ where $z \# y$. Then $[z]P \xrightarrow{1}_{nuc} P'\{y|z\}$. By the induction hypothesis, we have $P \xrightarrow{y/z}_{uc} P'$. Since $\text{supp}(\{y\}) = \{y\}$, we have that $z \# y$
is equivalent to \( z \notin \text{supp}(\{y\}) \) which is \( z \neq y \). We can apply rule \textit{SCOPE} and we get 
\[
(z)P \xrightarrow{uc} P'[y|z].
\]

Case \textit{O-OPEN} \textit{PV}. Suppose \( P \xrightarrow{nuc} P' \) where \( x \neq z \). Then \( [x]P \xrightarrow{uc} [x]P' \). By the induction hypothesis, we have \( P \xrightarrow{nuc} P' \). Since \( \text{supp}(\{z\}) = \{z\} \), we have that \( x \neq z \) is equivalent to \( x \notin \text{supp}(\{z\}) \) which is \( x \neq z \). We can apply rule \textit{O-OPEN} and we get 
\[
(x)P \xrightarrow{uc} P'.
\]

\( \square \)

\textbf{Remark 5.3.} If we apply step by step the method of proving the equivalence of several semantics presented before, in the proof of the Theorem 5.3 we obtain (by induction) that \( P \xrightarrow{\gamma} Q \) implies \( P' \xrightarrow{\gamma} Q' \) where \( P = \phi(P') \) and \( Q = \phi(Q') \) for fresh choices of bound names in \( P \) and respectively in \( Q \). Since \( \phi \) leaves the processes and the actions in both semantics unchanged, we have that \( P = \phi(P) \) and \( Q = \phi(Q) \). Now, because the kernel of \( \phi \) is precisely the \( \alpha \)-equivalence in PV, it follows that \( P \equiv_{\alpha} P' \) and \( Q \equiv_{\alpha} Q' \). By applying rule \textit{CONG} in the PV semantics of the fusion calculus, we also obtain that \( P \xrightarrow{uc} Q \). The procedure described in this remark is trivial, and it is done only in our mind. Formally, we write just \( P \xrightarrow{nuc} Q \) implies \( P \xrightarrow{uc} Q \), without employing \( \phi \).

\section*{5.4 FSM Semantics of Other Process Calculi}

Using the method developed in Section 5.3 we are able to define FSM semantics for other process calculi like \( \pi \)-calculus or \( \pi I \)-calculus. A complete study can be found in [9] and [11].

\subsection*{5.4.1 FSM Semantics of the \( \pi \)-calculus}

The \( \pi \)-calculus is a widely accepted model of interacting systems with dynamically evolving communication topology. The \( \pi \)-calculus allows channels to be passed as data along other channels, and this introduces channel mobility, which is an important feature of the \( \pi \)-calculus and is expressed by the changing configuration and connectivity among processes. This mobility increases expressive power, enabling the description of many high-level concurrent features. The \( \pi \)-calculus has several semantics. Among them, we mention particularly the early and the late (labelled) semantics.

The computational world of the \( \pi \)-calculus contains just processes (also called agents) and channels (also called names or ports). It can model networks in which messages are sent from one site to another site, and may contain links to active
5.4 FSM Semantics of Other Process Calculi

processes or to other sites. The \( \pi \)-calculus is a general model of computation which takes interaction as primitive. We present here the monadic version of the \( \pi \)-calculus: this means that a message consists of exactly one name. Let \( \mathcal{X} \) be a infinite set of names. The elements of \( \mathcal{X} \) are denoted by \( x, y, z, \ldots \). The terms of this formalism are called processes and processes are denoted by \( P, Q, R, \ldots \).

