PERMUTATIVE RENAMINGS IN THE EXTENDED FRAENKEL-MOSTOWSKI SET THEORY

BY

ANDREI ALEXANDRU and GABRIEL CIOBANU

Abstract. In the new framework of the extended Fraenkel-Mostowski set theory, we define an extended interchange function as an action on a permutation group, and a new notion of permutative renaming by generalizing an existing notion of finitary permutative renaming. Some algebraic and combinatorial properties of permutative renamings expressed by using the Fraenkel-Mostowski axioms remain valid in the new framework even if we replace one axiom with a weaker axiom.

Mathematics Subject Classification 2010: 03E25, 03E30, 03B70.

Key words: finite support axiom, extended Fraenkel-Mostowski framework, permutative renamings.

1. Introduction

Renaming the variables of an expression in a way that preserves its meaning is called α -renaming. Some of the subtleties related to α -renaming can be described by using the abstraction operation of the λ -calculus, together with the operation of application. Application and abstraction work together according to the β -rule $(\lambda x.M)N = M[x := N]$. Abstraction $\lambda x.M[x]$ binds a free variable x in M . Substitution $[x := N]$ is only performed for free occurrences of x . In order to avoid ambiguities, it is assumed that the bound variables occurring in a certain expression are different from the free ones, and this can be obtained by renaming bound variables. The expressions differing only in the names used for bound variables are identified by α -equivalence. A correct variable renaming is one that preserves the α -equivalence class of the expression. 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 [5, 7]; 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 (AC) from the other axioms of the Zermelo-Fraenkel (ZF) set theory. It was rediscovered and used by Gabbay and Pitts [5] 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 modulo α -equivalence can be modeled inductively. This is because nominal 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 [5], 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 .

In [1] we generalized 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 description of the FM set theory was replaced in [1] by a weaker axiom which requires only a certain structure of the set of atoms. Many algebraic properties of sets, which are valid in the FM framework, remain valid also in the EFM framework. In this paper 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 set theory can be translated to the FM set theory. We naturally extend some notions and results of nominal logic, and together with some mathematical properties obtained in [1] and some additional combinatorial results which are proved without using the axiom of choice, we are able now to give some new properties of the interchange function and permutative renamings.

The structure of the paper is as follows. Section 2 presents formal definitions related to permutative renamings and extended interchange function. In Section 3 we present several group theory and combinatorial results applied in the nominal logic. These results allow us to solve some counting problems involving renamings. Some properties of permutative renamings which are valid in FM approach can be extended in EFM approach, even if in EFM we assume only a weaker axiom 11' instead of the finite support property in FM set theory. In Section 4, using group theory, we present some algebraic properties of the (domain of the) extended interchange function. Some connections between old and new results are presented in Section 5. Conclusions end the paper.

2. Renamings in the extended Fraenkel-Mostowski framework

We remind several definitions and results from [1].

Let A be an infinite set of atoms (also called *names*). A is characterized by the axiom “ $y \in x \Rightarrow x \notin A$ ” which means that only non-atoms can have elements.

Definition 2.1.

- i) A *transposition* is a function $(ab) : A \rightarrow A$ with the property $(ab)(a) = b$, $(ab)(b) = a$ and $(ab)(n) = n$ for $n \neq a, b$.
- ii) A *permutation* of A is a bijection π from A to A .
- iii) A *substitution* is a function $\{b|a\} : A \rightarrow A$ with the property $\{b|a\}(n) = n$ if $n \neq a$ and $\{b|a\}(a) = b$.

Let S_A be the set of all permutations over A . S_A is a group. Let $\overline{S_A}$ be the group of finitary permutations (i.e the group of permutations which leave unchanged all but finitely many atoms). In fact $\overline{S_A}$ is the set of all functions π generated by composing finitely many transpositions. For $S \subset A$, we denote by $Fix(S)$ the set $\{\pi \mid \pi(a) = a \text{ for all } a \in S\}$.

