ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

Joanna Ochremiak

Uniwersytet Warszawski

Finitely supported sets with actions of endomorphism monoids

Praca semestralna nr 2

(semestr zimowy 2012/13)

Opiekun pracy: Bartosz Klin

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

FINITELY SUPPORTED SETS WITH ACTIONS OF ENDOMORPHISM MONOIDS

JOANNA OCHREMIAK

Abstract. We study m-sets i.e. sets equipped with an action of endomorphism monoid, with finitely supported elements. We prove a representation theorem for single-generated m-sets and functions that commute with endomorphisms. We show that in well-behaved atoms m-sets generalize nominal sets.

1. Introduction

The idea of studying properties of sets equipped with an action of a monoid comes from the theory of nominal sets [4], where the monoid is additionally required to be a group. In computer science, nominal sets were first introduced in papers by Gabbay and Pitts (see e.g. [3]), where they were used as an algebra for name binding.

Given an infinite set $\mathbb{A}$ of *atoms* and the group G of all its permutations, one can consider an arbitrary G-set X (i.e. a set equipped with an action of the group G) and study the relations between the canonical action of G on $\mathbb{A}$ and the action of G on X. We say that a G-set X is *nominal* if for each element $x \in X$ the result of applying any π in G to x is determined by a set of finitely many atoms. Formally, there exist a finite set S of atoms, called a *support* of x, such that $\pi(x) = x$ for all permutations π that act as the identity on S.

When we consider the group of all permutations of the set of atoms, we perceive atoms as interchangeable and with no structure, except for the equality. This kind of atoms turns out to be useful for describing variable names in programs or logical formulas, since their permutations provide a good way of modeling renaming of variables.

In [1] Bojańczyk, Klin and Lasota, studying languages and automata over infinite alphabets, introduced nominal sets over atoms with additional structure. They model atoms as countable relational structures together with their groups of automorphisms. This corresponds to the fact that the device, e.g. an automaton, gains more access to the structure of its infinite alphabet. For example, if the alphabet consists of totally ordered atoms, the automaton can decide which letter is bigger.

The more relational structure we put on atoms, the more access to them we obtain. In this paper, our idea is to go in the opposite direction and restrict this access to its positive part. For atoms with equality relation this means that we can only detect that the atoms are equal. For instance, an automata with such restricted access can

do a step if two atoms are equal, but can not detect and react to the fact that atoms are distinct.

Another example comes from π-calculus [5], where positive tests for equality of names are present, but distinct names cannot be detected. Accordingly, the so-called presheaf semantics for the π-calculus [2] is based on arbitrary functions between sets of names, and not just on injective functions.

A natural way of catching only the positive part of the relational structure of atoms, is to consider all their endomorphisms. In this paper we study sets equipped with an action of endomorphism monoids. We define a counterpart of a nominal set, which we call an *m-set*. For atoms with equality, we provide a finite representation of *single-generated* m-sets and functions that commute with endomorphisms. Moreover, we prove that if the atoms are well-behaved, the theory of m-sets generalizes the theory of nominal sets.

2. m-sets

An *action of a monoid* M on a set X is a binary operator $M \times X \to X$ that satisfies following conditions:

- for all $x \in X \quad e(x) = x$, where e is the neutral element of M,
- for all $x \in X$ and $f, g \in M \quad g(f(x)) = (g \circ f)(x)$.

Given an infinite set $\mathbb{A}$ of *atoms* and any monoid M of functions $f\colon \mathbb{A} \to \mathbb{A}$, one can consider an arbitrary set X equipped with an action of the monoid M and study the relations between the canonical action of M on $\mathbb{A}$ and the action of M on X.

Atoms are modelled as countable relational structures and considered together with their monoids of endomorphisms i.e. functions $f\colon \mathbb{A} \to \mathbb{A}$ that are consistent with the relational structure. Examples of atoms include:

- the *equality atoms* $(\mathbb{N}, =)$, where $\mathbb{N}$ is a countably infinite set with the equality relation. Here the monoid of endomorphisms $\mathrm{End}(\mathbb{N})$ contains all functions $f\colon \mathbb{N} \to \mathbb{N}$.
- the *total order atoms* $(\mathbb{Q}, \leq)$, where $\mathbb{Q}$ is the set of rational numbers with their order. Here the monoid of endomorphisms $\mathrm{End}(\mathbb{Q})$ contains all monotone functions $f\colon \mathbb{Q} \to \mathbb{Q}$.

The choice of atoms is a parameter of the notion of an *m-set*. Fix a relational structure $\mathbb{A}$ for the atoms. From now on, by endomorphism we understand an endomorphism of $\mathbb{A}$. Consider a set X equipped with an action of the endomorphism monoid $\mathrm{End}(\mathbb{A})$.

Definition 2.1. A set $S \subseteq \mathbb{A}$ of atoms *supports* an element $x \in X$ if $f(x) = g(x)$ for all endomorphisms f, g, such that $f|_S = g|_S$. A set X is an *m-set* if every its element is supported by a finite set S.