**Definition 5.11.** The processes are defined over the set \( \mathcal{X} \) of names by the grammar

\[
P :::= 0 \mid \bar{x}(z).P \mid x(y).P \mid P \mid Q \mid P + Q \mid !P \mid \text{new } xP
\]

The empty process is denoted by 0. The other process expressions are defined by guarded processes \( \bar{x}(z).P \) and \( x(y).P \), parallel composition \( P \mid Q \) (that is, the components \( P \) and \( Q \) can proceed independently and can interact via shared names), non-deterministic choice \( P + Q \), replication \( !P \) and a restriction \( \text{new } xP \) creating a local fresh channel \( x \) for the process \( P \) (components of \( P \) can use \( x \) to interact with one another but not with other processes). \( \pi \)-calculus replication \( !P \) can also be expressed by recursive equations of parametric processes (\( !P \) can be thought of as an infinite composition \( P | P | \ldots \)).

The guards are input guards and output guards. They represent sending and receiving a message (name) along a channel. The output guarded process \( \bar{x}(z).P \) sends \( z \) along \( x \) and then, after the output has completed, continues as \( P \). An input guarded process \( x(y).Q \) waits until a name is received along \( x \), substitutes it for the bound variable \( y \) and continues as \( Q \). The parallel composition \( \bar{x}(z).P \mid x(y).Q \) may synchronize two processes along a channel \( x \). The processes can interact by using names they share. A name received in one interaction can be used in another; by receiving a name, a process can interact with processes which are unknown to it, but which now share the same channel name. \( \pi \)-calculus mobility stems from its scoping of names and extrusion of names from their scopes.

There is an important distinction between input and output guards. The output guard is a simple sending of a name \( z \) along a channel \( x \), but the input guard has a more complex action: the name received along the channel \( x \) will replace \( y \) in the process following the input guard. Input guard is a binding operator involving substitutions. In \( x(y).P \), the name \( y \) binds free occurrences of \( y \) in \( P \). In a second binding operator \( \text{new } xP \), the name \( x \) binds free occurrences of \( x \) in \( P \). For the binding of a name in a process \( x(z).P \), the free occurrences of \( z \) in \( P \) indicate the places where the name received via \( x \) will be substituted when the process acts. It is by means of such substitutions of names for names that change of connectivity among the components of a system is expressed. The second binding operator \( \text{new } zP \) means that the components of \( P \) can use \( z \) to interact with one another but not with other processes. Also, in \( \text{new } zP \), components of \( P \) can also pass \( z \) to one another, and they can extrude the scope of \( z \) by sending \( z \) via some other name.

**5.4.1.1 Early Semantics of the \( \pi \)-calculus**

Activity within a system is described by simple reactions. Simple reactions do not explain how a system can interact with its environment, however. In order to understand the behaviour of a system by analyzing its parts, it is necessary to talk about
the actions that the parts can perform. We shall define a family of labelled transition relations on processes. The transition relations are defined by inference rules. This subsection presents the rules for early semantics of the \( \pi \)-calculus. The transition rules are labelled by the actions. We have four kinds of actions.

**Definition 5.12.** The actions are given by \( \alpha ::= \pi(y) | xy | \pi(z) | \tau \).

\( \pi(y) \) is sending the name \( y \) via the name \( x \), \( xy \) is receiving \( y \) via \( x \), and \( \pi(z) \) is sending a fresh name via \( x \). \( \tau \) is the internal action.

The transition relation labelled by \( \alpha \) is written \( \alpha \xrightarrow{e} \), where \( \alpha \) symbolizes the action and \( e \) is a notation for the semantics of the \( \pi \)-calculus in which we define the transition rule (in this subsection we work with the early semantics of the \( \pi \)-calculus).

For example \( P \xrightarrow{\pi(y)} e Q \) means that \( P \) can send \( y \) via \( x \) and evolve to \( Q \); \( P \xrightarrow{xy} e Q \) means that \( P \) can receive \( y \) via \( x \) and evolve to \( Q \); \( P \xrightarrow{\pi(z)} e Q \) means that \( P \) can send a fresh name \( y \) via \( x \) and evolve to \( Q \).