Definition 2.2. • Let X be a set defined by the axioms of ZFA set theory. An *interchange function* over X is a function $\cdot : S_A \times X \rightarrow X$ 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 exists a finite nonempty set $S \subset A$ such that for each $\pi \in Fix(S) \cap \overline{S_A}$ we have $\pi \cdot x = x$.

- An *FM set* is a pair $(X, \cdot)$, where X is a set defined in the ZFA set theory without axiom of choice, and $\cdot : S_A \times X \rightarrow X$ is an interchange function over X . We simply use X whenever no confusion arises.

Definition 2.3. Let X be an FM set. We say that $S \subset A$ *supports* x whenever for each $\pi \in \text{Fix}(S) \cap \overline{S_A}$ we have $\pi \cdot x = x$.

The properties of the interchange function allow always to find a finite set supporting x ; in fact this assertion is an axiom (axiom 11) in the description of the FM set theory. The new notion of “extended interchange function” was introduced in [1].

Definition 2.4. • Let X be a set defined by the axioms of ZFA set theory. An *extended interchange function* over X is a function $\cdot : S_A \times X \rightarrow X$ 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.

- An *EFM set* is a pair $(X, \cdot)$, where X is a set defined in the ZFA set theory without choice, and $\cdot : S_A \times X \rightarrow X$ is an extended interchange function on X . We simply use X whenever no confusion arises.

Remark 2.1. Since S_A is a group, the interchange function and the extended interchange function $\cdot : S_A \times X \rightarrow X$ are actions of the group S_A on the set X ; we have $Id \cdot x = x$ and $\pi \cdot \pi' \cdot x = (\pi \circ \pi') \cdot x$ for all $\pi, \pi' \in S_A$ and all $x \in X$.

Example 2.1. 1. The set A of atoms is both an FM set and an EFM set (when each subset of A is either finite or cofinite) with interchange function, respectively extended interchange function given by $\pi \cdot a = \pi(a)$, $\forall \pi \in S_A, a \in A$.

2. The set $\overline{S_A}$ is both an FM set and an EFM set (when each subset of A is either finite or cofinite) with the interchange function, respectively extended interchange function given by $\pi \cdot \sigma := \pi \circ \sigma \circ \pi^{-1}$ for all $\pi \in S_A$ and $\sigma \in \overline{S_A}$. $(\overline{S_A}, \cdot)$ is an FM set because for each $\sigma \in \overline{S_A}$ we have that the finite set $\{a \in A \mid \sigma(a) \neq a\}$ supports σ .

3. The set S_A is an EFM set (when each subset of A is either finite or cofinite) with the extended interchange function given by $\pi \cdot \sigma := \pi \circ \sigma \circ \pi^{-1}$ for all $\pi, \sigma \in S_A$.

We present the axiomatic descriptions of both the Fraenkel-Mostowski [5] and Extended Fraenkel-Mostowski [1] set theories.

The following axioms describes completely the Fraenkel-Mostowski set theory:

1. $\forall x.(\exists y.y \in x) \Rightarrow x \notin A$ (only non-atoms can have elements)
2. $\forall x, y.(x \notin A \text{ and } y \notin A \text{ and } \forall z.(z \in x \Leftrightarrow z \in y)) \Rightarrow x = y$
(axiom of extensionality)
3. $\forall x, y.\exists z.z = \{x, y\}$ (axiom of pairing)
4. $\forall x.\exists y.y = \{z \mid z \subset x\}$ (axiom of powerset)
5. $\forall x.\exists y.y \notin A \text{ and } y = \{z \mid \exists w.(z \in w \text{ and } w \in x)\}$ (axiom of union)
6. $\forall x.\exists y.(y \notin A \text{ and } y = \{f(z) \mid z \in x\})$, for each functional formula $f(z)$
(axiom of replacement)
7. $\forall x.\exists y.(y \notin A \text{ and } y = \{z \mid z \in x \text{ and } p(z)\})$, for each formula $p(z)$
(axiom of separation)
8. $(\forall x.(\forall y \in x.p(y)) \Rightarrow p(x)) \Rightarrow \forall x.p(x)$ (induction principle)
9. $\exists x.(\emptyset \in x \text{ and } (\forall y.y \in x \Rightarrow y \cup \{y\} \in x))$ (axiom of infinite)
10. *A is not finite*
11. $\forall x.\exists S \subset A.S \text{ is finite and } S \text{ supports } x$ (the finite support property)

Therefore, we can see the FM set theory like the ZFA set theory over an infinite set A of atoms infinite and with an additional property of finite support.