If $f|_S = g|_S$, we write $f \approx_S g$.

Example 2.2. For any atoms, the set of all atoms $\mathbb{A}$ is an m-set, as any atom $a \in \mathbb{A}$ is supported by the singleton $\{a\}$. Another example of an m-set is $\mathbb{A}^*$, with an action of the endomorphism monoid $\mathrm{End}(\mathbb{A})$ defined point-wise. The set of words $\mathbb{A}^*$ is an m-set because each word is supported by the set of its letters.

Example 2.3. Consider the equality atoms. The action of the endomorphism monoid on $\mathbb{A}$ extends element-wise to an action on the powerset of $\mathbb{A}$. Any finite set of atoms is clearly finitely supported, but no infinite set of atoms has a finite support. Therefore, the finite powerset of $\mathbb{A}$ is an m-set, while the whole powerset of $\mathbb{A}$ is not.

Example 2.4. For any atoms, we denote by $\mathbb{A}^{(n)}$ the set of non-repeating n-tuples of atoms. Consider a set $\mathbb{A}^{(2)} \cup \{*\}$, with an action of the endomorphism monoid defined as follows:

$$f(a,b) = \begin{cases} (f(a), f(b)) & \text{if } f(a) \neq f(b), \\ * & \text{otherwise,} \end{cases} \qquad f(*) = * \ .$$

A non-repeating pair (a, b) that belongs to $\mathbb{A}^{(2)} \cup \{*\}$ is supported by $\{a, b\}$ and the element $*$ has an empty support. Hence, the set $\mathbb{A}^{(2)} \cup \{*\}$ is an m-set.

Proposition 2.5. *If S supports an element x of an m-set X, then $f(S)$ supports $f(x)$, for any endomorphism f.*

Proof. If $g \approx_{f(S)} h$, then $g \circ f \approx_S h \circ f$. Therefore,

$$g(f(x)) = g \circ f(x) = h \circ f(x) = h(f(x)).$$

□

A support of an element of an m-set is not unique. In particular, supports are closed under adding atoms. If each element of every m-set X has a canonical least support, we say that the atoms *admit least supports*.

Proposition 2.6. *The equality atoms admit least supports.*

Proof. Take an element x of an m-set X, which is supported by finite sets S and T of atoms. We need to show that the set $S \cap T$ supports x. Let $f \approx_{S \cap T} g$ and consider any function h, such that:

$$h(a) = \begin{cases} f(a) & \text{if } a \in S, \\ g(a) & \text{if } a \in T. \end{cases}$$

Since $f \approx_S h$ and $h \approx_T g$, we have that $f(x) = h(x) = g(x)$. □

In m-sets functions should commute with endomorphisms. Take X and Y to be m-sets. We call a function $F \colon X \to Y$ *m-equivariant* if $F(f(x)) = f(F(x))$, for any $x \in X$ and any endomorphism f.

Proposition 2.7. *Let $F\colon X \to Y$ be an m-equivariant function between two m-sets. If S supports an element x of the m-set X, then it also supports the element $F(x)$ of the m-set Y.*

Proof. If $f \approx_S h$, then $f(F(x)) = F(f(x)) = F(h(x)) = h(F(x))$. □

Consider a set X equipped with an action of a monoid M. For any subset Y of X the set

$$M \cdot Y = \{f(x) \mid f \in M,\ x \in Y\} \subseteq X$$

is called a *segment generated* by Y. If $Y = \{x\}$ we write $M \cdot x$ instead of $M \cdot \{x\}$, and call $M \cdot x$ a *single-generated segment*.

In the special case when $M \cdot Y = X$ we say that Y *generates* X. Moreover, if there exists a finite set Y, such that $M \cdot Y = X$, then X is called *finitely-generated*. Observe that

$$M \cdot Y = \bigcup_{x \in Y} M \cdot x.$$

Therefore, a finitely-generated set is a sum of finitely many single-generated segments (not necessarily disjoint). If the set X is a single-generated segment itself i.e. $X = M \cdot x$, we call x a *generator* of X.

Example 2.8. For any atoms the action of the endomorphism monoid on $\mathbb{A}$ extends point-wise to an action on the set of tuples $\mathbb{A}^n$. In the equality atoms, the set $\mathbb{N}^2$ is a single-generated segment:

$$\mathbb{N}^2 \ = \ \mathrm{End}(\mathbb{N}) \cdot (1,2).$$

In the total order atoms, the set $\mathbb{Q}^2$ is finitely-generated:

$$\mathbb{Q}^2 \ = \ \mathrm{End}(\mathbb{Q}) \cdot (9,1) \ \ \cup \ \ \mathrm{End}(\mathbb{Q}) \cdot (-1,3).$$

Notice that the single-generated segments $\mathrm{End}(\mathbb{Q}) \cdot (9,1)$ and $\mathrm{End}(\mathbb{Q}) \cdot (-1,3)$ are not disjoint. Their intersection is also a single-generated segment $\mathrm{End}(\mathbb{Q}) \cdot (5,5)$.

