Institute of Computer Science
Romanian Academy

Algebraic Analysis and Processing of Data in Web Systems

Andrei Alexandru

Supervisor
Prof. Dr. Gabriel Ciobanu

2012
ANUNȚ

Vă facem cunoscut că în ziua de 29.10.2012 la ora 09.00 în Sala Mică de Conferințe a Academiei Române-Filiala Iași, va avea loc susținerea publică a tezei de doctorat intitulată: „ANALIZĂ ALGEBRICA SI PROCESAREA DATELOR IN SISTEME WEB” (in engleză „ALGEBRAIC ANALYSIS AND PROCESSING OF DATA IN WEB SYSTEMS”) elaborată de domnul Andrei Alexandru în vederea conferirii titlului științific de doctor.

Comisia de doctorat este alcătuită din:

- Prof. dr. Dan Cristea
  Institutul de Informatică Teoretică, Academia Română - Filiala Iași

- CS I dr. Gabriel Ciobanu
  Institutul de Informatică Teoretică, Academia Română - Filiala Iași

- Prof. dr. Ferucio Laurențiu Țiplea
  Universitatea „Alexandru Ioan Cuza” Iași, Facultatea de Informatică

- Prof. dr. Gheorghe Ștefănescu
  Universitatea București, Facultatea de Matematică și Informatică

- Prof. dr. Răzvan Lițcanu
  Universitatea „Alexandru Ioan Cuza” Iași, Facultatea de Matematică

- Președinte

- Conducător științific

- Referent

- Referent

- Referent

Vă invităm să participați la susținerea publică a tezei de doctorat.

Director,

Prof. dr. ing. Horia-Nicolai Teodorescu
Membru Corespondent al Academiei Române

Coordonator Programe Doctorale,

CS II dr. Florin Rotaru
Acknowledgements

I thank to my supervisor Dr. Gabriel Ciobanu for giving me this opportunity, and for his constant support and advice throughout this PhD.

I also thank my examiners: Dr. Razvan Litcanu, Dr. Gheorghe Stefanescu, Dr. Ferucio Tiplea, for their careful reading of the thesis and their helpful comments.

I thank the anonymous referees for their comments and suggestions which helped increase the quality of the papers in which parts of this thesis were published.

I am grateful to all my colleagues from the group of Formal Methods Laboratory, Institute of Computer Science, Romania Academy, Iasi Branch for their helpful suggestions.
Chapter 1

Introduction

1.1 Motivation

The notion of choosing a fresh name often arises when manipulating syntactic expressions; therefore it is necessary to indicate some constraints whenever describing such a syntactic manipulation. Often it is just said that a name is fresh without specifying any restrictions. In such a case, we mean that the fresh name must be different from any name occurring anywhere else in the expression or program. Some programming systems have mechanisms for renaming, for binding a name with a value and for managing sets of such bindings. Modern programming languages are designed to manage bindings and fresh names by using the notions of scopes, workspaces, or environments. Since renaming, binding and fresh names appear in several approaches, it became evident that they deserve to be studied in their own terms.

The nominal logic and semantics was presented by Gabbay and Pitts in [14, 27]; it uses the Fraenkel-Mostowski (FM) axioms of set theory. The FM set theory was originally developed to prove the independence of the Axiom of Choice from the other axioms of the Zermelo-Fraenkel (ZF) set theory. It was rediscovered and used by Gabbay and Pitts [14] to model the syntax of formal systems involving variable binding operations. An advantage of modeling syntax in a model of FM set theory is that datatypes of syntax quotiented by α-equivalence can be modeled inductively. This is because FM set theory delivers a model of variable symbols and α-abstraction. The FM axioms are precisely the Zermelo-Fraenkel with atoms (ZFA) axioms over an infinite set of atoms [14], together with the special property of finite support which claims that for each element \( x \) in an arbitrary set we can find a finite set supporting \( x \). This finite support axiom helps us to solve the problem of choosing fresh names, and the FM set theory seems to be a better framework for computer science that the old ZF set theory.

In this thesis we analyze the consequences of replacing the classical ZF
axioms of set theory with the new FM axioms of set theory, in computer
science. New semantics for various process calculi are defined according to
the FM axioms of set theory. These new semantics have the same expres-
sive power as the usual semantics (defined according the ZF axioms of set
theory), even the FM axioms of set theory are completely different that the
ZF axioms of set theory. We also define and study various algebraic struc-
tures in the FM framework emphasizing a strong connection between the
FM properties of these algebraic structures and their related ZF properties.
Finally, the axiomatic FM set theory is extended by replacing the finite sup-
port axiom with a weaker axiom. Many algebraic and topological properties
of sets are preserved in this new framework.

1.2 Outline

The thesis is organized as follows:

Chapter 2 We review some basic notions of nominal logic like nominal
set, FM-set, nominal quantifier, support, fresh element, abstraction, which
are used in the following chapters.

Chapter 3 We present several sets of compact transition rules for the
monadic versions of the π-calculus, πI-calculus and fusion calculus, respec-
tively which define the nominal semantics of these process calculi. These
transition rules are expressed, without side conditions, using the quantifiers
∀ and the nominal quantifier N. We prove a complete equivalence between
the new nominal semantics of the π-calculus, πI-calculus and fusion calcu-
lus, respectively, and the usual semantics of these process calculi. The work
presented in this chapter can be found in [AA4, AA6, AA9, AA11, AA12,
AA13].

Chapter 4 We formalize in the FM approach several algebraic concepts
which were initially described using the ZF axioms of set theory. We focus on
multisets, generalized multisets and event structures because these concepts
are often used in computer science. We define and study FM-multisets,
FM-generalized multisets and FM-event structures providing several new
nominal (FM) properties of these concepts. The nominal properties of these
algebraic structures are compared with the related ZF properties of them.
The work presented in this chapter can be found in [AA2, AA5, AA7, AA8].

Chapter 5 We generalize the FM set theory by giving a new set of
axioms which defines the Extended Fraenkel-Mostowski (EFM) set theory.
The finite support axiom in the FM set theory is replaced by a consequence
of it which states only that each subset of the set A of atoms is finite or
cofinite. Many algebraic and topological properties of sets which are valid
in the FM framework are also valid in the EFM framework. Permutative
renamings are also defined and studied in the EFM framework. The work
presented in this chapter can be found in [AA1, AA3, AA10].
Chapter 2

Fraenkel-Mostowski Set Theory

In this chapter we present the mathematical foundations of nominal logic, and several old and new nominal techniques used in the following chapters. For further information about this topic the reader is referred especially to papers [14, 27].