The free and bound names for each action are presented in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Kind</th>
<th>fn</th>
<th>bn</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \pi(y) )</td>
<td>free output</td>
<td>{x, y}</td>
<td>\emptyset</td>
</tr>
<tr>
<td>( xy )</td>
<td>input</td>
<td>{x, y}</td>
<td>\emptyset</td>
</tr>
<tr>
<td>( \pi(z) )</td>
<td>bound output</td>
<td>{x}</td>
<td>{z}</td>
</tr>
<tr>
<td>( \tau )</td>
<td>internal</td>
<td>\emptyset</td>
<td>\emptyset</td>
</tr>
</tbody>
</table>

**Definition 5.13.** The transition relations \( \{ \frac{\alpha}{e} \mid \alpha \text{ is an action} \} \) are defined by the rules of Table 5.1.

Note especially that \( x(z).P \) can receive any name via \( x \), and when a name is received, it is substituted for the placeholder \( z \) in \( P \).

### 5.4.1.2 Late Semantics of the \( \pi \)-calculus

The transition \( P \xrightarrow{xy} e Q \) expresses that \( P \) can receive the name \( y \) via \( x \) and evolve to \( Q \). An action of the form \( xy \) is sometimes referred to as a free input; it records both the name used for receiving and the name received. In the late relations, the free-input actions are replaced by the input prefixes, referred to in this context as *bound-input actions*. In late transitions \( P \xrightarrow{x(z)} l Q \), the label contains a placeholder \( z \) for the name to be received, rather than the name itself. If \( \alpha = x(z) \), then \( fn(\alpha) = x \) and \( bn(\alpha) = z \). We denote a late transition relation \( P \xrightarrow{\alpha} l Q \) by \( P \xrightarrow{\alpha} l Q \), where \( \alpha \) symbolizes the action and \( l \) is a notation for the semantics of the \( \pi \)-calculus where we define the transition rule (in this subsection we work with the late semantics of the \( \pi \)-calculus).
Table 5.1 Early semantics of the π-calculus

\begin{align*}
\text{OUT:} & \quad \pi(y).P & \xrightarrow{\pi(y)} & P \\
\quad P & \xrightarrow{\alpha & e} P', \quad \text{bn}(\alpha) \cap \text{fn}(Q) = \emptyset \\
\text{PARL:} & \quad P | Q & \xrightarrow{\alpha & e} & P' | Q \\
\text{COML:} & \quad P & \xrightarrow{\pi(y) & e} & P', Q & \xrightarrow{\pi(y) & e} & Q' \\
\text{TAU:} & \quad \tau.P & \xrightarrow{\tau} & P \\
\text{RES:} & \quad \new z P & \xrightarrow{\alpha & e} & \new z P', z \notin \text{n}(\alpha) \\
\text{REP act:} & \quad P & \xrightarrow{\alpha & e} & P', \quad \exists \tau & \xrightarrow{\alpha & e} & P' | \exists \tau \\
\text{CLOSEL:} & \quad P & \xrightarrow{\pi(z) & e} & P', Q & \xrightarrow{\pi(z) & e} & Q', \text{when } z \notin \text{fn}(Q) \\
\text{OPEN:} & \quad \new z P & \xrightarrow{\pi(z) & e} & P' \\
\end{align*}

The late semantics is given by the transition rules presented in Table 5.2. Usually in labelled transition systems for the π-calculus we use the following actions: \( x(y) \mid x(z) \mid \pi(z) \mid \tau \). The free and bound names for each action are presented in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Kind</th>
<th>fn</th>
<th>bn</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \pi(y) )</td>
<td>free output</td>
<td>{x, y}</td>
<td>\emptyset</td>
</tr>
<tr>
<td>( x(y) )</td>
<td>input</td>
<td>{x}</td>
<td>{y}</td>
</tr>
<tr>
<td>( \pi(z) )</td>
<td>bound output</td>
<td>{x}</td>
<td>{z}</td>
</tr>
<tr>
<td>( \tau )</td>
<td>internal</td>
<td>\emptyset</td>
<td>\emptyset</td>
</tr>
</tbody>
</table>

In the late semantics we use a transition \( x(z).P \xrightarrow{\pi(z) & l} P \) where the label \( x(z) \) indicates a placeholder \( z \) for the name to be received along channel \( x \) (rather than the name itself). This means that we replace the free-input actions with bound-input actions. Using the late rules, the placeholder \( z \) is instantiated by \( y \) when the communication is inferred, rather than when the input by the receiver is inferred. Thus, the early-late terminology is based on when a name is instantiated in inferring an interaction: when the input is inferred (early), or when the interaction is inferred (late).