In m-sets, the finitely-generated sets play the role of finite sets.

3. Representation of sets

From now on, we concentrate on m-sets over the equality atoms. In this section we show that every single-generated m-set can be represented in a finite way as a quotient of tuples of atoms.

3.1. **Positive quantifier-free formulas.** Let X be an m-set. A subset $Y \subseteq X$ is called *m-equivariant* if $f(y) \in Y$ for each $y \in Y$ and every endomorphism f. Note that an m-equivariant subset is an m-set itself.

Considering the point-wise action of the monoid on the product of m-sets we can talk about *m-equivariant relations*. For instance, a binary m-equivariant relation on sets X and Y is any m-equivariant subset of $X \times Y$.

Example 3.1. There are three m-equivariant binary relations on atoms: the empty ralation, the full relation and the equality relation:

$$\emptyset \qquad \mathbb{A} \times \mathbb{A} \qquad \{(a, a) \ : \ a \in \mathbb{A}\}.$$

Observe that the above relations are exactly the binary relations that can be defined by positive quantifier-free formulas. This is no coincidence, we will prove that in equality atoms m-equivariant relations on atoms are the same as relations definable by positive quantifier-free formulas.

The set of positive quantifier-free formulas, over variables $(x_1, \ldots, x_n)$, is defined by induction:

- $\bot$ and $\top$ are formulas,
- $x_i = x_j$ is a formula, for any variables x_i, x_j,
- if φ and ψ are formulas, then so are $\varphi \wedge \psi$ and $\varphi \vee \psi$.

We allow no constants. For instance,

$$x_1 = x_2 \quad \vee \quad x_2 = x_3$$

is a positive quantifier-free formula over variables (x_1, x_2, x_3). It determines a ternary m-equivariant relation with two overlapping single-generated segments:

$$\{(a, a, b) \ : \ a, b \in \mathbb{A}\} \qquad \{(a, b, b) \ : \ a, b \in \mathbb{A}\}.$$

A positive quantifier-free formula α, over the variables $(x_1, \ldots, x_n)$, that does not use disjunction is called a *type*. If an n-tuple of atoms satisfies the formula, we say that it has type α. A single n-tuple has many types. For example, the tuple $(1, 1, 2)$ has type $x_1 = x_2$ and type $\top$.

Up to logical equivalence, there are finitely many types over a given set of variables. It is not difficult to see that an m-equivariant n-ary relation on atoms is a single-generated segment if and only if it is defined by a type. Therefore, two tuples share a type if and only if there exists a single-generated segment of tuples that contains them both. Moreover, different single-generated segments are defined by non-equivalent types. Hence, there are only finitely many different single-generated segments contained in $\mathbb{A}^n$.

Example 3.2. The tuples $(1, 1, 2)$ and $(1, 1, 1)$ have type $x_1 = x_2$, which is equivalent to the fact that they both belong to a segment generated by $(2, 2, 8)$. But they also have type $\top$, which is a formula satisfied by all triples i.e. tuples in the segment generated by $(1, 2, 3)$.

Proposition 3.3. *A relation $R \subseteq \mathbb{A}^n$ is m-equivariant if and only if it is definable by a positive quantifier-free formula.*

Proof. The *if* part is simple. A set of tuples defined by a positive quantifier-free formula is preserved under the action of endomorphisms.

For the *only if* part, an m-equivariant relation is a union of single-generated segments. Every segment is defined by a type. Since there are finitely many possible

types, the union is finite, and therefore corresponds to a positive quantifier-free formula. □

Corollary 3.4. *Every m-equivariant relation on atoms is finitely-generated.*

3.2. **Quotient representation.** Let us consider the quotient of some m-set X by an m-equivariant equivalence relation R. There is a natural way of defining an action of the endomorphism monoid on X/R:

$$f([x]_R) = [f(x)]_R.$$

Any support S of an element $x \in X$ supports the equivalence class $[x]_R$, hence if X is an m-set then X/R is also an m-set. Moreover, it is easy to see that if X is single-generated, then so is the quotient X/R.

Let $R \subseteq \mathbb{A}^n \times \mathbb{A}^n$ be an m-equivariant equivalence relation. By Proposition 3.3, the relation R is defined by a positive quantifier-free formula φ over variables $(x_1, \ldots, x_n, y_1, \ldots, y_n)$. The n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are R-equivalent if and only if the assignment $x_i \mapsto a_i$, $y_i \mapsto b_i$ satisfies the formula. The quotient A^n/R will be denoted by A^n/φ.

We will now prove that every single-generated m-set is isomorphic to such a quotient and therefore can be represented in a finite way.

