FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Maryia Kapytka

The Number of Homomorphisms to a Fixed Algebra

Department of Algebra

Supervisor of the bachelor thesis: doc. Mgr. Libor Barto, Ph.D.
Study programme: Mathematics
Study branch: General Mathematics

Prague 2021

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In Prague, 25^{th} of May 2021 Maryia Kapytka

Title: The Number of Homomorphisms to a Fixed Algebra

Author: Maryia Kapytka

Department: Department of Algebra

Supervisor: doc. Mgr. Libor Barto, Ph.D., Department of Algebra

Abstract: In this work we give a partial answer to the following question: For which fixed finite algebras **A** is the number of homomorphisms from a similar algebra **X** to **A** bounded from above by a polynomial in the size of **X**? The work is divided into two parts: Preliminaries and Results. In the first part we introduce the reader to this topic and give some basic facts about the number of homomorphisms. In the main part we generalize the case of a two-element semilattice to a general finite semilattice, then we look at a specific three-element algebra with a majority operation and a specific three-element 2-semilattice, the rock-paper-scissors algebra. Then we study groups. Finally we consider unary algebras. All the algebras mentioned above apart from unary algebras give a positive answer to our question.

Keywords: universal algebra, homomorphism, semilattice, majority algebra, unary algebra

Contents

Introduction

The main question I study in my bachelor thesis is which finite algebras admit only polynomially many homomorphisms into them. More precisely, for which finite algebras $\mathbf{A}$ is there a polynomial p such that the number of homomorphisms from any algebra $\mathbf{X}$ (in the same signature as $\mathbf{A}$) is bounded from above by $p(|X|)$. It turns out that all such "polynomial" algebras on a two-element domain surprisingly come from some basic observations and from the fact that two-element semilattices, two-element majority algebras and two-element minority algebras admit polynomially many homomorphisms into them. This fact is studied and proven in the first version of the article Constraint Satisfaction Problems over Finite Structures [1].

In this work we will explore algebras beyond the two-element domain. We will generalize the case of a two-element semilattice to a general finite semilattice, then we will look at a specific three-element algebra with a majority operation and a specific three-element 2-semilattice, the rock-paper-scissors algebra. Then we will study groups.

All the algebras mentioned in the previous paragraph are examples of algebras with polynomially many homomorphisms. On the other hand, in the end of this work we will consider unary algebras and it will turn out that the number of homomorphisms into them is exponential.

The results presented in this work are original (with the help of my supervisor). Most of the results presented here have already been superseded in the second version of the paper Constraint Satisfaction Problems over Finite Structures [2], which uses a more advanced theory in Universal Algebra – the Tame Congruence Theory [3]. In a follow up work, which has not been published yet, the class of all "polynomial" algebras was fully characterized.

1. Preliminaries

1.1 Algebras and homomorphisms

We will start by defining some basic terms connected with this topic: an operation, an algebra and a homomorphism. At the end of this section we will look at terms and term operations, and we will also describe how homomorphisms affect them.

Most of the definitions in this chapter and further in this work are taken from Clifford Bergman's book Universal Algebra: Fundamentals and Selected Topics [4] and are standard in universal algebra.

Definition 1.1.1. Let A be a set and n a positive integer. We define A^n to be the set of all n-tuples of elements of A. We call a function $A^n \to A$ an *n-ary operation* on A. The natural number n is called the *arity* of the operation. Operations of arity 1 and 2 are usually called *unary* and *binary* operations, respectively.

A *signature* is a set of operation symbols Σ together with a mapping $\mathrm{ar} : \Sigma \to \mathbb{N}_0$ assigning to each operation symbol its *arity*. An *algebra in signature* Σ is a pair $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f\in\Sigma}\rangle$, where $f^{\mathbf{A}}$ is an operation on A of arity $\mathrm{ar}(f)$. The set A is called a *domain* of $\mathbf{A}$ and the $f^{\mathbf{A}}$ are called *basic operations* of $\mathbf{A}$.

From now on we will denote the domain of an algebra by the same letter as the algebra itself if not stated otherwise.

Definition 1.1.2. Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f\in\Sigma}\rangle$ be an algebra and B be a subset of A such that for each $n-$ary operation $f \in \Sigma$ and for all elements $b_1, \dots, b_n \in B$, $f^{\mathbf{A}}(b_1, \dots, b_n)$ is the element of B. Then the algebra $\mathbf{B} = \langle B, (f^{\mathbf{B}})_{f\in\Sigma}\rangle$, where each $f^{\mathbf{B}}$ is a restriction of $f^{\mathbf{A}}$, is called a *subalgebra of* $\mathbf{A}$.

Definition 1.1.3. Let $\mathbf{A} = \langle A, \wedge^{\mathbf{A}}\rangle$ be an algebra and A' be a subset of A. We say that A' is a *generating set of* $\mathbf{A}$ if $\mathbf{A}$ is the smallest subalgebra of $\mathbf{A}$ such that $A' \subset A$. In this case we also say that the algebra $\mathbf{A}$ is *generated by the set* A'.

When we have two algebras of the same signature we can define a mapping between them which preserves the operations of these algebras. We call such a mapping a homomorphism. Now we define this concept formally.