The following axioms describes completely the Extended Fraenkel-Mostowski set theory:

1. $\forall x.(\exists y.y \in x) \Rightarrow x \notin A$ (only non-atoms can have elements)
2. $\forall x, y.(x \notin A \text{ and } y \notin A \text{ and } \forall z.(z \in x \Leftrightarrow z \in y)) \Rightarrow x = y$
(axiom of extensionality)
3. $\forall x, y.\exists z.z = \{x, y\}$ (axiom of pairing)

4. $\forall x. \exists y. y = \{z \mid z \subset x\}$ (axiom of powerset)
5. $\forall x. \exists y. y \notin A \text{ and } y = \{z \mid \exists w. (z \in w \text{ and } w \in x)\}$ (axiom of union)
6. $\forall x. \exists y. (y \notin A \text{ and } y = \{f(z) \mid z \in x\})$, for each functional formula $f(z)$
(axiom of replacement)
7. $\forall x. \exists y. (y \notin A \text{ and } y = \{z \mid z \in x \text{ and } p(z)\})$, for each formula $p(z)$
(axiom of separation)
8. $(\forall x. (\forall y \in x. p(y)) \Rightarrow p(x)) \Rightarrow \forall x. p(x)$ (induction principle)
9. $\exists x. (\emptyset \in x \text{ and } (\forall y. y \in x \Rightarrow y \cup \{y\} \in x))$ (axiom of infinite)
10. *A is not finite*
- 11'. *Each subset of A is either finite or cofinite* (axiom of the structure of A)

Therefore, the Extended Fraenkel-Mostowski (EFM) set theory is similar to the ZFA set theory over an infinite set A of atoms infinite, having the additional property that each subset of A is either finite or cofinite.

Remark 2.2. Axiom 11' of the EFM set theory is a direct consequence of axiom 11 of the FM set theory (see Example 2 from [1]). Thus, the EFM set theory is a natural extension of the FM set theory; an interchange function can be seen as an extended interchange function, and an FM set can be seen as an EFM set.

Both in the FM framework and in the EFM framework, each subset of A is either finite or cofinite [1]. This structure of the atoms set A allows us to say that the axiom of choice fails both in the FM framework and in the EFM framework. More details are in [1].

We make the remark that, even the axiom of choice fails in the FM and EFM approach, a weaker form of the axiom of choice (where the choice is made from finite families) is valid.

Remark 2.3. The axiom of choice says that, for each family $\mathcal{F}$ of nonempty disjoint sets, we can find a system of representatives, namely a set that contains exactly one element from each set in $\mathcal{F}$. If $\mathcal{F}$ is a finite family of disjoint nonempty sets, this statement is a consequence of axioms

1-9 (and does not involve the axiom of choice). Indeed, if $\mathcal{F}$ contains only one nonempty set U , then we can find an element $x_0 \in U$ (because U is nonempty). According to the axiom of pairing, we obtain the set $\{x_0\}$ which is a set of representatives for $\mathcal{F}$. According to the induction principle, we can obtain a set of representatives for each finite family $\mathcal{F}$ of disjoint nonempty sets.

Now we generalize the notion of finitary permutative renaming. In this paper we deal with renamings induced by permutations, and not with renamings induced by substitutions and substitution actions (these renamings are presented in several papers of M.Gabbay and A.Pitts). In fact, a link between these viewpoints is given by the fact that for a λ -calculus expression t and two atoms a and b , we get $\{b|a\}t =_\alpha (ba) \cdot t$ for $b \notin fn(t)$ (the case $\{b|a\}t$ for $b \in fn(t)$ is explained in [4], and it is not considered here).