Lemma 3.5. *Every single-generated m-set is an m-equivariant image of $\mathbb{A}^n$, for some $n \in \mathbb{N}$.*

Proof. Take $S = \{a_1, a_2, \ldots, a_n\}$ to be the least support of an element x, which generates an m-set X. We define $F\colon \mathbb{A}^n \to X$ by

$$F(f(a_1, \ldots, a_n)) = f(x).$$

The function F is well defined: for every endomorphism f, the image $f(x)$ is uniquely determined by $f(a_1, \ldots, a_n)$, which is a consequence of the definition of a support. Since the whole m-set X is generated by x, the function F is surjective and it is easy to check that it is m-equivariant. □

Theorem 3.6. *Every single-generated m-set is isomorphic to $\mathbb{A}^n/\varphi$, for some $n \in \mathbb{N}$ and some positive quantifier-free formula φ over $2n$ variables defining an equivalence relation.*

Proof. Consider a single-generated m-set X. There exists an m-equivariant surjective function $F\colon \mathbb{A}^n \to X$. Let R be the kernel of F. Notice that R is an m-equivariant equivalence relation. If φ is its defining formula then the quotient $\mathbb{A}^n/\varphi$ is isomorphic to X. □

In the obtained representation, n is the number of atoms in the least support of a generating element x. It is not difficult to see that for every element that generates X, this number is the same. We call it the *dimension* of X.

Observe, that an equivalence class of any non-repeating tuple $(a_1, \ldots, a_n)$ generates $\mathbb{A}^n/\varphi$. Such a tuple is supported by the set $\{a_1, \ldots, a_n\}$. Therefore, the least

support of an equivalence class $[(a_1, \ldots, a_n)]_\varphi$ is contained in $\{a_1, \ldots, a_n\}$. Hence, it is easy to see that a single-generated set X of dimension n is not isomorphic to any A^m/ψ, for $m < n$. This is because there is no element in A^m/ψ with the least support containing n atoms. All least supports have at most m elements.

Example 3.7. Recall the m-set $\mathbb{A}^{(2)} \cup \{*\}$ defined in Example 2.4, with the action of the endomorphism monoid defined by:

$$f(a,b) = \begin{cases} (f(a), f(b)) & \text{if } f(a) \neq f(b), \\ * & \text{otherwise,} \end{cases} \qquad f(*) = * \ .$$

This set is isomorphic to $\mathbb{A}^2/\varphi$, where φ is the formula:

$$(x_1 = y_1 \wedge x_2 = y_2) \ \vee \ (x_1 = x_2 \wedge y_1 = y_2).$$

The equivalence relation defined by φ looks as follows: there is a singleton equivalence class for each non-repeating pair of atoms, and one infinite equivalence class containing all the other pairs.

Example 3.8. The same m-set $\mathbb{A}^{(2)} \cup \{*\}$ is also isomorphic to $\mathbb{A}^3/\psi$, where ψ is the formula:

$$(x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = x_3) \ \vee \ (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = y_3) \ \vee \ (x_1 = x_2 \wedge y_1 = y_2).$$

The equivalence relation defined by ψ looks as follows: for any two different atoms a_1, a_2, the triples that have a_1 on the first coordinate and a_2 on the second, belong to one equivalence class, and there is a single equivalence class containing all triples with first two coordinates equal.

3.3. **Canonical representation.** The above examples illustrate the fact that each m-set X is isomorphic to many different sets of the form $\mathbb{A}^m/\psi$. Notice, however, that the third coordinate in the second representation seems "insignificant". Our aim now is to find a canonical representation of a single-generated m-set. We begin with proving that, if n is the dimension of X, then every representation has only n "significant" coordinates.

Lemma 3.9. *Let the single-generated m-set $\mathbb{A}^m/\psi$ have dimension n. For the formula ψ over variables $(x_1, \ldots, x_m, y_1, \ldots, y_m)$ there exists an equivalent formula φ, which uses only those variables x_i, y_i, with index i belonging to some n-element subset of $\{1, \ldots, m\}$.*

Proof. Consider a non-repeating m-tuple $(a_1, \ldots, a_m)$. Its equivalence class generates the set $\mathbb{A}^m/\psi$. Therefore, the least support of this equivalence class contains n atoms. Without loss of generality let us assume that these are the atoms $a_1, \ldots, a_n$. Hence, for any atoms $b_{n+1}, \ldots, b_m$ the tuple $(a_1, \ldots, a_n, b_{n+1}, \ldots, b_m)$ is in the same generating equivalence class. Therefore, any two m-tuples of atoms, which are equal on the first n coordinates are equivalent. It follows that only those n coordinates matter and this equivalence relation can be defined using $2n$ variables with indices from the set $\{1, \ldots, n\}$. □

If the defining formula φ uses only $2n$ variables, then the m-set $\mathbb{A}^m/\varphi$ is isomorphic to $\mathbb{A}^n/\varphi$. This we call a *canonical representation*. We will now prove that it is unique up to permutation of coordinates and finally, give an algorithm that produces such representation.