Definition 1.1.4. Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f\in\Sigma}\rangle$ and $\mathbf{B} = \langle B, (f^{\mathbf{B}})_{f\in\Sigma}\rangle$ be two algebras of the same signature Σ. A function $h : B \to A$ is called a *homomorphism from* $\mathbf{B}$ *to* $\mathbf{A}$ if for each $f \in \Sigma$ such that $\mathrm{ar}(f) = k$ and each $b_1, ..., b_k \in B$, $h(f^{\mathbf{B}}(b_1, ..., b_k)) = f^{\mathbf{A}}(h(b_1), ..., h(b_k))$. We write $h : \mathbf{B} \to \mathbf{A}$ to indicate that h is a homomorphism from $\mathbf{B}$ to $\mathbf{A}$.

If $h : \mathbf{B} \to \mathbf{A}$ and $g : \mathbf{C} \to \mathbf{B}$ are homomorphisms, then we will denote their composition by symbol $\circ$, i.e. $h \circ g : \mathbf{C} \to \mathbf{A}$ is the composition of homomorphisms g and h. Note that $h \circ g$ is also a homomorphism: if $f^{\mathbf{C}}$ is a n-ary operation on $\mathbf{C}$ and $c_1, ..., c_n \in C$, then

$$h \circ g(f^{\mathbf{C}}(c_1, ..., c_n)) = h \circ f^{\mathbf{B}}(g(c_1), ..., g(c_n)) = h(f^{\mathbf{B}}(g(c_1), ..., g(c_n))) =$$
$$= f^{\mathbf{A}}(h(g(c_1), ..., h(g(c_n)))) = f^{\mathbf{A}}(h \circ g(c_1), ..., h \circ g(c_n)))$$

In this calculation we used the facts that both h and g are homomorphisms.

Let us look at an important property of homomorphisms that we will use in the future, namely the fact that they preserve term operations on algebras. But at first we need to say what terms and term operations are.

Definition 1.1.5. Let V be a set of variable symbols and Σ be a signature. The *set of terms over the set of variables V over Σ* is recursively defined to be the smallest set with the following properties:

- every variable symbol is a term: $V \subset T$,
- if n is a natural number or zero, then from every n terms $t_1, ..., t_n$ and every n-ary operation symbol $f \in \Sigma$ a larger term $f(t_1, ..., t_n)$ can be built.

Now when we have defined terms we can define term operations.

Definition 1.1.6. Let $t \in T$ be a term over the set of variables $V = \{v_1, v_2, \ldots, v_k\}$ and signature Σ. Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f \in \Sigma} \rangle$ be an algebra. Then we define *term operation* $t^{\mathbf{A}} : A^k \to A$ in the natural way, i.e. $t^{\mathbf{A}}(a_1, \ldots, a_k)$ is obtained by replacing each variable x_i by a_i, replacing each operation symbol f by the corresponding operation $f^{\mathbf{A}}$ and evaluating the obtained expression.

For example, let $V = \{v_1, v_2, v_3\}$ be a set of variable symbols and Σ be a signature containing a binary operation symbol $f \in \Sigma$. Then $t(v_1, v_2, v_3) = f(f(v_1, v_3), v_2)$ is a term over the set V. If, additionally, $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f \in \Sigma} \rangle$ is an algebra in the signature Σ, then the corresponing term operation $t^{\mathbf{A}} : A^3 \to A$ is given by $t^{\mathbf{A}}(a_1, a_2, a_3) = f^{\mathbf{A}}(f^{\mathbf{A}}(a_1, a_3), a_2)$ for all $a_1, a_2, a_3 \in A$.

We are ready to prove a useful fact that homomorphisms preserve term operations.

Lemma 1.1.1. *Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f \in \Sigma} \rangle$ and $\mathbf{X} = \langle X, (f^{\mathbf{X}})_{f \in \Sigma} \rangle$ be two algebras of the same signature Σ, let h be a homomorphism from $\mathbf{X}$ to $\mathbf{A}$, and let t be a term in the signature Σ over $V = \{v_1, \ldots, v_k\}$. Then $h(t^{\mathbf{X}}(x_1, ..., x_k)) = t^{\mathbf{A}}(h(x_1), ..., h(x_k))$ for all $x_1, ..., x_k \in X$.*

Proof. We prove the claim by induction on the number n of operation symbols appearing in the term t.

If $n = 1$, then $t = f$ for some $f \in \Sigma$, so $h(t^{\mathbf{X}}(x_1, ..., x_k)) = h(f^X(x_1, ..., x_k)) = f^A(h(x_1), ..., h(x_k)) = t^{\mathbf{A}}(h(x_1), ..., h(x_k))$ according to Definition 1.1.4.

If $n \geq 2$, then $t = f(t_1, ..., t_l)$ for some terms $t_1, ..., t_l$, $l \in \mathbb{N}$ and for some $f \in \Sigma$. Then again, we can rewrite the image of $t^{\mathbf{X}}(x_1, ..., x_k)$ under h according to Definition 1.1.4.

$$h(t^{\mathbf{X}}(x_1, ..., x_k)) = h(f^X(t_1^{\mathbf{X}}(x_1, ..., x_k), ..., t_l^{\mathbf{X}}(x_1, ..., x_k))) =$$

$$= f^A(h(t_1^{\mathbf{X}}(x_1, ..., x_k)), ..., h(t_l^{\mathbf{X}}(x_1, ..., x_k))) =$$

$$= f^A(t_1^{\mathbf{A}}(h(x_1), ..., h(x_k)), ..., t_l^{\mathbf{A}}(h(x_1), ..., h(x_k)) = t^{\mathbf{A}}(h(x_1), ...h(x_k))$$

We have used the inductive assumption for the term operations $t_1^{\mathbf{X}}, ..., t_l^{\mathbf{X}}$.