Definition 2.5. 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 $\pi \in S_A$ and $\cdot : S_A \times X \rightarrow X$ is an extended interchange function on X .

The same definition can be used to characterize the permutative renamings of elements from an FM set. In the FM universe only finitely supported objects are allowed. According to Example 2.1 (3) we know that S_A is an EFM set (when each subset of A is either finite or cofinite). For each $\sigma \in S_A$ we have that $\{a \in A \mid \sigma(a) \neq a\}$ is the least set supporting σ in the sense of Definition 2.3. If we assume the supplementary axiom of finite support (axiom 11) we must have that $\{a \in A \mid \sigma(a) \neq a\}$ is finite. Hence, in the FM framework, each permutation in S_A have to be finitary which means that S_A coincides with $\overline{S_A}$ in FM. 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 .

Our intuition says that a *permutative renaming* of x in FM framework is of the form $(ab) \cdot x$, where $a, b \in A$ and $(ab) \cdot x$ is denoting the result of interchanging a and b in x . If a permutation π is a composition of many transpositions, then $\pi \cdot x$ is also a permutative renaming of x . For example, $((cd) \circ (ab)) \cdot x$ denotes the result of interchanging c and d in $(ab) \cdot x$, where $(ab) \cdot x$ is defined before. In the EFM framework we eliminate the finite support property (axiom 11), and hence we allow the presence of non-finitary permutations. It is natural to define the permutative renamings of an element x as the elements of form $\pi \cdot x$, where $\pi \in S_A$, even if S_A

is different from $\overline{S_A}$ in the EFM framework. By now on, the permutative renamings are simply called renamings.

Remark 2.4. 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 S_A is the set of all bijections from A to A , X is an EFM set and the extended interchange function is defined on S_A not only on $\overline{S_A}$ (like in [4, 5]). A permutative renaming in our approach is of the form $\pi \cdot x$, where $\pi \in S_A$. The particular class of finitary permutative renamings (namely the class of permutative renamings under the action $\cdot|_{\overline{S_A}}$) is well described in [4]. The notion of permutative renaming defined in [4] is a particular case of the notion of permutative renaming defined by Definition 2.5.

3. Combinatorial properties of permutative renamings

We present several counting problems on renamings using the algebraic properties of EFM sets described in [1] and some combinatorial results which can be proved without using the axiom of choice.

Let G be a subgroup of S_A .

Definition 3.1. 1. The representation of S_A by permutations of the EFM set X is a group homomorphism $\varphi : S_A \rightarrow S(X)$ given by $\varphi(\pi)(x) = \pi \cdot x$.

2. Let x and y be elements of an EFM set X .

- (a) x and y are called equivalent, and denote this by $x \sim y$, whenever we can obtain one from another by a renaming.
- (b) x and y are called equivalent under permutations in G , and denote this by $x \sim_G y$, whenever we can obtain one from another by a renaming under a permutation in G (i.e. if there is $\pi \in G$ such that $y = \pi \cdot x$).

3. Let X be an EFM set.

- (a) $REN(x) = \{\pi \cdot x \mid \pi \in S_A\}$ is the set of all renamings of x ; we also say that $REN(x)$ is a class of renamings in X .

- (b) $REN_G(x) = \{\pi \cdot x \mid \pi \in G\}$ is the set of all renamings of x under the permutations in G ; we also say that $REN_G(x)$ 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) $IREN(x) = \{\pi \in S_A \mid \pi \cdot x = x\}$ is the set of permutations for which we obtain an invariant renaming of x (a renaming which keeps x unchanged).
- (b) $IREN_G(x) = \{\pi \in G \mid \pi \cdot x = x\}$ is the set of permutations in G for which we obtain an invariant renaming of x .