We recall that we denote the late relations by \( \rightarrow_l \) and the early relations by \( \rightarrow_e \). By induction on inferences, we can prove that there is a close relationship between the early and the late relations.
Table 5.2 Late semantics of the $\pi$-calculus

$$L-{\text{OUT}} : \quad \pi(y).P \xrightarrow{\pi(y)} P$$

$$L-{\text{PARL}} : \quad P \xrightarrow{\alpha \downarrow} P', \text{ such that } bn(\alpha) \cap f n(Q) = \emptyset$$

$$L-{\text{COML}} : \quad P \xrightarrow{\pi(z)} P', Q \xrightarrow{\alpha} Q'$$

$$L-{\text{TALU}} : \quad \tau. P \xrightarrow{\tau} P$$

$$L-{\text{RES}} : \quad \text{new } z P \xrightarrow{\alpha} \text{new } z P', \text{ if } z \notin n(\alpha)$$

$$L-{\text{INP}} : \quad x(z). P \xrightarrow{x(z)} P$$

$$L-{\text{INP}} : \quad P \xrightarrow{\alpha} P'$$

$$L-{\text{INP}} : \quad P + Q \xrightarrow{\alpha} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\pi(z)} P', Q \xrightarrow{\alpha} Q'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\pi(z)} P', z \neq x$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad \text{new } z P \xrightarrow{\pi(z)} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

$$L-{\text{INP}} : \quad P \xrightarrow{\tau} P'$$

Theorem 5.4 ([137]).

1. $P \xrightarrow{\pi(z)} P'$ if and only if $P \xrightarrow{\pi(z)} P'$.  
2. $P \xrightarrow{x(z)} P'$ if and only if there are $Q$ and $y$ such that $P \xrightarrow{\pi(y)} Q$ and $P' = Q\{z|y\}$.  
3. $P \xrightarrow{\tau} P'$ if and only if $P \xrightarrow{\tau} P'$.  
4. $P \xrightarrow{\tau} P'$ if and only if $P \xrightarrow{\tau} P'$.

More details on the late semantics of the $\pi$-calculus are in [137].

5.4.1.3 FSM Semantics of the $\pi$-calculus

We can represent variable symbols as atoms, and binding operators as FSM abstractions. In this way we are able to provide a new semantics of the $\pi$-calculus with transition rules expressed compactly without additional freshness conditions. Moreover, we make a refinement of the transition rule $L-{\text{CLOSEL}}$ such that we assume a
similar rule to be valid only for those $z$ which are fresh for $P$. This approach helps us to describe the mobility mechanism in a different way than in the late semantics [9] (i.e. without employing structural congruence rules). Before defining the transition rules of the new (FSM) semantics of the $\pi$-calculus we state the following property:

**Remark 5.4.** The syntax and the basic actions (input, output, bound output and internal action) are the same in both the late semantics and the FSM semantics of the $\pi$-calculus, with the remarks that $\alpha$-equivalent terms are identified in the FSM approach and bindings are assimilated to FSM abstraction.

In the new $\pi$-calculus FSM semantics, in a labelled transition $P \xrightarrow{\alpha_n} Q$ we assume (by convention) that $\alpha$ has no bound names (i.e. $\alpha$ is neither an input nor a bound output).

**Definition 5.14.** The labelled transition rules of Table 5.3 define the FSM semantics of the $\pi$-calculus. A transition of the form $P \xrightarrow{u} Q$ (where $u$ is the action) in the FSM semantics of the $\pi$-calculus is denoted by $P \xrightarrow{n} Q$.