□

1.2 Polynomially many homomorphisms

Now we will start describing "polynomial" algebras introduced in the beginning of this work. We will begin with the definition of a function $C_{\mathbf{A}}(n)$. If $\mathbf{A}$ is an algebra and n is a natural number, then this function will give us an upper estimate for the number of homomorphisms to $\mathbf{A}$ from all algebras with the cardinality of their domain at most n. Then using this function we will define what exactly a "polynomial" algebra means.

Definition 1.2.1. Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f\in\Sigma}\rangle$ be an algebra, n be a positive integer. Then we define function $C_{\mathbf{A}} : \mathbb{N} \to \mathbb{N}$ by

$$C_{\mathbf{A}}(n) = \max\{|\{f : \mathbf{X} \to \mathbf{A}; f \text{ is a homomomorphism}\}|; \mathbf{X} = \langle X, (f^{\mathbf{X}})_{f\in\Sigma}\rangle, |X| \leq n\},$$

where $|.|$ stands for the cardinality of the set.

So $C_{\mathbf{A}}(n)$ is the maximal number of homomorphisms from algebras of the same signature as $\mathbf{A}$ and with domain of cardinality at most n to the algebra $\mathbf{A}$. And we are looking for algebras $\mathbf{A}$ such that the function $C_{\mathbf{A}}(n)$ is a polynomial of n.

Definition 1.2.2. We say that $\mathbf{A}$ *admits polynomially many homomorphisms* if there exists a polynomial p such that, for all positive integers n, $C_{\mathbf{A}}(n) \leq p(n)$.

Remark 1.2.1. *Equivalently we can define that* $\mathbf{A}$ *admits polynomially many homomorphisms if there exist a real number* $c > 0$ *and a positive integer* k *such that, for all positive integers* n, $C_{\mathbf{A}}(n) \leq cn^k$. *This definition is indeed equivalent: if there exists a polynomial* p *such that for all positive integers* n: $C_{\mathbf{A}}(n) \leq p(n)$, *then there always exists an integer* k *such that* $p(n) \leq cn^k$: *we can the degree of* p *as* k *and the sum of the absolute values of all coefficients as* c. *For example, if* $p(n) = 5n^3 - 2n^2 + 1$ *then we can take a polynomial* $5n^3 + 2n^3 + n^3 = 6n^3$. *Clearly* $p(n) \leq 6n^3$, *so* $c = 6$ *and* $k = 3$ *in this case.*

Remark 1.2.2. *In order to prove that* $\mathbf{A}$ *admits polynomially many homomorphisms it is enough to show that* $C_{\mathbf{A}}(n) \leq cn^k$ *for* $n \geq M$ *for some constant* M. *If we have shown this, then we can multiply* cn^k *by some large constant* d *such that* $C_{\mathbf{A}}(n) \leq dcn^k$ *is true also for* $n < M$. *Then clearly* $C_{\mathbf{A}}(n) \leq dcn^k$ *is true for all positive integers* n.

We have described "polynomial" algebras. But we will also study algebras which are somehow opposite to polynomial. That is to say, the number of homomorphisms to them is exponential. We need to define these algebras as well.

Definition 1.2.3. We say that $\mathbf{A}$ *admits exponentially many homomorphisms* if there exist real numbers c, d such that $c > 0$, $d > 1$ and for all positive integers n: $C_{\mathbf{A}}(n) \geq cd^n$.

Remark 1.2.3. *In order to prove that* $\mathbf{A}$ *admits exponentially many homomorphisms it is enough to show that* $C_{\mathbf{A}}(n) \geq cd^n$ *for* $n \geq M$ *for some constant* M. *If we have shown this, then we can multiply* cd^n *by some small positive constant* e *such that the inequality* $C_{\mathbf{A}}(n) \geq ecd^n$ *is true also for* $n < M$. *Then clearly* $C_{\mathbf{A}}(n) \geq ecd^n$ *is true for all positive integers* n.

1.3 Basic facts

We will start with the discussion of two basic facts about the number of homomorphisms. They have already been proven in [2]. The first one is the fact that the operations on algebra somehow "connect" its elements, so when we "throw away" some operations, the number of homomorphisms naturally increases. We will formalize this observation using the term reduct of an algebra.

Definition 1.3.1. We say that an algebra $\mathbf{B}$ is *reduct* of $\mathbf{A}$ if they have the same domain and each basic operation of $\mathbf{B}$ is a term operation of $\mathbf{A}$.

Now we will show that the number of homomorphisms to the reduct of an algebra is greater than or equal to the number of homomorphisms to the original algebra.

Lemma 1.3.1. *Let* $\mathbf{A}$ *be an algebra and* $\mathbf{B}$ *be its reduct. Then* $C_{\mathbf{A}}(n) \leq C_{\mathbf{B}}(n)$*.*

Proof. Let n be a natural number and $\mathbf{X}$ be an algebra such that the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is $C_A(n)$ and $|X| \leq n$.

Now we define an algebra $\mathbf{X'} = \langle X, (f^{\mathbf{X'}})_{f\in\Sigma}\rangle$ (where Σ is the signature of $\mathbf{B}$) as follows. Since $\mathbf{B}$ is a reduct of $\mathbf{A}$, there exists a term t (in the signature of $\mathbf{A}$) such that $f^{\mathbf{B}} = t^{\mathbf{A}}$. We define $f^{\mathbf{X'}} = t^{\mathbf{X}}$.