5. Let X be an EFM set.

- (a) An element $x \in X$ for which $IREN(x) = S_A$ is called invariant on all renamings. The set of elements in X which are invariants on all renamings is denoted by $IRN(X)$.
- (b) An element $x \in X$ for which $IREN_G(x) = G$ is called invariant on renamings under permutations in G . The set of elements in X which are invariants on renamings under permutations in G is denoted by $IRN_G(X)$.

Let X be an EFM set, and $G \leq S_A$. From the general theory of group actions we have the following results which we present without proofs.

Proposition 3.1.

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 3.1. If G is a finite subgroup of S_A , we denote by $\pi IREN_G(x)$ the left cosets modulo $IREN_G(x)$. A function $\psi : \{\pi IREN_G(x) \mid \pi \in G\} \rightarrow REN_G(x)$ 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 3.2. *Let G be a finite subgroup of S_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 requested (see Remark 2.3). Then, by using the classes equation in group theory,*

$$\begin{aligned} |X| &= |IRN_G(X)| + \sum_{x \in S'} |REN_G(x)| = |IRN_G(X)| + \sum_{x \in S'} [G : IREN_G(x)] \\ &= |IRN_G(X)| + \sum_{x \in S'} \frac{|G|}{|IREN_G(x)|} \end{aligned}$$

Let $IREN(\pi)$ be the set of invariants $x \in X$ under π , i.e., $IREN(\pi) = \{x \in X \mid \pi \cdot x = x\}$. If X is an FM set we say that $S \subset A$ supports x whenever for each $\pi \in Fix(S) \cap \overline{S_A}$ we have $\pi \cdot x = x$. If X is a finite FM set, $\pi \in Fix(S)$ and S supports each $x \in X$, then $IREN(\pi) = X$. Let $G \leq S_A$ be a finite group of permutations. Then we can find the number of orbits under the extended interchange function for finite EFM sets, even though we work in a set theory without the axiom of choice

Proposition 3.3. *Let X be a finite EFM set. If $G \leq S_A$ 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 $\cdot : G \times X \rightarrow X$) 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 2.3). We have $(\pi, x) \in M$ iff $\pi \in IREN_G(x)$, and 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 Theorem for finite groups and Remark 3.1,

$$(1) \quad |M| = \sum_{x \in X} |IREN_G(x)| = \sum_{x \in X} \frac{|G|}{[G : IREN_G(x)]} = \sum_{x \in X} \frac{|G|}{|REN_G(x)|}$$

By Proposition 3.1, 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 $X_1, X_2, \dots, X_k$, then they form a partition of X . According to (1), we have

$$(2) \quad |M| = \sum_{i=1}^k \sum_{x \in X_i} \frac{|G|}{|IREN_G(x)|} = \sum_{i=1}^k \sum_{x \in X_i} \frac{|G|}{|X_i|} = \sum_{i=1}^k |G| = k \cdot |G|$$

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,

$$(3) \quad |M| = \sum_{\pi \in G} |IREN(\pi)|$$

From (2) and (3) it follows 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 finite counting problems, and so they can be obtained from the axioms of the EFM set theory (see Remark 2.3). $\square$

Remark 3.2. If X is a finite FM set, S supports each $x \in X$ and $G \leq S_A$ 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

$$\begin{aligned} k &= \frac{1}{|G|} \sum_{\pi \in G} |IREN(\pi)| = \frac{1}{|G|} \left(\sum_{\substack{\pi \in G \\ \pi \in Fix(S)}} |IREN(\pi)| + \sum_{\substack{\pi \in G \\ \pi \notin Fix(S)}} |IREN(\pi)| \right) \\ &= \frac{1}{|G|} (|Fix(S)||X| + \sum_{\substack{\pi \in G \\ \pi \notin Fix(S)}} |IREN(\pi)|) = \frac{|Fix(S)||X|}{|G|} + \sum_{\substack{\pi \in G \\ \pi \notin Fix(S)}} \frac{|IREN(\pi)|}{|G|} \end{aligned}$$

Generally S_A is not finite; however, locally, it has a finite behavior. By Theorem 3.2, the previous result remains true even if G is generated by a finite set of permutations of atoms. Therefore, in such a case, we can also

obtain a formula which gives the number of classes of renamings in X under the permutations in G .