Let $S_A$ be the set of all finitary permutations of $A$ (i.e. the set of all permutations of $A$ which leave unchanged all but finitely many atoms). $S_A$ is a group under the usual composition of permutations.

**Definition 2.1.**

- Let $X$ be a set defined by the axioms of ZF model. 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 set defined by the axioms of ZF model, and $\cdot : S_A \times X \to X$ is an $S_A$-action on $X$. We simply use $X$ whenever no confusion arises.

**Definition 2.2.** 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 $\text{Fix}(S) = \{\pi \in S_A \mid \pi(a) = a, \forall a \in S\}$.

**Definition 2.3.** Let $(X, \cdot)$ be an $S_A$-set. We say that $X$ is a nominal set if for each $x \in X$ there exists a finite set $S_x \subseteq A$ which supports $x$.

**Theorem 2.4.** Let $X$ be an $S_A$-set, and for each $x \in X$ let us define $F_x = \{S \subseteq A \mid S \text{ finite, } S \text{ supports } x\}$. If $F_x$ is nonempty 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 2.5.** If $x \in A$ and $y \in Y$ where $Y$ is a nominal set, we say that $x$ is fresh for $y$ and denote this by $x \# y$ if $\text{supp}(x) \cap \text{supp}(y) = \emptyset$. 

3
For an arbitrary name, we can always find a name outside its support, because for all \( y \) we know that \( \text{supp}(y) \) is finite and, because \( A \) is infinite, we can find an atom \( x \) such that \( x \notin \text{supp}(y) \). This means \( \forall x. \exists a \in A. a \# x \).

**Definition 2.6.** Let \( P \) be a predicate on \( A \). We say that \( \forall a. P(a) \) if \( P(a) \) is true for all but finitely many elements of \( A \). \( \forall \) is called the **nominal quantifier**.

The following two propositions are used to express, in Chapter 3, nominal semantics for several process calculi. These propositions show us how freshness conditions can be replaced by \( \forall \).

**Proposition 2.7.** Let \( (x_i)_i \) be a set of distinct variables and \( p \) a formula in the logic of \( FM \). We have the following implications:

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

**Proposition 2.8.** If the free variables of the formula \( p \) are contained in the set of distinct variables \( \{a, (x_i)_i\} \), we also have the converse implication: \( [\exists a \in A. (a \# (x_i)_i \wedge p)] \) implies \( [\forall a. (a \# (x_i)_i \Rightarrow p)] \).

**Definition 2.9.** Let \( X \) be a nominal set.

1. For \( a \in A \) and \( x \in X \) we can define an **abstractive element** to be of form \([a]x\) where \([a]x = \bigcap \{ V \subset A \times X \mid (a, x) \in V \wedge \text{supp}(V) \subset \text{supp}(x) \setminus \{a\} \} \).

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

The notion of “abstractive elements” is the analogue of the \( \alpha \)-abstraction in the \( \lambda \)-calculus because of the following theorem, and because in \( \lambda \)-calculus the notions of “support” and “free names” coincide.

**Theorem 2.10.** Let \( X \) be a nominal set, \( a \in A \) and \( x \in X \). Then \([A]X\) is also a nominal set. Moreover we have \( \text{supp}([a]x) = \text{supp}(x) \setminus \{a\} \).
Chapter 3

Nominal Process Calculi

3.1 About this chapter

The aim of this chapter is to present several sets of compact transition rules for the monadic versions of the \( \pi \)-calculus, \( \pi I \)-calculus and fusion calculus, respectively. These transition rules are expressed using the quantifiers \( \forall \) and the nominal quantifier \( \mathcal{N} \). Using some results presented in the second chapter of this thesis we are able to compare the new semantics of the \( \pi \)-calculus, \( \pi I \)-calculus and fusion calculus with the known semantics of these process calculi.

The \( \pi \)-calculus 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 some 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 \( \pi \)-calculus embodies the view that in principle most, if not all, distributed computation may usefully be explained in terms of exchanges of names on named communication channels. The finite support property gives us a mathematical reason for why such a renaming is always possible. Also, the Fraenkel-Mostowski set theory is the axiomatic support for the construction of nominal logic. Since we can use the same axiomatic model of set theory for describing both nominal logic and \( \pi \)-calculus, we apply nominal techniques in \( \pi \)-calculus.
The $\pi I$-calculus (or simply $\pi I$) was introduced by Sangiorgi in [33]; it is a variant of the $\pi$-calculus in which the free outputs are disallowed.

The update calculus and its polyadic version, known as the fusion calculus, have emerged as a good foundational model for distributed computation paradigms like web-services and service oriented architectures.

The update calculus was presented for the first time in [24]. It contains the monadic $\pi$-calculus as a proper subcalculus (as it is proved in Section 2.3 from [24]) 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.

3.2 Conclusions

In this chapter we change the transition rules of the $\pi$-calculus, $\pi I$-calculus and fusion calculus, respectively, by using specific nominal techniques. For this we use a special nominal 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. $\forall x.\mathcal{N}y.\forall z.\text{expression}$ is true iff $\forall x,y,z.(y \text{ is fresh for } x) \Rightarrow (\text{expression})$. We finally provide new nominal semantics for $\pi$-calculus, $\pi I$-calculus and fusion calculus, respectively. We prove several nominal properties of the binding operators of the $\pi$-calculus (namely new and input) and of the fusion calculus (namely scope) which allow us make a comparison between the nominal semantics of these process calculi and the other known semantics defined before. The central idea of this chapter is to use atoms to represent variable symbols and nominal abstraction to represent binding operators in several process calculi. A mixing of $\forall$ and $\mathcal{N}$ is used to replace the side conditions in the transition rules of these process calculi.

In the first section, following our approach from [AA4, AA13], we prove that the mobility mechanism can be described in the new semantics of the $\pi$-calculus as well as in the late semantics of the $\pi$-calculus, using a transition rule which is assumed to be valid only in a more restrictive hypothesis than its related rule in the late semantics of the $\pi$-calculus. Moreover, the nominal quantifier helps us to “encode” the freshness conditions in the hypothesis of the transition rules and to present a compact transition rule in the “weakest” form we need for expressing the mobility. Even one transition rule in the new semantics of the $\pi$-calculus is assumed to be valid only
when some freshness conditions are satisfied whilst its related rule in the late semantics of the $\pi$-calculus is assumed to be valid without requesting those freshness conditions to be satisfied, we are able to prove that the new semantics and the late semantics of the $\pi$-calculus are completely equivalent. The main result in this section states that the nominal semantics and the late semantics of the $\pi$-calculus have the same expressive power.