Let h be a homomorphism from $\mathbf{X}$ to $\mathbf{A}$. We will show that h is also a homomorphism from $\mathbf{X'}$ to $\mathbf{B}$. Take an arbitrary $l-$ary operation symbol $f \in \Sigma$, take t as above, and take $x_1, \dots, x_l \in X$. As h is the homomorphism, then according to Lemma 1.1.1 it also preserves term operations. Using these facts we obtain the following calculation.

$$h(f^{\mathbf{X'}}(x_1, \dots, x_l)) = h(t^{\mathbf{X}}(x_1, \dots, x_l)) \overset{Lemma\ 1.1.1}{=} t^{\mathbf{A}}(h(x_1), \dots, h(x_l)) =$$
$$= f^{\mathbf{B}}(h(x_1), \dots, h(x_l))$$

So h is indeed the homomorphism from $\mathbf{X'}$ to $\mathbf{B}$. We have shown that each homomorphism from $\mathbf{X}$ to $\mathbf{A}$ is a homomorphism from $\mathbf{X'}$ to $\mathbf{B}$. Therefore $C_{\mathbf{A}}(n) \leq C_{\mathbf{B}}(n)$. □

Now we will look at the second fact about the number of homomorphisms. It turns out that if there's a homomorphism from $\mathbf{X}$ to $\mathbf{A}$, where $\mathbf{X}$ is a general algebra and $\mathbf{A}$ is an algebra satisfying some special identities, for example a group or a semilattice, then without the loss of generality we can assume $\mathbf{X}$ satisfies the same identities as $\mathbf{A}$. But at first we will define the term identity and some other terms which we will use in our proof.

Definition 1.3.2. Let Σ be a signature and $V = \{v_1, \dots, v_k\}$ be a set of variables. An *identity* is an ordered pair of terms over the set V and signature Σ, written $p \approx q$. If $\mathbf{A}$ is an algebra of signature Σ we say that $\mathbf{A}$ *satisfies* $p \approx q$ if $p^{\mathbf{A}} = q^{\mathbf{A}}$.

Definition 1.3.3. Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f\in\Sigma}\rangle$ and θ be an equivalence relation on the set A. We say that θ is a *congruence relation* if for each $f^{\mathbf{A}}$, $f \in \Sigma$ of arity $n \in \mathbb{N}$ and for each $a_1, ..., a_n, b_1, ..., b_n \in A$ the following implication is true:

$$\text{whenever } a_1\theta b_1, ..., a_n\theta b_n, \text{ then } f^{\mathbf{A}}(a_1, ..., a_n)\theta f^{\mathbf{A}}(b_1, ..., b_n)$$

Definition 1.3.4. Let θ be an equivalence relation on the set A. For $a \in A$ we write

$$a/\theta = \{x \in A : a\theta x\},$$

the *equivalence class of a modulo* θ. The set of equivalence classes modulo θ is denoted A/θ and is called the *quotient of* A *by* θ.

Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f\in\Sigma}\rangle$ be an algebra and θ a congruence relation on $\mathbf{A}$. The quotient algebra $\mathbf{A}/\theta$ is the algebra $\mathbf{A}/\theta = \langle A/\theta, (f^{\mathbf{A}/\theta})_{f\in\Sigma}\rangle$ with basic operations defined by equation:

$$f^{\mathbf{A}/\theta}(a_1/\theta, ..., a_n/\theta) = f^{\mathbf{A}}(a_1, ..., a_n)/\theta$$

The basic operations on the quotient algebra are well-defined: if $a_i/\theta = b_i/\theta$ for all $i \leq n$, then $a_i\theta b_i$ for all $i \leq n$. According to the definition of a congruence relation this implies that $f^{\mathbf{A}}(a_1, ..., a_n)\theta f^{\mathbf{A}}(b_1, ..., b_n)$, therefore $f^{\mathbf{A}}(a_1, ..., a_n)/\theta = f^{\mathbf{A}}(b_1, ..., b_n)/\theta$.

Definition 1.3.5. Let $f : A \to B$ be any function. We define

$$Kerf = \{ \ (x, y) \in A \times A \mid f(x) = f(y) \ \}$$

called the *kernel of f.*

The kernel of a homomomorphism is an equivalence relation due to the reflexivity, transitivity and antisymmetry of the relation $=$. Moreover, the kernel of a homomomorphism is a congruence relation. Take algebras $\mathbf{X}$, $\mathbf{A}$ and let $h : \mathbf{X} \to \mathbf{A}$ be a homomorphism. Assume that $(x_1, y_1), ..., (x_n, y_n) \in Kerh$. This means that $h(x_i) = h(y_i)$ for $i \leq n$, then $h(f^{\mathbf{A}}(x_1, ..., x_n)) = f^{\mathbf{A}}(h(x_1), ..., h(x_n)) = f^{\mathbf{A}}(h(y_1), ..., h(y_n)) = h(f^{\mathbf{A}}(y_1, ..., y_n))$ according to Definition 1.1.4 of a homomorphism. This exactly means that $(f^{\mathbf{A}}(x_1, ..., x_n), f^{\mathbf{A}}(y_1, ..., y_n) \in Kerh$, therefore $Kerh$ is indeed a congruence relation.