The following results present some properties of permutative renamings in the EFM framework which follow from the mathematical properties of EFM sets described in [1]. By the following results we emphasize that, even we use only axiom 11' and the notion of extended interchange function to define the permutative renamings, these have similar properties with those of permutative renamings defined in [4] where the authors use axiom 11 (i.e. the finite support property) and the notion of interchange function.

By Theorem 1 from [1] which states that S_A is a torsion group we obtain:

Theorem 3.1. *Let x be an element of an arbitrary EFM set X , and π an arbitrary permutation of atoms from A . We can obtain only a finite number of renamings of x generated by applying the extended interchange function to x and to each permutation obtained by composing π and π^{-1} multiple times (a permutation obtained by composing π and π^{-1} multiple times is of form π^k for an arbitrary $k \in \mathbb{Z}$).*

By Theorem 2 from [1] we know that S_A is locally finite. In the nominal framework we translate this as:

Theorem 3.2. *Let x be an element of an arbitrary EFM set X . If we have a finite number of permutations (in particular of transpositions), then we can obtain only a finite number of renamings of x generated by applying the extended interchange function to x and to each compositions of these permutations and their inverses. A composition of permutations $\pi_1, \pi_2, \dots, \pi_m$ and their inverses is of the form $\pi_1^{k_1} \circ \pi_2^{k_2} \circ \dots \circ \pi_r^{k_r}$, where r is a positive integer and $k_1, k_2, \dots, k_r$ are arbitrary from $\mathbb{Z}$ and $\pi_i, i = \overline{1, r}$ are arbitrary from the set $\{\pi_1, \pi_2, \dots, \pi_m\}$, not necessarily distinct.*

Corollary 3.1. *Let X be a finite EFM set, and a group $G \stackrel{\text{def}}{=} [\{\pi_1, \pi_2, \dots, \pi_m\}]$ generated by $\{\pi_1, \pi_2, \dots, \pi_m\}$, where $\pi_1, \pi_2, \dots, \pi_m \in S_A$. Then the number k of classes of renamings in X under the permutations in G is*

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

Proof. The result follows from Proposition 3.3. According to the proof of the previous theorem, it follows that G is finite, and so Proposition 3.3 could be applied. $\square$

In this section we show that renamings defined in EFM approach have similar properties with the renamings defined in FM approach [4]. Therefore, we can work in a set theory where, instead of an axiom which forces each element 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.

We do not say that our EFM set theory is better than the FM set theory (the finite support property have important benefits). We just emphasize that some weaker axioms can lead to similar properties of permutative renamings.

4. Algebraic properties of permutative renamings

We present other algebraic properties of the domain S_A of the extended interchange function which are also properties of permutative renamings because permutative renamings are defined involving the extended interchange function. We emphasize that the axiom of choice is not used in the proofs of these properties, and so the proofs remains true both in the FM framework and in the new EFM framework.

First we present a collection of some known results from group theory providing certain characterizations of renamings and extended interchange function. We also give a characterization of the transitive subgroups of S_A .

Definition 4.1. A group $G \leq S_A$ is called *transitive* if each atom can be obtain by other atom after a renaming under a permutation in G (i.e., the canonical action $\cdot : G \times A \rightarrow A$ has only one orbit).

Proposition 4.1. Let $G \leq \overline{S_A}$.

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 $D(G) = D(D(G))$.

Some results of the group theory could be used in proving properties of the interchange function and permutative renamings:

1. Let $G \leq \overline{S_A}$ with G transitive. For each $a \in A$, the subgroup $IREN(a) = \{\pi \in G \mid \pi(a) = a\}$ is not soluble [2].

2. Let $G \leq S_A$ with the property that G is transitive, and there is no $B \subset A$ 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 $\overline{S_A}$, then G must contain the group of even permutations in $\overline{S_A}$ [3].
3. Let $G \leq \overline{S_A}$ with G transitive, and B a finite subset of A . Then there is $\sigma \in G$ such that $\sigma(B) \cap B = \emptyset$ [6].