There exists many papers where process calculi are modeled by using different techniques for binding. In [16], D. Hirschkoff formalised 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 [30] and in Coq [17]. However, approaches based on HOAS can suffer by 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 name $\to$ term. If these functions range over the entire function space they may produce exotic terms, so the formalisations have to ensure that those terms are avoided. The nominal logic is a first order logic and, hence, exotic terms can not appear. Moreover, in the nominal framework the existence of fresh names is axiomatically assumed (each time when a such a name is requested) 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 [17]).

Nominal techniques have also been used in order to formalise the $\pi$-calculus. In [5] the $\pi$-calculus is formalised in Isabelle using the nominal datatype package [40]. In paper [12], M.Gabbay also uses nominal techniques to obtain new transition rules for the $\pi$-calculus. In this section we present a nominal semantics of the $\pi$-calculus which is completely equivalent with the late semantics of the $\pi$-calculus. However our transition rules are different from those proposed by M. Gabbay. We want to emphasize the benefit of using nominal techniques in order to encode some freshness conditions which allow us to present the transition rules in the “weakest” form we need for characterizing the mobility mechanism. We show that we can characterize mobility by using a rule in the hypothesis of which we assume a freshness condition presented in the nominal approach. We have to recognize that the first idea of using nominal techniques to formalise the $\pi$-calculus belongs to M. Gabbay. In this section we try to introduce a slightly different perspective (we do not say we introduce a better one!). Our nominal transition rules also provide a semantics of the $\pi$-calculus which is equivalent with the late semantics of the $\pi$-calculus. However our approach is motivated by the description of the mobility mechanism and our transition rules are different than those in [12].

In the second section, following our approach from [AA9, AA11], we prove that the new semantics and the original semantics of the $\pi I$-calculus presented in [33] have the same expressive power.
In the third section, following our approach from [AA6, AA12], we prove that the new semantics of the monadic fusion calculus and the original semantics of the monadic fusion calculus presented in [24] are also equivalent. A similar result can be given, in this case, for the structural congruence.
Chapter 4

Algebraic Structures in the Fraenkel-Mostowski Framework

The aim of this chapter is to formalize in the FM approach several algebraic concepts which were initially described using the ZF axioms of set theory. We focus on multisets, generalized multisets and event structures because these concepts are often used in computer science. It is not our aim to rewrite the entire algebra in nominal terms. However we provide an algorithm of translating a certain algebraic concept in the FM framework. This algorithm is based on the remark that only finitely supported objects are allowed in the FM universe. We present in detail many nominal properties of multisets, generalized multisets and event structures, emphasizing the analogy between the results obtained by using the FM axioms of set theory and those obtained by using the ZF axioms of set theory. However the techniques developed in this chapter can be extended to other concepts (like monoids, groups, fields, posets, lattices etc) as well.

4.1 Multisets in the Fraenkel-Mostowski Framework

Multisets are used more and more in computer science for quantitative analysis and models of resources. The concept of multiset was introduced in order to capture the idea of multiplicity of appearance, or resource. Multisets are defined by assuming that for a given set $\Sigma$ an element $x$ occurs a finite number of times. For example the prime factorization of a natural number $n$ is a multiset whose elements are primes. The invariants of a finite abelian group also form a multiset. Even processes in an operating system can be seen as a multiset, and the examples can continue.
Multisets already have many applications in computer science. References [18] and [19] are the early known references to the applications of multisets in computer science. Multisets and permutations of multisets are applied in a variety of search and sort procedures in [18]. Eilenberg [10] had applied the general theory of multisets to automata. Later, Engelfriet [11] used the multisets to provide a semantical description of some form of the \( \pi \)-calculus. Peterson [26] shows that the very foundation of Petri net theory needs the use of multisets. Pratt [28] shows how partially order multisets (pomsets) can be used to represent parallel processes. He also describes how Petri nets can be modelled as pomsets. Multisets are also used in database theory (see [20] and [32]) or in membrane computing (see [1], [2] and [25]). There are also several attempts to use multisets in programming [4], in describing the evolution of biological systems [22] and new models inspired by cell biology [3]. A collection of papers on applications of multisets in computer science can be found in [7] or [35].

These papers justify that multisets are interesting as a specific data type, and they deserve to be studied from various perspectives. In this section we study the multisets from both an algebraic a nominal perspective.

Ordinary sets are composed of pairwise different elements which means no two elements are the same. If we accept multiple but finite 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 \( \mathbb{N} \) where each element in \( \Sigma \) has associated its multiplicity. For a complete study of multisets see [6, 8, 39].

The aim of this section is to prove several algebraic properties of multisets and to formalize in the FM approach the concept of “multiset”. Using nominal techniques we define “FM-multisets” presenting also some properties of this new concept. FM-multisets intend to provide a constructive framework in which we work with sets having finite support property. The analogy between the properties of multisets obtained by using the FM axioms of set theory and those obtained in by using the ZF axioms of set theory is emphasized. The work in this section can be found in [AA8].

### 4.1.1 Algebraic Properties of Multisets

We consider the following notations:

- multiset over \( \Sigma \)-function from \( \Sigma \) to \( \mathbb{N} \)
- \( \mathbb{N}(\Sigma) \)-the set of all multisets over a finite alphabet \( \Sigma \)
- \( \Sigma^* \)-the free monoid over a finite alphabet \( \Sigma \)

The main results in this subsection are expressed by the following theorems:
Theorem 4.1 (ZF). \((\mathbb{N}(\Sigma), +)\) is a free abelian \(\mathbb{N}\)-semimodule with a basis given by \(\{\tilde{a} \mid a \in \Sigma\}\) where \(\tilde{a} : \Sigma \to \mathbb{N}\) is defined by \(\tilde{a}(b) = 1\) if \(b = a\) and \(\tilde{a}(b) = 0\) if \(b \in \Sigma \setminus \{a\}\).