Theorem 1.3.2. *(The Fundamental Homomorphism Theorem)*
Let $\mathbf{A}$ and $\mathbf{B}$ be two algebras of the same signature Σ, θ be a congruence on $\mathbf{A}$ and let $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism such that $\theta \subset Kerh$. Let π be a natural homomorphism $\pi : \mathbf{A} \to \mathbf{A}/\theta$, i.e. the homomorphism such that $\pi(a) = a/\theta$ for all $a \in A$. Then there is a unique homomorphism $g : \mathbf{A}/\theta \to \mathbf{B}$ such that $g \circ \pi = h$.

Finally we are ready to prove the fact which we will often use later in our proofs: if $\mathbf{A}$ is an algebra satisfying some special identies and $\mathbf{X}$ is some general algebra, then there exists an algebra $\mathbf{Y}$ satisfying the same identities as $\mathbf{A}$ with the same number of homomorphisms to $\mathbf{A}$ as $\mathbf{X}$.

Lemma 1.3.3. *Let $\mathbf{A} = \langle A, (f^{\mathbf{A}})_{f \in \Sigma} \rangle$ and $\mathbf{X} = \langle X, (f^{\mathbf{X}})_{f \in \Sigma} \rangle$ be two algebras of the same signature Σ. Let S be a finite set of identities satisfied in $\mathbf{A}$. Then there exists an algebra $\mathbf{Y}$ such that:*

- $|Y| \leq |X|$
- *the number of homomorphisms from $\mathbf{Y}$ to $\mathbf{A}$ is equal to the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$*
- *each identity in S is satisfied in $\mathbf{Y}$*

Proof. At first we notice that if each identity in S is satisfied in $\mathbf{X}$, then we can take an algebra $\mathbf{X}$ as the algebra $\mathbf{Y}$. It satisfies all the conditions and the proof is complete.

Now assume that there are identities in S which are not satisfied in $\mathbf{X}$ and let $p \approx q$ be such an identity in S. If $k \in \mathbb{N}$ is the arity of $p^{\mathbf{X}}$ and $q^{\mathbf{X}}$, then there are elements $x_1, ..., x_k \in X$ such that $p^{\mathbf{X}}(x_1, ..., x_k) \neq q^{\mathbf{X}}(x_1, ..., x_k)$. Now let θ be the smallest congruence containining all elements $(p^{\mathbf{X}}(x_1, ..., x_k), q^{\mathbf{X}}(x_1, ..., x_k))$ for all $x_1, ..., x_k \in X$ such that $p^{\mathbf{X}}(x_1, ..., x_k) \neq q^{\mathbf{X}}(x_1, ..., x_k)$. The smallest congruence always exists, it is an intersection of all congruences which contain $(p^{\mathbf{X}}(x_1, ..., x_k), q^{\mathbf{X}}(x_1, ..., x_k))$. It can be written formally as follows.

$$\theta = \cap\varphi, \varphi \text{ is a congrunce such that } p^{\mathbf{X}}(x_1, ..., x_k)\varphi q^{\mathbf{X}}(x_1, ..., x_k)$$
$$\text{for all } x_1, ..., x_k \in X \text{ such that } p^{\mathbf{X}}(x_1, ..., x_k) \neq q^{\mathbf{X}}(x_1, ..., x_k)$$

Take $\mathbf{Y}_1 = \mathbf{X}/\theta$ and note that $|Y_1| < |X|$.

Now let h be a homomorphism from $\mathbf{Y}_1$ to $\mathbf{A}$. Consider a natural homomorphism $\pi : \mathbf{X} \to \mathbf{Y}_1$, i.e. the homomorphism such that $\pi(x) = x/\theta$. Then the composition $h \circ \pi$ is a homomorphism from $\mathbf{X}$ to $\mathbf{A}$.

On the other hand, let f be a homomorphism from $\mathbf{X}$ to $\mathbf{A}$. Consider two arbitrary elements $p^{\mathbf{X}}(x_1, ..., x_k)$ and $q^{\mathbf{X}}(x_1, ..., x_k)$, where $x_1, ..., x_k \in X$, such that $p^{\mathbf{X}}(x_1, ..., x_k)\theta q^{\mathbf{X}}(x_1, ..., x_k)$. Now look at their images under f:

$$f(p^{\mathbf{X}}(x_1, ..., x_k)) = p^{\mathbf{A}}(f(x_1), ..., f(x_k))$$

and

$$f(q^{\mathbf{X}}(x_1, ..., x_k)) = q^{\mathbf{A}}(f(x_1), ..., f(x_k))$$

by Definition 1.1.4 of a homomorphism. But $p \approx q$ is an identity in S, so it is satisfied in $\mathbf{A}$. This implies that

$$p^{\mathbf{A}}(f(x_1), ..., f(x_k)) = q^{\mathbf{A}}(f(x_1), ..., f(x_k)) \text{ as } f(x_1), ..., f(x_k) \in A.$$

Therefore we have shown that

$$f(p^{\mathbf{X}}(x_1, ..., x_k)) = f(q^{\mathbf{X}}(x_1, ..., x_k)) \text{ for each } (p^{\mathbf{X}}(x_1, ..., x_k), q^{\mathbf{X}}(x_1, ..., x_k)) \in \theta.$$

Therefore all the pairs $(p^{\mathbf{X}}(x_1, ..., x_k), q^{\mathbf{X}}(x_1, ..., x_k))$ are in $Kerf$ and, since θ is the smallest congruence of $\mathbf{X}$ containing these pairs and $Kerf$ is a congruence of $\mathbf{X}$, we get that $\theta \subseteq Kerf$. Then according to Theorem 1.3.2 (The Fundamental Homomorphism Theorem) there exists a unique homomorphism $g : \mathbf{X}/\theta \to \mathbf{A}$ such that $f = g \circ \pi$, where π is the homomorphism such that $\pi(x) = x/\theta$ for all $x \in X$. Therefore for each homomorphism f from $\mathbf{X}$ to $\mathbf{A}$ there exists a unique homomorphism $g : \mathbf{Y}_1 \to \mathbf{A}$ such that $f = g \circ \pi$.