Lemma 3.10. *If single-generated m-sets $\mathbb{A}^n/\varphi$ and $\mathbb{A}^n/\psi$, of dimension n, are isomorphic, then the formulas φ and ψ are equivalent, up to permutation of indices of the variables.*

Proof. Let $F\colon \mathbb{A}^n/\varphi \to \mathbb{A}^n/\psi$ be an isomorphism. The equivalence class of a non-repeating tuple $(a_1, \ldots, a_n)$ generates the set $\mathbb{A}^n/\varphi$. Its least support is the set $\{a_1, \ldots, a_n\}$. Consider an image of this equivalence class under the isomorphism F. It is supported by the same set and therefore

$$F([(a_1, \ldots, a_n)]_\varphi) = [(a_{\sigma(1)}, \ldots, a_{\sigma(n)})]_\psi,$$

where σ is some permutation of indices. Because F is m-equivariant, we have

$$\begin{aligned} F([(f(a_1), \ldots, f(a_n))]_\varphi) = F(f([(a_1, \ldots, a_n)]_\varphi)) = f(F([(a_1, \ldots, a_n)]_\varphi)) = \\ = f([(a_{\sigma(1)}, \ldots, a_{\sigma(n)})]_\psi) = [(f(a_{\sigma(1)}), \ldots, f(a_{\sigma(n)}))]_\psi. \end{aligned}$$

It follows that the n-tuples of atoms $(b_1, \ldots, b_n)$ and $(c_1, \ldots, c_n)$ are φ-equivalent if and only if the tuples $(b_{\sigma(1)}, \ldots, b_{\sigma(n)})$ and $(c_{\sigma(1)}, \ldots, c_{\sigma(n)})$ are ψ-equivalent. Hence, the two equivalence relations are the same, up to permutation σ. □

An algorithm for obtaining a canonical representation works as follows: given a set $\mathbb{A}^m/\psi$ it takes the formula ψ and produces an equivalent formula φ in $2n$ variables, where n is the least possible. By Lemma 3.9 the set $\mathbb{A}^n/\varphi$ is a canonical representation. We describe the algorithm in detail below. For the proof of its correctness we need an auxiliary lemma.

Lemma 3.11. *Let α, β, γ be types. Then $\alpha \Rightarrow \beta \vee \gamma$ if and only if $\alpha \Rightarrow \beta$ or $\alpha \Rightarrow \gamma$.*

Proof. Denote by A, B and C the single-generated segments of n-tuples defined by α, β and γ, respectively. The fact that $\alpha \Rightarrow \beta \vee \gamma$ means that $A \subseteq B \cup C$. Consider a tuple $(a_1, \ldots, a_n)$ that generates A. Without loss of generality we can assume that it belongs to B. Then $A \subseteq B$, which is equivalent to $\alpha \Rightarrow \beta$.

The other direction is straightforward. □

Proposition 3.12. *There is an algorithm, which inputs a single-generated m-set $\mathbb{A}^m/\psi$, and outputs its canonical representation.*

Proof. Any positive quantifier-free formula is effectively equivalent to a disjunction of types. Therefore, we can assume that ψ is of the form

$$\psi = \bigvee_{i=1}^{n} \alpha_i.$$

The first step of the algorithm is to replace all literals $x_i = x_i$ and $y_i = y_i$ by $\top$. Then, whenever $\alpha_i \Rightarrow \alpha_j$, the algorithm eliminates the type α_i from the formula. The formula φ that we obtain is clearly equivalent to ψ.

Suppose that there exists an equivalent formula ϕ in $2m$ variables, where $m < n$. Without loss of generality we can assume that ϕ is a disjunction of types and that there are no implications between those types. The formulas are of the form:

$$\varphi = \bigvee_{i \in I} \alpha_i, \qquad \phi = \bigvee_{j \in J} \beta_j.$$

Because $\varphi \Rightarrow \phi$, we have $\alpha_i \Rightarrow \phi$, for each $i \in I$. If $\alpha_i \Rightarrow \phi$ then, by Lemma 3.11, $\alpha_i \Rightarrow \beta_j$, for some $j \in J$. Summing up:

$$\text{for each } i \in I \text{ there exists } j \in J \text{ such that } \alpha_i \Rightarrow \beta_j.$$

At the same time:

$$\text{for each } j \in J \text{ there exists } i \in I \text{ such that } \beta_j \Rightarrow \alpha_i.$$

Since in both formulas there are no implications between types, this means that each type in φ has its equivalent counterpart in ϕ. Therefore, the formula ϕ can not use less variables. □

Example 3.13. Recall the m-set $\mathbb{A}^{(2)} \cup \{*\}$ defined in Example 2.4. Its second representation given in Example 3.8 is $\mathbb{A}^3/\psi$, where ψ is the formula:

$$(x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = x_3) \vee (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = y_3) \vee (x_1 = x_2 \wedge y_1 = y_2).$$

What does the algorithm do with the representation?