Theorem 4.2 (ZF). If \(M\) is any abelian monoid and \(f : \Sigma \to M\) an arbitrary function, then there is a unique homomorphism of abelian monoids \(g : \mathbb{N}(\Sigma) \to M\) with \(g(\tilde{a}) = f(a)\) for all \(a \in \Sigma\).

Theorem 4.3 (ZF). For each monoid \(M\) and each function \(f : \Sigma \to M\), there is a unique homomorphism of monoids \(g : \Sigma^* \to M\) with \(g \circ i = f\) for all \(a \in \Sigma\).

Theorem 4.4 (ZF). \(\Sigma^*/\text{Ker } g \cong \mathbb{N}(\Sigma)\), where \(g : \Sigma^* \to \mathbb{N}(\Sigma)\) satisfy \(g \circ i = j\), where \(i : \Sigma \to \Sigma^*\) is the standard inclusion of \(\Sigma\) into \(\Sigma^*\) which maps each element \(a \in \Sigma\) into the word \(a\).

4.1.2 Nominal Multisets

We can express the results in the previous subsection in the FM framework, in terms of finitely supported objects:

Definition 4.5. An FM-monoid is a triple \((M, +, \cdot)\) such that the following conditions are satisfied:

- \((M, +, 0)\) is a monoid.
- \((M, \cdot)\) is a nominal 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 \(\pi \cdot 0 = 0\).

Theorem 4.6 (FM). \(\mathbb{N}(\Sigma)\) is a free abelian FM-monoid whenever \((\Sigma, \cdot)\) is a finite nominal set.

Theorem 4.7 (FM). \(\Sigma^*\) is an FM-monoid whenever \((\Sigma, \cdot)\) is a finite nominal set. Moreover each element \(x_1x_2 \ldots x_n\) from \(\Sigma^*\) is supported by the set \(U = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k)\) when \(\Sigma = \{a_1, \ldots, a_k\}\).

Theorem 4.8 (FM). Let \((\Sigma, \cdot)\) be a finite nominal set. Let \(j : \Sigma \to \mathbb{N}(\Sigma)\) be the function which maps each \(a_i \in \Sigma\) into \(\tilde{a}_i \in \tilde{\Sigma}\). If \((M, +, \circ)\) is an arbitrary abelian FM-monoid and \(\varphi : \Sigma \to M\) is an arbitrary function, then there exists a unique finitely supported homomorphism of abelian monoids \(\psi : \mathbb{N}(\Sigma) \to M\) with \(\psi \circ j = \varphi\).

Theorem 4.9 (FM). Let \((\Sigma, \cdot)\) be a finite nominal set. Let \(i : \Sigma \to \Sigma^*\) be the standard inclusion of \(\Sigma\) into \(\Sigma^*\). If \((M, +, \circ)\) is an arbitrary FM-monoid and \(\varphi : \Sigma \to M\) is an arbitrary function, then there exists a unique finitely supported homomorphism of monoids \(\psi : \Sigma^* \to M\) with \(\psi \circ i = \varphi\).
Theorem 4.10 (FM). \( \Sigma^*/\text{Ker} \, g \) is an FM-monoid and the isomorphism \( \Theta \) between the monoids \( \Sigma^*/\text{Ker} \, g \) and \( \mathbb{N}(\Sigma) \), defined by \( \Theta([w]) = \psi(w) \) for each \( w \in \Sigma^* \) (where \( [w] \) is the equivalence class of \( w \) modulo the equivalence relation \( \text{Ker} \, g \)) is finitely supported.

4.1.3 Conclusions

The aim of this section is to define and study “multisets” in nominal framework. This concept was initially described using the classical ZF axioms of set theory. Using nominal techniques, we define “FM-multisets”, presenting also some properties of this new concept. The analogy between the results obtained by using the FM axioms of set theory and those obtained by using the ZF axioms of set theory is emphasized by the results presented in Subsection 4.1.2. We prove that the set of all multisets over a finite alphabet \( \Sigma \) coincides with the set of all FM-multisets over \( \Sigma \). Moreover, the set of multisets over \( \Sigma \) is a free abelian FM-monoid, and it satisfies the universality property expressed in Theorem 4.8. The free monoid over \( \Sigma \) is also an FM-monoid and it satisfies a specific universality property (Theorem 4.9).

By repeatedly applying these universality properties, a connection between the set of all multisets over \( \Sigma \) and the free monoid over \( \Sigma \) is given first in the ZF approach and second in the FM approach, in terms of finitely supported morphisms (Theorem 4.10).

As an intuitive general rule, an FM result is obtained from the ZF results by replacing “ZF-structure” with “FM-structure” (“ZF-set” with “nominal set”, “ZF-monoid” with “FM-monoid”) and “function” with “finitely supported function” because in the FM universe only finitely supported objects are allowed.

In fact in this section we present an algorithm of how a classical ZF concept can be translated FM. The techniques presented here can be extended also to other concepts. Several concepts like generalized multisets, event structures or various algebraic structures can be formalized in FM in the same way we did in this section with the multisets.

4.2 Generalized Multisets in the Fraenkel-Mostowski Framework

Generalized multisets try to extend the usual multisets 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 the 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 Loeb (see [21]). He used the notion of hybrid set for what we call...
generalized multiset. However, the first application of the concept of "generalized multiset" is due to Reisig [29] which uses the generalized multisets and the 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.

The aim of this section is to prove several algebraic properties of generalized multisets and to formalize in the FM approach the concept of "generalized multisets" which was initially described using the classical ZF model of set theory [AA5]. Using nominal techniques we define "FM-generalized multisets" presenting also some properties of this new concept. FM-generalized multisets intend to provide a constructive framework in which we work with sets having finite support property. The analogy between the results obtained by using the FM axioms of set theory and those obtained in [AA5] by using the ZF axioms of set theory is emphasized. The work in Subsection 4.2.1 can be found in [AA5], and the work in Subsection 4.2.2 can be found in [AA7].

4.2.1 Algebraic Properties of Generalized Multisets

Generalized multisets as groups

We make the following notations:

- generalized multiset over $\Sigma$-function from $\Sigma$ to $\mathbb{Z}$
- $\mathbb{Z}(\Sigma)$-the set of all generalized multisets over $\Sigma$
- $F(\Sigma)$-the free group over $\Sigma$

**Theorem 4.11 (ZF).** $(\mathbb{Z}(\Sigma), +)$ is a free abelian group with a basis given by $\tilde{\Sigma} = \{\tilde{a} \mid a \in \Sigma\}$ where $\tilde{a} : \Sigma \to \mathbb{Z}$ is defined by $\tilde{a}(b) = 1$ if $b = a$ and $\tilde{a}(b) = 0$ if $b \in \Sigma \setminus \{a\}$

**Theorem 4.12 (ZF).** 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 $g(\tilde{a}) = f(a)$ for all $a \in \Sigma$.