In the last two paragraphs we have shown that $g \mapsto g \circ \pi$ is a bijection between the set of homomorphisms from $\mathbf{Y}_1$ to $\mathbf{A}$ and the set of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$.

Now we iterate this process on all the identities in S. More precisely, denote $S = \{p_1 \approx q_1, ..., p_t \approx q_t\}$ for some $t \in \mathbb{N}$ and let θ_i be the smallest congruence containing all the elements $(p_i^{\mathbf{Y}_{i-1}}(y_1, ..., y_s), q_i^{\mathbf{Y}_{i-1}}(y_1, ..., y_s))$ for all $y_1, ..., y_s \in Y_{i-1}$ such that $p_i^{\mathbf{Y}_{i-1}}(y_1, ..., y_s) \neq q_i^{\mathbf{Y}_{i-1}}(y_1, ..., y_s)$. Then in each step we take $\mathbf{Y}_i = \mathbf{Y}_{i-1}/\theta_i$. Note that $\mathbf{Y}_i$ automatically satisfies all the "previous" identities $p_1 \approx q_1, \dots, p_{i-1} \approx q_{i-1}$.

The algebra $\mathbf{Y}_t$ is the algebra $\mathbf{Y}$ we are looking for. □

1.4 Two-element classification

In this section we discuss one of the main result of [1] that essentially classifies two-element algebras admitting polynomially many homomorphisms. We start by introducing terminology for some types of operations.

Definition 1.4.1. An n-ary operation $f : A^n \to A$ is *essentially unary* if there exists $g : A \to A$ and $i \in \{1, ..., n\}$ such that for all $a \in A^n$, the equality $f(a_1, ..., a_n) = g(a_i)$ holds. We say than an algebra is *essentially unary* if each operation in its signature is essentially unary.

Definition 1.4.2. A *semilattice* is an algebra $\langle S, \wedge \rangle$ with a binary *semilattice operation* $\wedge$ (pronounced "meet") satisfying the following identities.

$(a_\wedge)$	$x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$	(associativity)
$(i_\wedge)$	$x \wedge x \approx x$	(idempotency)
$(c_\wedge)$	$x \wedge y \approx y \wedge x$	(commutativity)

Note that there are exactly two semilattices on the domain $S = \{0, 1\}$, the meet can be the (binary) minimum or maximum on S.

Definition 1.4.3. A *majority algebra* is an algebra $\langle A, M \rangle$ with a ternary *majority operation* $M : A^3 \to A$ satisfying the identities

$$M(x, x, y) \approx M(x, y, x) \approx M(y, x, x) \approx x.$$

A *minority algebra* is an algebra $\langle A, m \rangle$ with a ternary *minority operation* $m : A^3 \to A$ satisfying the identities

$$m(x, x, y) \approx m(x, y, x) \approx m(y, x, x) \approx y.$$

Note that there is a unique majority algebra on the domain $A = \{0, 1\}$, the majority operation maps (x, y, z) to the value that appears at least twice among x, y, z. Similarly, there is a unique minority algebra on $\{0, 1\}$, the minority operation is equal to $(x, y, z) \mapsto x + y + z$, where addition is modulo 2.

Surprisingly, all two-element algebras which are not essentially unary contain at least one of these operations (semilattice, majority, minority) as a term operation. This follows from a full classification of two-element algebras up to term equivalence [5].

Theorem 1.4.1. *Let* $\mathbf{A} = \langle \{0, 1\}, (f^{\mathbf{A}})_{f \in \Sigma} \rangle$ *be an algebra. If* $\mathbf{A}$ *contains an operation that is not essentially unary, then* $\mathbf{A}$ *has a term operation that is a semilattice operation, a majority operation, or a minority operation.*

In [1] it is proven that a two-element semilattice, the two-element majority algebra, and the two-element minority algebra all admit polynomially many homomorphisms. We will explore generalizations and similar algebras in Sections 2.1 – 2.4. If, on the other hand, $\mathbf{A}$ contains only essentially unary operations, we show in Subsection 2.5 that $\mathbf{A}$ admits exponentially many homomorphisms (this hasn't appeared in [1] in this form, a more general result appears in [2]). Theorem 1.4.1 together with Lemma 1.3.1 thus gives us the following dichotomy for a two-element $\mathbf{A}$: either $\mathbf{A}$ is essentially unary and then it admits exponentially many homomorphisms, or it is not essentially unary and then it admits polynomially many homomorphisms.

2. Results

2.1 Semilattices

In this section we generalize the result that two-element semilattices admit polynomially many homomorphisms [1] to arbitary finite semilattices.

At first we recall a well-known fact (see e.g. [4]) that a semilattice operation on a set S induces a partial ordering on S by setting

$$x \leq y \quad \text{if and only if} \quad x \wedge y = x. \tag{2.1}$$

It can be easily checked that this relation is reflexive, transitive and antisymmetric, so it defines a partial ordering on the set S.

It is also easily seen that $s_1 \wedge \cdots \wedge s_m$ is the infimum of $\{s_1, \ldots, s_m\}$ with respect to $\leq$. In particular, if S is finite, say, $S = \{s_1, ..., s_m\}$, then S has the least element with respect to $\leq$ and it is equal to $\min S = s_1 \wedge s_2 \wedge ... \wedge s_m$.