**Theorem 5.5 ([9]).** For any two processes $P$ and $Q$ and any action $u$, we have the following equivalence:

$$P \xrightarrow{u_l} Q \text{ if and only if } P \xrightarrow{u_n} Q.$$

### 5.4.2 FSM Semantics of the $\pi I$-calculus

In [136], Sangiorgi separates the mobility mechanisms of the $\pi$-calculus into two, respectively called *internal mobility* and *external mobility*. The former arises when an input meets a bound output, i.e. the output of a private name; the latter arises when an input meets a free output, i.e. the output of a known name. Internal mobility is responsible for much of the expressiveness of the $\pi$-calculus, whereas external mobility is responsible for much of the semantic complications.

The main distinction between internal and external mobility is clearly explained in Section 2.2 of [136]. Internal mobility appears when a bound output interacts with an input: $\pi(z).P | x(z).Q \xrightarrow{z} new \pi(P|Q)$. The interaction consumes the two prefixes but leave unchanged the derivatives underneath. With internal mobility, $\alpha$-conversion is the only form of name substitution involved. External mobility appears when a free output interacts with an input: $\pi(y).P | x(z).Q \xrightarrow{z} P|Q|\{y|z\}$. In this case a substitution must be imposed.

**Definition 5.15.** The class of the $\pi I$ processes is described by the following grammar:

$$P ::= 0 \mid \pi(z).P \mid x(y).P \mid P \mid Q \mid P + Q \mid new xP$$

In the $\pi I$-calculus, the input and output constructs are truly symmetric: Since only outputs of private names are possible, an input $x(z).P$ means “receive a fresh
Table 5.3 FSM Semantics of the $\pi$-calculus

1. $\forall x, y, P, x[y]P \xrightarrow{x(y)} P$

2. $\forall P, R, \alpha, Q$. $P \xrightarrow{n} Q$

3. $\forall P \xrightarrow{n} P$

4. $\forall P, Q$. $P \xrightarrow{n} Q$  

5. $\forall P, Q, R$. $P \xrightarrow{n} Q$

6. Rule for bound concurrent composition:

(a) $\forall R, \forall x, P, Q. P \xrightarrow{\bar{x}(y)} Q$

(b) $\forall R, \forall y, x, P, Q. P \xrightarrow{\bar{x}(y)} Q$

7. Rule for bound restriction:

(a) $\forall x, y, \forall \forall, Q. P \xrightarrow{n} Q$

(b) $\forall x, y, \forall \forall, Q. P \xrightarrow{n} Q$

8. $\forall x, y, P, x(y). P \xrightarrow{n} P$

9. $\forall R, \forall y, \forall \forall, Q. P \xrightarrow{n} Q$

10. $\forall P, Q, x, y, z, R, S$. $P \xrightarrow{n} (Q \{y\})|S$

11. $\forall P, \forall \forall, Q, R, S, x, y. P \xrightarrow{n} new[z](\{R \{y\}\}|S)$

12. $\forall P, \forall \forall, Q. P \xrightarrow{n} Q$

13. $\forall P, Q, x, y, z, R. P \xrightarrow{n} ((Q \{y\})|R)|P$

14. $\forall P, \forall \forall, Q, R, x, y, P \xrightarrow{n} new[z](\{Q \{y\}\}|R)|P$
name at \( x \)'', which is precisely the dual of the output \( \overline{x}(z) \cdot P \). Indeed, we can define a "dual" operation which transforms every output into an input and vice versa: the symmetry of the calculus is then manifested by the fact that dual commutes with the transition relation [136].

5.4.2.1 Sangiorgi Semantics of the \( \pi I \)-calculus

The transition rules are labelled by the actions. In \( \pi I \), we have three kind of actions.

**Definition 5.16.** The actions in the \( \pi I \)-calculus are given by

\[
\alpha ::= \overline{x}(z) \mid x(y) \mid \tau
\]

The *bound-output* action \( \overline{x}(z) \) is sending a fresh name \( z \) via \( x \); here \( x \) is a free name, and \( z \) is a bound name. The *bound-input* action \( x(y) \) is receiving a fresh name \( y \) via \( x \); here \( x \) is a free name, and \( y \) is a bound name. \( \tau \) is the internal action; it has no free or bound names.