**Theorem 4.13 (ZF).** For each group $G$ and each function $f : \Sigma \to G$, there is a unique homomorphism of groups $g : F(\Sigma) \to G$ with $g \circ i = f$, where $i : \Sigma \to F(\Sigma)$ is the standard inclusion of $\Sigma$ into $F(\Sigma)$.

**Theorem 4.14 (ZF).** $F(\Sigma)/\text{Ker} g \cong \mathbb{Z}(\Sigma)$ where $g : F(\Sigma) \to \mathbb{Z}(\Sigma)$ such that $g \circ i = j$, 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 $[a]$.

Orders on generalized multisets

**Theorem 4.15.** $\mathbb{Z}(\Sigma)$ is a lattice ordered group.
Corollary 4.16 (Riesz Decomposition). Let \( f, g_1, \ldots, g_n \in \mathbb{Z}(\Sigma) \) such that \( \theta \leq g_i, i = \overline{1, n} \) 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 \( \theta \leq h_i \leq g_i, i = \overline{1, n} \).

Corollary 4.17. 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.

Corollary 4.18. 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.

Corollary 4.19. 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 with the factor group \( \mathbb{Z}(\Sigma)/H)/(G/H) \).

Corollary 4.20. 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 with \( (G + H)/H \).

Theorem 4.21. \( \mathbb{Z}(\Sigma) \) is \( l \)-isomorphic with an \( l \)-permutation group.

Theorem 4.22. \( \mathbb{Z}(\Sigma) \) is \( l \)-isomorphic to an \( l \)-subgroup of \( A(F) \) for some totally ordered field \( F \).

Theorem 4.23. For a total order on \( \mathbb{Z}(\Sigma) \), there is a total order on \( F(\bar{\Sigma}) \) such as the natural surjection of \( F(\bar{\Sigma}) \) onto \( F(\bar{\Sigma})/D(F(\bar{\Sigma})) = \mathbb{Z}(\Sigma) \) is \( o \)-homomorphism.

Theorem 4.24. There is an injective \( l \)-homomorphism between \( (\mathbb{Z}(\Sigma), \wedge, \lor) \) and a divisible \( l \)-group.
Comments

In [9, 15, 31, 36] the theory of $l$-groups was studied from the perspective of Reverse Mathematics. Reverse Mathematics (see [34]) is a subfield of logic which tries to answer questions like this by finding 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 says that if we have a formula in $\mathbb{Z}^2$, the set of numbers which satisfy it exists. Mathematically this can be written as: $\exists X \forall a (a \in X \leftrightarrow \varphi(a))$ where $\varphi$ 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. We mention here just two of them. A complete study of these subsystems could be found in [31] or [34].

$RCA_0$ is the system whose set comprehension scheme is limited to $\Delta^0_1$ formulas (there are also included axioms allowing $\Sigma^0_1$ induction). 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: $\forall X ((0 \in X \land \forall n (n \in X \rightarrow n+1 \in X)) \rightarrow \forall n (n \in X)$; the $\Delta^0_1$ comprehension scheme consists of all axioms of form: $\forall n (\varphi(n) \leftrightarrow \psi(n)) \rightarrow \exists X \forall n (n \in X \leftrightarrow \varphi(n))$ where $\varphi$ is a $\Sigma^0_1$ formula, $\psi$ is a $\Pi^0_1$ formula and $X$ does not occur free in either $\varphi$ or $\psi$. The $\Sigma^0_1$ formula induction scheme contain the following axiom for each $\Sigma^0_1$ formula $\varphi$: $(\varphi(0) \land \forall n (\varphi(n) \rightarrow \varphi(n+1)) \rightarrow \forall n(\varphi(n))$. $RCA_0$ 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 König’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” (the notions presented in this lemma were defined in Definition 2.2 from [36] or Definition 1.14 from [38]).

Many properties of $\mathbb{Z}(\Sigma)$ remains also valid if some axioms from the Zermelo-Fraenkel with Choice (ZFC) model of set theory are relaxed. First, $\mathbb{Z}(\Sigma)$ is an $l$-group according to $RCA_0$ 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 $RCA_0$ (look also to Example 3.3 in [36] or Example 2.5 in [38]-the part where a free abelian group with $\omega$ generators is organized as a group in $RCA_0$; the
proof of this part remains valid even \( Z(\Sigma) \) has a finite (countable) number of generators). Another possibility of representing \( Z(\Sigma) = Z^\Sigma \) as a set in the second order arithmetic is to use finite sequences of pairs \( (x, z) \) with \( x \in \Sigma \) and \( z \in \mathbb{Z} - \{0\} \). This was done in Definition 3.4 from [37] which can also be applied to our case since \( \Sigma \) is a finite set. Moreover the binary operations on \( Z(\Sigma) \) satisfy the conditions on Definition 2.6 in [31]. This means that \( Z(\Sigma) \) is an \( l \)-group in \( RCA_0 \).

Now, by Theorem 2.21 in [31] we can say that Theorem 4.16 is provable in \( RCA_0 \). By Theorem 5.3 in [31] it follows that Corollary 4.17 is provable in \( RCA_0 \). An important result given as Corollary 6.5 in [31] shows us that Corollary 4.21 is provable in \( RCA_0 \) (see Corollary 5.2 in [36] or Proposition 5.5 and Corollary 5.3 in [38]). Moreover, in \( RCA_0 \) is also provable Theorem 4.23 which says that \( Z(\Sigma) \) is the \( o \)-epimorphic image of a totally ordered free group (see the proof of Theorem 5.7 in [38]).

We can conclude that, even we replace some axioms of the ZFC model of set theory with some weaker ones, many properties of \( Z(\Sigma) \) obtained in the ZFC approach are preserved. The Fraenkel-Mostowski (FM) model of set theory could be a more suitable framework for computer science. In the next subsection we formalize the concept of generalized multisets in the FM approach. We adapt the notions and results in this subsection to the FM framework, and we prove that many results in this subsection are preserved even if we work in the FM axiomatic model of set theory.