For a semilattice $\mathbf{S} = \langle S, \wedge^{\mathbf{S}} \rangle$ we denote the induced partial ordering by $\leq^{\mathbf{S}}$.

Let us consider finite semilattices $\mathbf{X} = \langle X, \wedge^{\mathbf{X}} \rangle$ and $\mathbf{S} = \langle S, \wedge^{\mathbf{S}} \rangle$. Let $f : \mathbf{X} \to \mathbf{S}$ be a homomorphism. In the following statements we will prove that preimages of elements of $\mathbf{S}$ under f contain the least element (with respect to $\leq^{\mathbf{X}}$) and we will show that f is "defined" by these least elements (this will be made precise in Theorem 2.1.2).

Lemma 2.1.1. *Let $\mathbf{X} = \langle X, \wedge^{\mathbf{X}} \rangle$, $\mathbf{S} = \langle S, \wedge^{\mathbf{S}} \rangle$ be finite semilattices. Let $f : \mathbf{X} \to \mathbf{S}$ be a homomorphism. Then each set $f^{-1}(a)$ for $a \in f(X)$ has the least element.*

Proof. Let us take an arbitrary element $a \in S$. At first let us observe that the set $f^{-1}(a)$ is not empty, because $a \in f(X)$. Let $x_1, ..., x_m$ be the elements of $f^{-1}(a)$. Now we define an element x as $x = x_1 \wedge^{\mathbf{X}} ... \wedge^{\mathbf{X}} x_m$. According to Definition 1.1.4 of a homomorphism $f(x) = f(x_1 \wedge^{\mathbf{X}} ... \wedge^{\mathbf{X}} x_m) = f(x_1) \wedge^{\mathbf{S}} .... \wedge^{\mathbf{S}} f(x_m) = a \wedge^{\mathbf{S}} ... \wedge^{\mathbf{S}} a = a$, so x is the element of $f^{-1}(a)$. Since $x \leq^{\mathbf{S}} x_i$ for every i and $x \in f^{-1}(a)$, then x is the least element of $f^{-1}(a)$, as required. □

Now what does it exactly mean that the homomorphism is "defined" by the least element in each class? We will say that in the statement of the following theorem and then we will prove it.

Theorem 2.1.2. *Let $\mathbf{X} = \langle X, \wedge^{\mathbf{X}} \rangle$, $\mathbf{S} = \langle S, \wedge^{\mathbf{S}} \rangle$ be finite semilattices. Let $f, g : \mathbf{X} \to \mathbf{S}$ be two homomorphisms from $\mathbf{X}$ to $\mathbf{S}$ such that $f(X) = g(X)$. Then the following implication is true:*

$$\textit{If } \forall y \in f(X) : \min f^{-1}(y) = \min g^{-1}(y), \textit{ then } f = g.$$

Proof. We assume that homomorphisms $f, g : \mathbf{X} \to \mathbf{S}$ are such that $\min f^{-1}(y) = \min g^{-1}(y)$ for all $y \in f(X)$.

We want to prove that for all $x \in X$: $f(x) = y_1$, $g(x) = y_2$ implies that $y_1 = y_2$. We can rewrite $f(x) = y_1$ and $g(x) = y_2$ as $x \in f^{-1}(y_1)$, $x \in g^{-1}(y_2)$ respectively. Both $f^{-1}(y_1)$ and $g^{-1}(y_2)$ have the least element as we have shown in Lemma 2.1.1. We denote these elements by z_1 and z_2 respectively, i.e., $z_1 = \min f^{-1}(y_1), z_2 = \min g^{-1}(y_2)$. Due to our assumption $z_1 = \min f^{-1}(y_1) = \min g^{-1}(y_1)$, so $g(z_1) = y_1$. Similarly $z_2 = \min g^{-1}(y_2) = \min f^{-1}(y_2)$, so $f(z_2) = y_2$.

The element z_1 is the least element in $f^{-1}(y_1)$, so $z_1 \leq^{\mathbf{X}} x$ and according to (2.1) $z_1 \wedge^{\mathbf{X}} x = z_1$. Because g is a homomorphism, it preserves the operation $\wedge$, this means that $g(z_1 \wedge^{\mathbf{X}} x) = g(z_1) \wedge^{\mathbf{S}} g(x) = y_1 \wedge^{\mathbf{S}} y_2$. At the same time $g(z_1 \wedge^{\mathbf{X}} x) = g(z_1) = y_1$. Therefore we have shown that $y_1 \wedge^{\mathbf{S}} y_2 = y_1$, or equivalently $y_1 \leq^{\mathbf{S}} y_2$.