The transition relation labelled by \( \alpha \) is written in \( \pi I \) as \( \alpha \xrightarrow{\text{\( \pi I \)}} P \), where \( \alpha \) symbolizes the action and \( \pi I \) indicates the calculus used. For example \( P \xrightarrow{\pi I} \alpha \) means that \( P \) can send \( y \) via \( x \) and evolve to \( Q \); \( P \xrightarrow{\pi I} x(y) \) means that \( P \) can receive \( y \) via \( x \) and evolve to \( Q \).

**Definition 5.17.** The following labelled transition rules define the Sangiorgi semantics of the \( \pi I \)-calculus.

\[
\begin{align*}
\text{OUT} & : & \overline{x}(y) \cdot P & \xrightarrow{\pi I} P \\
\text{TAU} & : & \tau \cdot P & \xrightarrow{\pi I} P \\
\text{ALPHA} & : & P \equiv \alpha \cdot Q & \xrightarrow{\pi I} R \\
\text{PAR} & : & P | Q & \xrightarrow{\pi I} P | Q \\
\text{RES} & : & \new{z}P & \xrightarrow{\pi I} \new{z}P
\end{align*}
\]

\[
\begin{align*}
\text{INP} & : & x(y) \cdot P & \xrightarrow{\pi I} x(y) \cdot P \\
\text{SUM} & : & P + Q & \xrightarrow{\pi I} P' \\
\text{COM} & : & P \xrightarrow{\pi I} P', Q \xrightarrow{\pi I} Q' & \xrightarrow{\pi I} \new{z}(P' \mid Q') \\
\text{RES} & : & \new{z}P & \xrightarrow{\pi I} \new{z}P'
\end{align*}
\]
5.4.2.2 FSM Semantics of the $\pi I$-calculus

Our goal is to present a compact semantics for the $\pi I$-calculus with transition rules expressed by using a mixing of quantifiers instead of side conditions. Before defining the transition rules of the new (FSM) semantics of the $\pi I$-calculus we state the following property.

Remark 5.5. The syntax and the basic actions (bound input, bound output and internal action) are the same in both the Sangiorgi semantics and in the FSM semantics of the $\pi I$-calculus with the remark that $\alpha$-equivalent terms are identified in the FSM approach. The binding operators are replaced by FSM abstractions.

Definition 5.18. The following labelled transition rules define the FSM semantics of the $\pi I$-calculus.

1. $\forall x, y, P, \overline{x}[y] P \xrightarrow{n I} P$
2. $\forall x, y, P, x[y] P \xrightarrow{n I} P$
3. $\forall P, \tau, P \xrightarrow{n I} P$
4. $\forall \alpha, P, Q, R, P + R \xrightarrow{n I} Q$
5. For parallel composition we have the following three transition rules (for bound output, bound input and $\tau$):
   a. $\forall R, N, x, P, Q, P \xrightarrow{n I} Q$
   b. $\forall R, N, x, P, Q, P \xrightarrow{n I} Q$
   c. $\forall P, Q, R, P \xrightarrow{n I} Q$
6. For restriction we have the following three transition rules (for bound output, bound input and $\tau$):
   a. $\forall x, N, \overline{y}, P, Q, P \xrightarrow{n I} Q$
   b. $\forall x, N, \overline{y}, P, Q, P \xrightarrow{n I} Q$
5.5 Comments