(1) It removes the literal $x_3 = x_3$ from the first type.
(2) Since $(x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = y_3) \Rightarrow (x_1 = y_1 \wedge x_2 = y_2)$, it eliminates the type $x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = y_3$ from the formula.

It outputs a formula

$$\varphi = (x_1 = y_1 \wedge x_2 = y_2) \vee (x_1 = x_2 \wedge y_1 = y_2),$$

which gives us a representation $\mathbb{A}^2/\varphi$. The m-set $\mathbb{A}^{(2)} \cup \{*\}$ has dimension 2, so this is indeed a canonical representation.

4. Representation of functions

In this section we give a representation of m-equivariant functions between single-generated m-sets. We assume that all sets under consideration have dimension at least one.

A function $f\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ will be denoted $f\colon m \to n$. Given such a function f and a formula ψ over variables $(x_1, \ldots, x_m, y_1, \ldots, y_m)$, let $f(\psi)$ be a formula obtained by a following substitution: $x_i \mapsto x_{f(i)}$, $y_i \mapsto y_{f(i)}$.

Proposition 4.1. *Let $\mathbb{A}^n/\varphi$ and $\mathbb{A}^m/\psi$ be single-generated m-sets. If a function $f\colon m \to n$ satisfies $\varphi \Rightarrow f(\psi)$, then a function $F\colon \mathbb{A}^n/\varphi \to \mathbb{A}^m/\psi$, defined by $F([(a_1,\dots,a_n)]_\varphi) = [(a_{f(1)},\dots,a_{f(m)})]_\psi$, is well defined and m-equivariant.*

Proof. We begin with showing that F is well defined. The n-tuples $(a_1,\dots,a_n)$ and $(b_1,\dots,b_n)$ are φ-equivalent if and only if the assignment $x_i \mapsto a_i$, $y_i \mapsto b_i$ satisfies φ. Since $\varphi \Rightarrow f(\psi)$, it follows that the assignment $x_i \mapsto a_{f(i)}$, $y_i \mapsto b_{f(i)}$ satisfies ψ. Hence, the m-tuples $(a_{f(1)},\dots,a_{f(m)})$ and $(b_{f(1)},\dots,b_{f(m)})$ are ψ-equivalent. It remains to show that F is m-equivariant. Consider an endomorphism g. Then:

$$F(g([(a_1,\dots,a_n)]_\varphi)) = F([(g(a_1),\dots,g(a_n))]_\varphi) = [(g(a_{f(1)}),\dots,g(a_{f(m)}))]_\psi =$$
$$= g([(a_{f(1)},\dots,a_{f(m)})]_\psi) = g(F([(a_1,\dots,a_n)]_\varphi)).$$

□

Proposition 4.2. *Let $\mathbb{A}^n/\varphi$ and $\mathbb{A}^m/\psi$ be single-generated m-sets. For every m-equivariant function $F\colon \mathbb{A}^n/\varphi \to \mathbb{A}^m/\psi$ there exists a function $f\colon m \to n$ such that $F([(a_1,\dots,a_n)]_\varphi) = [(a_{f(1)},\dots,a_{f(m)})]_\psi$.*

Proof. The equivalence class of a non-repeating tuple $(a_1,\dots,a_n)$ generates the set $\mathbb{A}^n/\varphi$. Its least support is the set $S = \{a_1,\dots,a_n\}$. Take an endomorphism g, which acts as the identity on S, and which has image equal to S. Consider any m-tuple $(b_1,\dots,b_m)$ that belongs to the equivalence class $F([(a_1,\dots,a_n)]_\varphi)$. Since S supports $F([(a_1,\dots,a_n)]_\varphi)$, we have that $g(b_1,\dots,b_m) \in F([(a_1,\dots,a_n)]_\varphi)$. It follows from the definition of g, that all atoms in the tuple $g(b_1,\dots,b_m)$ are from $\{a_1,\dots,a_n\}$. Let us define $f\colon m \to n$ as the unique function, such that $g(b_1,\dots,b_m) = (a_{f(1)},\dots,a_{f(m)})$.

So far we know that $F([(a_1,\dots,a_n)]_\varphi) = [(a_{f(1)},\dots,a_{f(m)})]_\psi$ for a fixed, non-repeating tuple $(a_1,\dots,a_n)$. Take any n-tuple $(a'_1,\dots,a'_n)$. There exist an endomorphism g, such that $(a'_1,\dots,a'_n) = (g(a_1),\dots,g(a_n))$. Since F is m-equivariant, we have that:

$$F([(a'_1,\dots,a'_n)]_\varphi) = F([(g(a_1),\dots,g(a_n))]_\varphi) = F(g([(a_1,\dots,a_n)]_\varphi)) =$$
$$= g(F([(a_1,\dots,a_n)]_\varphi)) = g([(a_{f(1)},\dots,a_{f(m)})]_\psi) = [(g(a_{f(1)}),\dots,g(a_{f(m)}))]_\psi =$$
$$= [(a'_{f(1)},\dots,a'_{f(m)})]_\psi.$$