### 4.2.2 Nominal Generalized Multisets

We formalize now the concept of generalized multisets in the FM universe.

**Definition 4.25.** An FM-group is a triple \((G, +, \cdot)\) such that the following conditions are satisfied:

- \((G, +)\) is a group.
- \((G, \cdot)\) is a nominal set.
- For each \( \pi \in S_A \) and each \( x, y \in G \) we have \( \pi \cdot (x + y) = \pi \cdot x + \pi \cdot y \) and \( \pi \cdot (-a) = -(\pi \cdot a) \).

**Theorem 4.26** (FM). \( Z(\Sigma) \) is a free abelian FM-group whenever \((\Sigma, \cdot)\) is a finite nominal set.

**Theorem 4.27** (FM). \( F(\Sigma) \) is an FM-group whenever \((\Sigma, \cdot)\) is a finite nominal set. Moreover each element \([x_1^{e_1}x_2^{e_2} \ldots x_n^{e_n}]\) from \( F(\Sigma) \) is supported by the set \( U = \text{supp}(a_1) \cup \ldots \cup \text{supp}(a_k) \) when \( \Sigma = \{a_1, \ldots, a_k\} \).
Theorem 4.28 (FM). Let \((\Sigma, \cdot)\) be a finite nominal set. Let \(j : \Sigma \to \mathbb{Z}(\Sigma)\) be the function which maps each \(a_i \in \Sigma\) into \(\tilde{a}_i \in \tilde{\Sigma}\). If \((G, +, \diamond)\) is an arbitrary abelian FM-group and \(\varphi : \Sigma \to G\) is an arbitrary function, then there exists a unique finitely supported homomorphism of abelian groups \(\psi : \mathbb{Z}(\Sigma) \to G\) with \(\psi \circ j = \varphi\).

Theorem 4.29 (FM). Let \((\Sigma, \cdot)\) be a finite nominal set. Let \(i : \Sigma \to F(\Sigma)\) be the standard inclusion of \(\Sigma\) into \(F(\Sigma)\). If \((G, +, \diamond)\) is an arbitrary FM-group and \(\varphi : \Sigma \to G\) is an arbitrary function, then there exists a unique finitely supported homomorphism of groups \(\psi : F(\Sigma) \to G\) with \(\psi \circ i = \varphi\).

Theorem 4.30 (FM). \(F(\Sigma)/\text{Ker} \ g\) is an FM-group and the isomorphism \(\Theta\) between the groups \(F(\Sigma)/\text{Ker} \ g\) and \(\mathbb{Z}(\Sigma)\), defined by \(\Theta(w \uparrow \text{Ker} \ g) = g(w)\) for each \(w \in F(\Sigma)\) (where \(w \uparrow \text{Ker} \ g\) is the left coset of \(w\) modulo \(\text{Ker} \ g\)) is finitely supported.

Theorem 4.31 (FM). There exists a finitely supported isomorphism from \(\mathbb{Z}(\Sigma)\) to an FM-subgroup of \(S_{\mathbb{Z}(\Sigma)}\).

4.2.3 Conclusions

The aim of this section is to define and study “generalized multisets” both in the ZF framework and in the nominal framework. This concept was initially described using the classical ZF model of set theory (Subsection 4.2.1). Using nominal techniques, we define “FM-generalized multisets”, presenting also some nominal properties of these new concept (Subsection 4.2.2). The analogy between the results obtained by using the FM axioms of set theory and those obtained by using the ZF axioms of set theory is emphasized by the results presented in Subsection 4.2.2.

In Subsection 4.2.1 several algebraic properties of generalized multisets are presented. The central idea of this subsection is the result which states that \(\mathbb{Z}(\Sigma)\) is a finitely-generated, lattice-ordered, free abelian group. From this property of \(\mathbb{Z}(\Sigma)\), and from the general theory of groups we get new properties of generalized multisets. Some other properties of \(\mathbb{Z}(\Sigma)\) could also be obtained from the indicated references by particularizing to \(\mathbb{Z}(\Sigma)\) some results from the general theory of \(l\)-groups. We mention here just the most important ones and especially the result which are not trivial (\(\mathbb{Z}(\Sigma)\) has a known structure!) and which provide new properties for \(\mathbb{Z}(\Sigma)\). We also prove that \(\mathbb{Z}(\Sigma)\) can be organized as a totally ordered group and we obtain some ordering properties for the free group on \(\Sigma\), \(F(\Sigma)\) (see Theorem 4.23).

The algebraic properties of generalized multisets are analyzed in reverse mathematics.

We prove that the set of all generalized multisets over a finite alphabet \(\Sigma\) coincides with the set of all FM-generalized multisets over \(\Sigma\). Moreover, the set of generalized multisets over \(\Sigma\) is a free abelian FM-group and it
satisfies the universality property expressed in Theorem 4.28. The free group over $\Sigma$ is also an FM-group, and it satisfies a certain universality property (Theorem 4.29). By repeatedly applying these universality properties, a connection between the set of all generalized multisets over $\Sigma$ and the free group over $\Sigma$ is given in the FM approach, in terms of finitely supported morphisms (Theorem 4.30). Finally, an FM embedding theorem of Cayley type is given for the set of generalized multisets over $\Sigma$ (Theorem 4.31).

4.3 Event Structures in the Fraenkel-Mostowski Framework

Event structures were introduced in [23] 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, whether they exclude each other, or whether they may happen concurrently. The aim of this section is to define and study “elementary event structures”, “event structures” and “causality function” in FM framework. These concepts were initially described using the classical ZF model of set theory [23]. Using nominal techniques, we define “FM-elementary event structures”, “FM-event structures” and “FM-causality function”, presenting also some properties of these new concepts. The analogy between the results obtained by using the FM axioms of set theory and those obtained by using the ZF axioms of set theory is emphasized. The results in this section were presented in [AA2].

4.3.1 Nominal Event Structures

Definition 4.32 (Winskel). An elementary event structure is a partial order $(E, \leq)$, where $E$ is a set of events and $\leq$ is a partial order over $E$.

Definition 4.33 (FM). An FM-elementary event structure $E$ is a nominal set $(E, \cdot)$ together with an equivariant partial order relation ”$\leq$” on $E$.

Definition 4.34 (ZF). A complete elementary event structure $E$ is an elementary event structure $(E, \leq)$ such that every subset $X \subseteq E$ has a least upper bound with respect the order relation $\leq$.