Process calculi are used as a formal framework for the study of concurrent computation. In this chapter, our goal is to provide FSM transition rules for the monadic fusion calculus. We use the quantifier $\forall$ to “encode” the freshness conditions in the hypothesis of the transition rules of the monadic fusion calculus, and we obtain a set of compact transition rules which defines the FSM semantics of the monadic fusion calculus. Thus, using FSM results, we are able to replace the side conditions in the transition rules of the monadic fusion calculus by a mixture of binding operators $\forall$ and $\forall$. This compact presentation is obtained by using the finite support requirement, Proposition 2.12, Proposition 2.13 and other technical results presented in Chapter 2. The main result of this chapter states that the Parrow-Victor semantics and the FSM semantics of the monadic fusion calculus have the same expressive power (see Theorem 5.3). A similar equivalence result for the structural congruence is presented in Theorem 5.2. However, it is worth noting that the FSM semantics of the fusion calculus is presented by involving only Tarski logical notions (such as IFM sets) and Tarski logical symbols (such as the quantifier $\forall$), whereas the original Parrow-Victor semantics of the fusion calculus is presented by assuming additional freshness conditions for each transition rule, and so it is not logical in Tarski’s sense.

Actually, we provide an algorithm for obtaining an FSM semantics for a certain process calculus. This algorithm shows us how to remove the side conditions from the transition rules of a process calculus, and can be applied to other process calculi such as the $\pi$-calculus or the $\pi I$-calculus (see [9, 11]). The FSM semantics of the $\pi$-calculus and of the $\pi I$-calculus are briefly described in Section 5.4. A complete presentation of FSM (nominal) semantics for various process algebras can also be found in [4]. The results in this chapter are valid because the construction of FSM makes sense in both the ZF framework and the ZFA framework. The approach presented in this chapter establishes an agreement between different presentations which, potentially, may break down for more powerful systems.

There exist many papers where process calculi are modelled by using different techniques for binding. In [89], D. Hirschkoff formalized a subset of the $\pi$-
calculus excluding match, mismatch and sum in Coq by using de Bruijn indices. Higher-order abstract syntax (HOAS) was used to model the $\pi$-calculus in both Isabelle [131] and Coq [91]. However, approaches based on HOAS can suffer some problems. For example the function spaces can be too large. Also, function spaces can destroy the inductive structure. When using HOAS terms, binders are represented as functions of type $\text{name} \rightarrow \text{term}$. If these functions range over the entire function space they may produce exotic terms [70], so the formalization’s have to ensure that those terms are avoided. The nominal logic is a first-order logic (see [125]), so exotic terms cannot appear. Moreover, in the framework of invariant sets, the existence of fresh names is axiomatically assumed (each time such a name is required) whilst in HOAS, if we need to generate names, we may need to index all predicates and relations by an explicit set of known names (see [91]).

FM techniques (which correspond to the FSM techniques presented in this book, if FSM is defined over the logic of ZFA) have also been used in order to formalize the $\pi$-calculus. In [37] the $\pi$-calculus is formalized in Isabelle using the nominal datatype package [157]. The FM techniques used in [37] are quite different from those proposed by us because the freshness quantifier is not used in [37]. Our FSM semantics of the monadic fusion calculus is based on the freshness quantifier which is used in order to “encode” the freshness conditions in the hypothesis of the transition rules. It is worth noting that the first idea of using the freshness quantifier in order to describe a new semantics for the $\pi$-calculus belongs to M. Gabbay [70]. However, there are some differences between our approach and the approach from [70], which are pointed out in [9]. In order to avoid defining a structural congruence relation in the FSM (nominal) semantics of the $\pi$-calculus, we made a refinement of the transition rule $L\text{-CLOSE}_L$ such that we assumed a similar rule to be valid only when some freshness conditions are satisfied. These freshness conditions are motivated by the manner in which the links are moved in a virtual space of linked processes. Using the finite support axiom in the FM framework, we established a complete equivalence between the FSM (nominal) semantics and the late semantics of the $\pi$-calculus [9].
References

34. Banach, S., Tarski, A.: Sur la décomposition des ensembles de points en parties respectivement congruentes. Fundamenta Mathematicae. 6, 244–277 (1924)
References

100. Krishnamurthy, V., Krishnamurthy, E.V.: Rule-based programming paradigm: a formal basis for biological, chemical and physical computation. Biosystems. 49, 205–228 (1999)