Hence, f defines F, which also means that $\varphi \Rightarrow f(\psi)$. □

Example 4.3. Consider an m-equivariant function $F\colon \mathbb{A}^2 \to \mathbb{A}^{(2)} \cup \{*\}$, which acts as the identity on non-repeating pairs and maps all other pairs to $*$. Recall that $A^{(2)} \cup \{*\}$ is isomorphic to $\mathbb{A}^2/\psi$, where ψ is the formula

$$(x_1 = y_1 \wedge x_2 = y_2) \ \vee \ (x_1 = x_2 \wedge y_1 = y_2),$$

while $\mathbb{A}^2$ is the set of pairs quotiened by a formula $\varphi = (x_1 = y_1 \wedge x_2 = y_2)$. The function F is represented by $f\colon 2 \to 2$, which is the identity. Clearly $\varphi \Rightarrow f(\psi)$:

$$(x_1 = y_1 \wedge x_2 = y_2) \;\Rightarrow\; (x_1 = y_1 \wedge x_2 = y_2) \vee (x_1 = x_2 \wedge y_1 = y_2).$$

We have shown that m-equivariant functions $F\colon \mathbb{A}^n/\varphi \to \mathbb{A}^m/\psi$ correspond to functions $f\colon m \to n$, that satisfy $\varphi \Rightarrow f(\psi)$. Observe, however, that a single m-equivariant function $F\colon \mathbb{A}^n/\varphi \to \mathbb{A}^m/\psi$ might correspond to many different functions $f\colon m \to n$. For instance, an m-equivariant function $F\colon \mathbb{A}^2 \to \mathbb{A}^{(2)} \cup \{*\}$, that maps all tuples to $*$, is defined by both constant functions $f\colon 2 \to 2$. It follows, that the representation of m-equivariant functions is not unique. But, as we will show now, it is easy to decide if the represented functions are the same.

Given functions $f\colon m \to n$ and $g\colon m \to n$, and a formula ψ over variables $(x_1, \ldots, x_m, y_1, \ldots, y_m)$, we denote by $[f, g](\psi)$ the formula obtained by a following substitution: $x_i \mapsto x_{f(i)}$, $y_i \mapsto y_{g(i)}$. Suppose that f and g define m-equivariant functions $F\colon \mathbb{A}^n/\varphi \to \mathbb{A}^m/\psi$ and $G\colon \mathbb{A}^n/\varphi \to \mathbb{A}^m/\psi$, respectively. Notice that $F = G$ if and only if, whenever the n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are φ-equivalent, the m-tuples $(a_{f(1)}, \ldots, a_{f(m)})$ and $(b_{g(1)}, \ldots, b_{g(m)})$ are ψ-equivalent. Hence, we obtain the following:

Proposition 4.4. *A function $f\colon m \to n$ that satisfies $\varphi \Rightarrow f(\psi)$ and a function $g\colon m \to n$ that satisfies $\varphi \Rightarrow g(\psi)$ define the same m-equivariant function from $\mathbb{A}^n/\varphi$ to $\mathbb{A}^m/\psi$ if and only if $\varphi \;\Rightarrow\; [f, g](\psi)$.*

Example 4.5. Recall that the m-equivariant function $F\colon \mathbb{A}^2 \to \mathbb{A}^{(2)} \cup \{*\}$, which maps all tuples to $*$, is defined by a function $f\colon 2 \to 2$, which maps 1 and 2 to 1, and also by $g\colon 2 \to 2$, which maps 1 and 2 to 2. We apply $[f, g]$ to the formula $\psi = (x_1 = y_1 \wedge x_2 = y_2) \vee (x_1 = x_2 \wedge y_1 = y_2)$, that defines $\mathbb{A}^{(2)} \cup \{*\}$. The obtained formula $(x_1 = y_2 \wedge x_1 = y_2) \vee (x_1 = x_1 \wedge y_2 = y_2)$ is always satisfied. Hence, $\varphi \;\Rightarrow\; [f, g](\psi)$, where φ is the formula $x_1 = y_1 \wedge x_2 = y_2$, that defines $\mathbb{A}^2$.

5. M-sets generalize nominal sets

In this section we come back to atoms with additional structure. We show, that under some natural assumptions, the theory of m-sets generalizes the theory of nominal sets, studied in [1]. First let us briefly recall a few basic facts about nominal sets.

For any relational structure $\mathbb{A}$ a pair $(\mathbb{A}, \mathrm{Aut}(\mathbb{A}))$ is called an *atom symmetry*. We say that the atom symmetry *admits least supports* if every element of every nominal set has the least finite support (with respect to the action of automorphisms).

Fact 5.1. *Let X be a nominal set. If S is the least support of an element $x \in X$, then $\pi(S)$ is the least support of $\pi(x)$ for any automorphism π.*

In nominal sets functions commute with the automorphisms. A function F from a nominal set X to a nominal set Y is *equivariant* if $F(\pi(x)) = \pi(F(x))$, for any $x \in X$ and any automorphism π.