Definition 4.35 (FM). An FM-complete elementary event structure $E$ is an FM-elementary event structure $(E, \leq, \cdot)$ such that every finitely-supported subset $X \subseteq E$ has a least upper bound with respect the order relation $\leq$.

Theorem 4.36 (ZF). Let $(E, \leq)$ be a complete elementary event structure. Then every subset $X \subseteq E$ has a greatest lower bound with respect the order relation $\leq$. 

18
Theorem 4.37 (FM). Let \((E, \leq, \cdot)\) be an FM-complete elementary event structure. Then every finitely-supported subset \(X \subseteq E\) has a greatest lower bound with respect the order relation \(\leq\).

Definition 4.38 (ZF). Let \((E, \leq)\) be an elementary event structure. A causality function on \(E\) is a causality preserving function from \(E\) to \(E\), i.e. a function \(f : E \to E\) with the property that: \(e \leq e'\) implies \(f(e) \leq f(e')\) for all \(e, e' \in E\).

Definition 4.39 (FM). Let \((E, \leq, \cdot)\) be an FM-elementary event structure. An FM-causality function on \(E\) is a causality preserving, finitely-supported function from \(E\) to \(E\), i.e. a finitely supported function \(f : E \to E\) with the property that: \(e \leq e'\) implies \(f(e) \leq f(e')\) for all \(e, e' \in E\).

Theorem 4.40 (ZF). Let \((E, \leq)\) be a complete elementary event structure and \(f : E \to E\) a causality function on \(E\). Let \(P\) be the set of fixed points of \(f\). Then \((P, \leq)\) is a complete elementary event structure.

Theorem 4.41 (FM). Let \((E, \leq, \cdot)\) be an FM-complete elementary event structure and \(f : E \to E\) an equivariant causality function over \(E\). Let \(P\) be the set of fixed points of \(f\). Then \((P, \leq, \cdot)\) is an FM-complete elementary event structure.

4.3.2 Conclusions

The aim of this section is to study the "event structures" in the nominal framework. We define the so-called "FM-elementary event structures" providing several nominal properties of this new concept. The main result of this section is a Tarski-like theorem given in the FM approach (Theorem 4.41).

Since the elementary event structures are actually the posets, the causality functions are the monotone functions, and the complete elementary event structures are the complete lattices, all the results in this section can be adapted to the theory of partially ordered sets. An FM-poset can be defined as an FM-elementary event structure. An FM-monotone function can be defined as an FM-causality function. An FM-complete lattice can be defined as an FM-complete elementary event structure. The results in this section can be rewritten in terms of FM-posets, FM-monotone functions, and FM-complete lattices as well. For example the main result can be expressed as: Let \((E, \leq, \cdot)\) be an FM-complete lattice and \(f : E \to E\) an equivariant monotone function over \(E\). Let \(P\) be the set of fixed points of \(f\). Then \((P, \leq, \cdot)\) is an FM-complete lattice. However we choose to present the results in this section in terms of event structures (and not in terms of posets or lattices) because the concept of "event structures" is often used in computer science.
Chapter 5

Extensions of the Fraenkel-Mostowski Set Theory

The finite support property of the FM set theory is very strong. We try to study what happens if we replace this strong axiom with a weaker one. In this chapter we generalize the FM set theory by giving a new set of axioms which defines the Extended Fraenkel-Mostowski (EFM) set theory. As usual, we denote the infinite set of atoms (in the ZFA approach) by \( A \), and the group of all bijections of \( A \) by \( P_A \) both in the Fraenkel-Mostowski and in the Extended Fraenkel-Mostowski approach. We prove that some properties of \( P_A \) defined in the EFM framework are also properties of \( P_A \) defined in the FM framework. We also define an extended interchange function without using the finite support property in the FM set theory. We use only the new Axiom 11’ of the EFM set theory which states that each subset of \( A \) is either finite or cofinite and which is a consequence of the Axiom 11 of the FM set theory. We decided to work with EFM axioms instead of FM axioms because many properties of the interchange function can be proved by using in the axiomatic model we work, a more relaxed axiom which is axiom 11’ in the description of the EFM set theory, instead of a very strong axiom which is axiom 11 in the description of the FM set theory. So, for the proof of some important algebraic and topological properties of the domain of the interchange function we don’t need to assume that each element of an arbitrary set has finite support as it is done in the axiomatic construction of the FM set theory (see axiom 11). These properties of \( P_A \) are valid if we assume only the axiom which says that each subset of the set \( A \) of atoms is either finite or cofinite (i.e. the axiom 11’).

We present a new axiomatic set theory in which the sets are pairs \((X, \cdot)\), where \( X \) is defined by ZFA–C rules, and \( \cdot \) is an extended interchange function which is an action on \( X \) of the group of all bijections of \( A \). Using some
group theory results which can be proved without involving the axiom of choice, we obtain some new results about the extended interchange function which remain valid also for the interchange function. The properties of the extended interchange function and interchange function obtained in this chapter, can also be successfully applied in nominal logic, since the permutative renamings [13] are defined as a result of applying the interchange function to a permutation and to an element in a nominal set. The notion of renaming can be generalized in the EFM set theory and some new results can be obtained.

5.1 Extended Fraenkel Mostowski Axioms

The Extended Fraenkel Mostowski axioms are the FM axioms with the finite support axiom (axiom 11) replaced by a weaker axiom (axiom 11’):

- axiom 11 in FM: \( \forall x. \exists S \subset A. S \text{ is finite and } S \text{ supports } x \).
- axiom 11’ in EFM: Each subset of \( A \) is either finite or cofinite.

5.2 Algebraic and Topological Properties of EFM-Sets

We give now some results which finally allows us to say that the domain of the interchange function and the domain of the extended interchange function have some similar algebraic and topological properties.

The properties of the domain of the extended interchange function (interchange function) are properties of the extended interchange function (interchange function). Since the sets in the EFM approach (respectively in the FM approach) are pairs \((X, \cdot)\) where \(X\) is a ZFA-set and \(\cdot\) is an extended interchange function over \(X\) (respectively \(\cdot\) is an interchange function over \(X\)), we can also say that the algebraic and topological properties of extended interchange function (interchange function) provide algebraic properties of EFM-sets (FM-sets). The work in this section can be found in [AA1, AA10, AA3].