Remark 4.1. A transitive group $G \leq \overline{S_A}$ has the property that for any finite subset B of A there is a permutation $\pi \in G$ which moves B away from itself completely.

The following result gives another characterization of the *domain* of the extended interchange function. This could be not particularly relevant for computer scientists, but it is interesting for mathematicians. Some techniques and results of this type can be found in [3]. We present here a specific result for the EFM set theory which contradicts the axiom of choice. Other results of this type (which characterize the domain of extended interchange function) could be proved by using the EFM axioms.

We consider an additional condition on A only for the following result. We denote by FPA the partitions of A in which all the parts are finite. If $(A_i)_i \in FPA$, then there exists a unique natural number $|(A_i)_i|$ such that all but finitely many parts of $(A_i)_i$ have the cardinal $|(A_i)_i|$, and the cardinal $|(A_i)_i|$ is called the cardinal of the partition $(A_i)_i$. We can prove this in a similar way to the Theorem 3.1 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 a maximum cardinal (which can be as large as needed). We call this cardinal the “dimension of A ”, and the partition with maximum cardinal is called a “maximal partition”. Over FPA we introduce the following order relation: $(A_i)_{i \in I} \leq (B_j)_{j \in J}$ iff $\forall j \in J \exists I_j \subset I$ 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 $B \subset A$, B infinite and $B = \bigcup_{i \in I_1 \subset I} A_i$, then for $C \subset B$ 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.

The next result shows that there is a one-to-one function between the subgroups lattice $S_A/\overline{S_A}$ and the lattice of equivalence classes of partitions

of A , where $\overline{S_A}$ is the subgroup of S_A such that every permutation in $\overline{S_A}$ keeps fixed the points of A , except a finite number of them (this number could be 0).

Proposition 4.3. *There exists a one-to-one function from the subgroups lattice $S_A/\overline{S_A}$ to the lattice of equivalence classes of partitions of A .*

Proof. Let $H \leq S_A/\overline{S_A}$, and $\sigma_1, \sigma_2, \dots, \sigma_m \in S_A$ be some left coset representatives for $\overline{S_A}$. Let $(A_i)_{i \in I}$ be a maximal partition of A . Then for each $j \in \{1, 2, \dots, m\}$ we have that σ_j keeps fixed the equivalence class of $(A_i)_{i \in I}$; altering them on a finite subset, we can assume that all of them keeps $(A_i)_{i \in I}$ fixed. A result from the classical set theory says that if $(A_i)_{i \in I} \in FPA$, then there is $(B_j)_{j \in J} \in FPA$ such that $(A_i)_{i \in I} \sim (B_j)_{j \in J}$ and $(B_j)_{j \in J}$ is formed only by members with cardinal $|(B_j)_{j \in J}|$ and members of cardinal 1. We can say that $\sigma_1, \dots, \sigma_m$ keep fixed all except 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 $\sigma_1, \dots, \sigma_m$, and $|A_j| = |(A_i)_{i \in I}| = r$. We use the notation $A_j = \{1, \dots, r\}$. Now we consider a function f defined on S_A having values in S_r with the property that for each $\sigma \in S_A$, $f(\sigma)$ is the induced permutation in S_r for the representative of an equivalence class of σ modulo $\overline{S_A}$. It is not difficult to prove that f is a group homomorphism, and $\text{Ker}(f) = \overline{S_A}$; this homomorphism does not depend on the choice of representatives of the equivalence classes modulo $\overline{S_A}$. By renumbering the points of A_j , we can change the image with a conjugate in S_r . Since in every element in S_A all except 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 $\langle \sigma_1, \dots, \sigma_m \rangle$ keep the partition $(A_i)_{i \in I}$ fixed, and $\langle \sigma_1, \dots, \sigma_m \rangle$ acts semiregularly on all except 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 cardinal $|H|$ in these parts of $(A_i)_{i \in I}$, and so defines a partition whose cardinal is $|H|$.