Fact 5.2. *Let $F\colon X \to Y$ be an equivariant function. If S supports an element x of the nominal set X, then it also supports an element $F(x)$ of the nominal set Y.*

From now on, we will only consider atoms that are *homogeneous* relational structures over finite vocabularies. Under those assumptions nominal sets are particularly well-behaved (see e.g. [1]).

Definition 5.3. A relational structure $\mathbb{A}$ is *homogeneous* if any isomorphism between finite substructures of $\mathbb{A}$ extends to an automorphism of $\mathbb{A}$.

Both equality and total order atoms are homogeneous and have a finite vocabulary. Moreover, they admit least supports with respect to the action of automorphisms (see e.g. [1]).

We will now show that, given atoms $\mathbb{A}$ one can define atoms $\tilde{\mathbb{A}}$, with a richer relational structure, such that the nominal sets in $\mathbb{A}$ are equivalent to the m-sets in $\tilde{\mathbb{A}}$. Suppose that the relational structure $\mathbb{A}$ has r relation symbols. Without loss of generality we can assume that one of the relations is the equality. For each k-ary relation R, let R' be its negation i.e. the relation R' consists of those k-tuples of atoms, which are not in the relation R. The newly obtained relational structure $\tilde{\mathbb{A}}$ has the same universe and $2r$ relation symbols in its signature.

Example 5.4. If $\mathbb{A} = (\mathbb{N}, =)$ then $\tilde{\mathbb{A}} = (\mathbb{N}, =, \neq)$. If $\mathbb{A} = (\mathbb{Q}, \leq)$ then $\tilde{\mathbb{A}} = (\mathbb{Q}, \leq, >)$.

Notice that the relational structure $\mathbb{A}$ and the corresponding relational structure $\tilde{\mathbb{A}}$ have the same automorphisms, which means that nominal sets over those atoms are the same. If the relational structure $\mathbb{A}$ is homogeneous, then so is $\tilde{\mathbb{A}}$.

Moreover, any endomorphism of the structure $\tilde{\mathbb{A}}$ is necessarily injective, as $\tilde{\mathbb{A}}$ contains the inequality relation that has to be preserved.

Proposition 5.5. *If the atom symmetry $(\mathbb{A}, \mathrm{Aut}(\mathbb{A}))$ admits least supports, the category of nominal sets and equivariant functions is isomorphic to the category of m-sets over atoms $\tilde{\mathbb{A}}$ with m-equivariant functions.*

Proof. Since the nominal sets over $\mathbb{A}$ and the nominal sets over $\tilde{\mathbb{A}}$ are the same, we fix a relational structure $\tilde{\mathbb{A}}$ for the atoms and prove that in those atoms the categories of nominal sets and m-sets are isomorphic.

Consider a nominal set X. We need to define an action of the endomorphism monoid on X. Take an endomorphism f and let S be the least support of some element $x \in X$ (with respect to the action of the automorphisms group). Since f is injective and the atoms are homogeneous, there exists an automorphism π such that $\pi|_S = f|_S$. Let $f(x) = \pi(x)$. It is not difficult to check that the action is well defined. Moreover, S is a finite support of x with respect to the action of the endomorphism monoid. Hence, X is an m-set.

Now, consider an equivariant function $F\colon X \to Y$. Take an element x of X and let S be the least support of x with respect to the action of $\mathrm{Aut}(\tilde{\mathbb{A}})$. Recall that S

supports $F(x)$ as well. Therefore, for any endomorphism f of atoms

$$F(f(x)) = F(\pi(x)) \quad \text{and} \quad f(F(x)) = \pi(F(x)),$$

where π is an automorphism, which satisfies $\pi|_S = f|_S$. Since $F(\pi(x)) = \pi(F(x))$, we have that $F(f(x)) = f(F(x))$.

The other direction is straightforward, since $\mathrm{Aut}(\tilde{\mathbb{A}}) \subseteq \mathrm{End}(\tilde{\mathbb{A}})$. □

References

[1] M. Bojańczyk, B. Klin, and S. Lasota, *Automata theory in nominal sets*, to appear.

[2] M. P. Fiore and D. Turi, *Semantics of Name and Value Passing*, Procs. LICS (93-104), 2011.

[3] M. Gabbay and A. M. Pitts, *A new approach to abstract syntax with variable binding*, Formal As. Comput., 13(3-5): pp. 341-363, 2002.

[4] A. M. Pitts, *Nominal Sets: Names and Symmetry in Computer Science*, Cambridge University Press, 2013.

[5] D. Sangiorgi and D. Walker, *The Pi-Calculus - a theory of mobile processes*, Cambridge University Press, 2001.

Institute of Mathematics of the Polish Academy of Sciences, Warsaw, Poland

E-mail address: joanna.ochremiak@gmail.com