We make the following notations:

- \(P_A\)-the set of all bijections on the set \(A\) of atoms.
- \(S_A\)-the set of all finitary permutations on \(A\).

5.2.1 Algebraic and Topological Properties of the Group of Permutations of Atoms in the EFM Model

Theorem 5.1. If we work in the extended Fraenkel-Mostowski axiomatic model of set theory then each subgroup of \(P_A\) which is finitely generated is
also finite.

**Proposition 5.2.** There is a one-to-one function from the subgroups lattice $P_A/S_A$ to the lattice of equivalence classes of partitions of $A$.

For each group $G$ we denote by $\mathcal{L}(G)$ its subgroups lattice.

**Theorem 5.3.** $\mathcal{L}(P_A)$ 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 5.4.** 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 $P_A$.

**Theorem 5.5.** Let $\mathcal{F}$ be an open set in $\mathcal{L}(P_A)$ (i.e. an open family of subgroups with respect 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 $H \supseteq K$.

**Theorem 5.6.** A continuous function $f : \mathcal{L}(P_A) \rightarrow \mathcal{L}(P_A)$ is completely determined by its values on the finite subgroups of $P_A$.

**Theorem 5.7.** A function $f : \mathcal{L}(P_A) \rightarrow \mathcal{L}(P_A)$ is Scott-continuous if and only if $f$ is monotone and for each directed family $\mathcal{F}$ of subgroups of $G$ we have $f(\bigcup_{H \in \mathcal{F}} H) = \bigcup_{H \in \mathcal{F}} f(H)$.

**Theorem 5.8.** A function $f : \mathcal{L}(P_A) \rightarrow \mathcal{L}(P_A)$ 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 $P_A$.

**Theorem 5.9.** Whenever $H \ll K$ in $\mathcal{L}(P_A)$ we can interpolate a finite subgroup of $P_A$ between $H$ and $K$.

**Theorem 5.10.** Each continuous function $f : \mathcal{L}(P_A) \rightarrow \mathcal{L}(P_A)$ has a least fixpoint. It is given by $\bigcup_{n \in \mathbb{N}} f^n(\{\text{id}_A\})$ where $\text{id}_A$ is the identity map on $A$.

Since the axiom 11’ of the EFM set theory is a direct consequence of the axiom 11 of the FM set theory, we can conclude that the results expressed in Theorems 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 and 5.10 remain valid also if we work in the classical Fraenkel-Mostowski model of set theory.

### 5.2.2 Conclusions

The main purpose of describing the EFM model is to prove that some properties of $P_A$ which are valid in the FM approach remain also valid if, instead of the axiom 11 in the description of FM model, we introduce the weaker
axiom 11’ in the description of EFM model. For the proof of some important properties of \( P_A \), we don’t necessarily need to assume that for each element in an FM-set there is a finite nonempty set supporting it as we did in the axiomatic description of the FM model (see axiom 11). To prove some properties of \( P_A \) instead of axiom 11, we can use only a consequence of it (i.e. axiom 11’) which says that each subset of \( A \) is either finite or cofinite. This section shows that the domain of the extended interchange function defined in EFM approach and the domain of the interchange function defined in FM approach have similar properties.

5.3 Permutative 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, and how some results obtained in the EFM model can be translated to the FM model. We naturally extend some notions and results of nominal logic, and together with some mathematical properties obtained in Section 5.2 and some additional combinatorial results (which remain valid in an axiomatic model of set theory where the axiom of choice is disallowed), we are able now to give some new properties of permutative renamings. The work in this section can be found in [AA10].

5.3.1 Algebraic and Combinatoric Properties of Permutative Renamings

**Definition 5.11.** 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 \( \cdot : P_A \times X \rightarrow X \) is an extended interchange function on \( X \).

A similar definition can be used to characterize the permutative renamings of elements from an FM-set. An important remark is that in the FM universe all the permutations of \( A \) are finitary i.e. \( S_A \) coincides with \( P_A \). 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 \( \pi \in S_A \) and \( \cdot : S_A \times X \rightarrow X \) is an interchange function on \( X \). In the EFM framework we allow the presence of non-finitary permutations and hence it is natural to define the permutative renamings of an element \( x \) as the elements of form \( \pi \cdot x \), where \( \pi \in P_A \).

**Remark 5.12.** It is worth noting that M.Gabbay and A.Pitts work with permutations obtained by composing finitely many transpositions. 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 from \( A \) to \( A \), \( X \) is an EFM-set and the extended interchange function is defined on \( P_A \) not
only on $S_A$ (like in [13, 14]). A permutative renaming in our approach is of the form $\pi \cdot x$, where $\pi \in P_A$. The particular class of finitary permutative renamings (namely the class of permutative renamings under the action $\cdot|_{S_A}$) is well described in [13]. The notion of permutative renaming defined in [13] is a particular case of the notion of permutative renaming defined by Definition 5.11.

**Theorem 5.13.** Let $x$ be an element of an arbitrary EFM-set $X$. If we consider a finite number of permutations, then we can obtain only a finite number of renamings of $x$ generated by applying the extended interchange function to $x$ and to each composition of these permutations and their inverses.

Let $IREN(\pi)$ be the set of invariants $x \in X$ under $\pi$, i.e., $IREN(\pi) = \{x \in X \mid \pi \cdot x = x\}$.

**Corollary 5.14.** Let $X$ be a finite EFM-set, and a group $G \overset{\text{def}}{=} \{\{\pi_1, \pi_2, \ldots, \pi_m\}\}$ 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

$$k = \frac{1}{|G|} \sum_{\pi \in G} |IREN(\pi)|.$$ 

Theorem 5.13 and Corollary 5.14 are also valid in FM framework.

**5.3.2 Conclusions**

We prove that some properties of renamings which are valid in the FM approach remain also valid in EFM approach in which a weaker axiom 11’ is used instead of axiom 11 of FM model. As we already mentioned, the proofs of some important properties of renamings do not require that for each element in an arbitrary FM-set there is a finite nonempty set supporting it (as we did in the axiomatic description of the FM model by axiom 11). In this section we show that renamings defined in EFM approach have similar properties with the renamings defined in FM approach [13]. Therefore, we can work in a model where, instead of an axiom which forces each element in each set to have finite support (i.e. axiom 11), we use an axiom on the structure of $A$ (axiom 11’), and finally obtain similar properties of renamings.
Bibliography

ISI Publications


IEEE


Technical Reports

Bibliography