In the following we prove that 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 $H = K$. $\square$

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 too much the generality because the maximum cardinal can be as large as we need. Even without this condition, P. Cameron and S. Tarzi proved in a similar way that there is a one-to-one function from the set of finitely generated subgroups of $S_A/\overline{S_A}$ to the set of equivalence classes of the partitions of A .

5. Connections between permutative renamings and finitary permutative renamings

Fresh names and renamings are studied in some papers written by M. Gabbay and A. Pitts. In this paper we present a different perspective, extending the notion of permutative renamings to the EFM framework. Even the finite support axiom was relaxed in the new framework, we are able to present a connection between permutative renamings and finitary permutative renamings:

Theorem 5.1. *All the results presented in Sections 3 and 4 remain valid if we replace “EFM set” with “FM set”, “extended interchange function” with “interchange function” and axiom 11’ of the EFM set theory with “finite support property” (i.e. axiom 11) of the FM set theory .*

Proof. According to Example 2 in [1], we see that the finite support property implies that each subset of A is either finite or cofinite, and so all the results presented in Sections 3 and 4 for the EFM framework remains valid also for the FM framework. $\square$

6. Conclusions and related work

Renaming, fresh names and binding appear in several new formalisms in computer science, and so they deserve to be studied by their own. Using group theory results, we present some properties of permutative renamings in the new Extended Fraenkel-Mostowski set theory which are also valid in the known Fraenkel-Mostowski set theory. The main benefit is that we can work with a weaker set of axioms (axioms 1-11’) in the description of EFM set theory to obtain similar properties for permutative renamings as in the FM set theory (that assumed stronger axioms). Some important results are presented (e.g., Theorem 3.1, Theorem 3.2, Corollary 3.1); in their proofs, we use a weaker axiom 11’ instead of the corresponding axiom 11 of FM set theory. Generalizing the notion of permutative renaming for the EFM framework (Definition 2.5), we prove that the permutative renamings have

in the EFM framework similar properties as in the FM framework. A strong connection between the permutative renamings and the finitary permutative renamings is established in Theorem 5.1.

An axiomatic description of the EFM set theory is presented in [1]. However, in this paper, we want to rewrite a part of nominal logic in EFM terms. A new notion of *permutative renaming* is given. Some properties of EFM sets obtained in [1] lead to similar properties of permutative renamings (Theorems 3.1 and 3.2). New algebraic and combinatorial properties of permutative renamings are proved according to the EFM axioms (Corollary 3.1 and Propositions 3.3 and 4.3). In a future work we will try to translate the nominal binding in the EFM framework.

REFERENCES

1. ALEXANDRU, A.; CIOBANU, G. – *An extension of a permutative model of set theory*, An. Ştiinţ. Univ. "Al.I. Cuza" Iaşi. Mat. (N.S.), 58 (2012), 1–18.
2. ASAR, A.O. – *On finitary permutation groups*, Turkish J. Math., 30 (2006), 101–116.
3. CAMERON, P.J. – *Permutation Groups*, London Mathematical Society Student Texts, 45, Cambridge University Press, Cambridge, 1999.
4. GABBAY, M.J.; HOFMANN, M. – *Nominal renaming sets*, Lecture Notes in Computer Science, 5330 (2008), 158–173.
5. GABBAY, M.J.; PITTS, A. – *A new approach to abstract syntax with variable binding*, Formal Aspects of Computing, 13 (2002), 341–363.
6. NEUMANN, P.M. – *The structure of finitary permutation groups*, Arch. Math. (Basel), 27 (1976), 3–17.
7. PITTS, A.M. – *Nominal logic, at first order theory of names and binding*, TACS 2001 (Sendai), Inform. and Comput., 186 (2003), 165–193.

Received: 26.XII.2012

Accepted: 2.IV.2013

Romanian Academy, Iaşi,
Institute of Computer Science,
ROMANIA
gabriel@info.uaic.ro