We can use a similar argument as in the previous paragraph for z_2: $f(z_2 \wedge^{\mathbf{X}} x) = f(z_2) \wedge^{\mathbf{S}} f(x) = y_2 \wedge^{\mathbf{S}} y_1$ and at the same time $f(z_2 \wedge^{\mathbf{X}} x) = f(z_2) = y_2$. Therefore $y_2 \wedge^{\mathbf{S}} y_1 = y_2$, i.e. $y_2 \leq^{\mathbf{S}} y_1$. Finally the inequalities $y_1 \leq^{\mathbf{S}} y_2$ and $y_2 \leq^{\mathbf{S}} y_1$ imply that $y_1 = y_2$, and the proof is concluded. □

Corollary 2.1.3. *Every finite semilattice* $\mathbf{S}$ *admits polynomially many homomorphisms.*

Proof. Let $\mathbf{X}$ be an algebra of the same signature as $\mathbf{S}$. We have proven in Lemma 1.3.3 that there exists an algebra $\mathbf{Y}$ such that $|Y| \leq |X|$, the numbers of homomorphisms from $\mathbf{Y}$ to $\mathbf{S}$ and from $\mathbf{X}$ to $\mathbf{S}$ are equal and each identity for semilattice operation on $\mathbf{S}$ is satisfied in $\mathbf{Y}$. Therefore without the loss of generality we can assume that $\mathbf{Y} = \mathbf{X}$ is a semilattice.

As we have shown in Theorem 2.1.2, the homomorphism is "defined" by the least elements in the preimages of the elements in the set S. So the choice and the order of these elements uniquely determine the whole homomorphism. The number of these elements is the same as the cardinality of $f(X)$ and can range from one (if $f(X)$ contains just one element) to $|S|$. Of course not all of these possibilities may happen, but a rough estimate is enough for us. If we denote the cardinality of $f(X)$ by k, then there are $\binom{|X|}{k}$ ways to choose the set of the least elements and also $k!$ ways to order them.

Let us denote the cardinality of X by n, the cardinality of S by m, then the number of homomorphisms is not greater than $\binom{n}{1} + \binom{n}{2} \cdot 2! + \binom{n}{3} \cdot 3! + \ldots + \binom{n}{m-1} \cdot (m-1)! + \binom{n}{m} \cdot m! = n + n \cdot (n-1) + \ldots + n \cdot (n-1) \cdot \ldots \cdot (n-m+2) + n \cdot (n-1) \cdot \ldots \cdot (n-m+1)$, which is a polynomial of degree m. □

2.2 Majority algebras

The argument in [1] to show that the two-element majority algebra admits polynomially many homomorphisms applies the corresponding result for two-element semilattices. Corollary 2.1.3 enables us to extend the result and prove that some other majority algebras admit polynomially many homomorphisms. We illustrate the technique on a specific 3-element majority algebra.

Theorem 2.2.1. *Let* $\mathbf{A} = \langle \{0, 1, 2\}, M^{\mathbf{A}} \rangle$ *be the three-element majority algebra such that* $M^{\mathbf{A}}(x, y, z) = x$ *whenever* x, y, *and* z *are pairwise different. Then* $\mathbf{A}$ *admits polynomially many homomorphisms.*

Proof. Let $\mathbf{X}$ be an algebra in the same signature as $\mathbf{A}$. Similarly as in the proof of Corollary 2.1.3, we can assume that $\mathbf{X}$ is a majority algebra by applying Lemma 1.3.3.

Fix an arbitrary element p in $\mathbf{A}$. We will find a polynomial upper bound $q(|X|)$ for the number of homomorphisms $f : \mathbf{X} \to \mathbf{A}$ such that $f(p) = 0$. Since the structure of $\mathbf{A}$ is symmetric with respect to its elements, the same upper bound will hold for the number of homomorphisms f with $f(p) = 1$ and $f(p) = 2$. The total number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ will thus be upper bounded by $3q(|X|)$, which is still a polynomial.

Let us consider a binary operation $\wedge^{\mathbf{A}}$ on A defined by $a \wedge^{\mathbf{A}} b = M^{\mathbf{X}}(0, a, b)$ for $a, b \in A$ and a binary operation $\wedge^{\mathbf{X}}$ on X defined by $x \wedge^{\mathbf{X}} y = M^{\mathbf{X}}(p, x, y)$ for $x, y \in X$.

We now show that $\mathbf{A}' = \langle A, \wedge^{\mathbf{A}} \rangle$ is a semilattice.

- Idempotency:
$$a \wedge^{\mathbf{A}} a = M^{\mathbf{A}}(0, a, a) = a.$$
- Commutativity:
$$a \wedge^{\mathbf{A}} b = M^{\mathbf{A}}(0, a, b) = 0 \text{ if } a \neq b$$
and
$$a \wedge^{\mathbf{A}} b = M^{\mathbf{A}}(0, a, b) = a \text{ if } a = b.$$
Similarly,
$$b \wedge^{\mathbf{A}} a = M^{\mathbf{A}}(0, b, a) = 0 \text{ if } a \neq b$$
and
$$b \wedge^{\mathbf{A}} a = M^{\mathbf{A}}(0, b, a) = a \text{ if } a = b.$$
Therefore $a \wedge^{\mathbf{A}} b = b \wedge^{\mathbf{A}} a$.
- Associativity:
$$(a \wedge^{\mathbf{A}} b) \wedge^{\mathbf{A}} c = M^{\mathbf{A}}(0, M^{\mathbf{A}}(0, a, b), c)$$
and
$$a \wedge^{\mathbf{A}} (b \wedge^{\mathbf{A}} c) = M^{\mathbf{A}}(0, a, M^{\mathbf{A}}(0, b, c).$$
There are several possibilities:
  1. If $a = b = c$, then because of the idempotency
  $$(a \wedge^{\mathbf{A}} a) \wedge^{\mathbf{A}} a = a \wedge^{\mathbf{A}} a = a,$$
  similarly
  $$a \wedge^{\mathbf{A}} (a \wedge^{\mathbf{A}} a) = a \wedge^{\mathbf{A}} a = a.$$
  2. If $a = b \neq c$, then
  $$(a \wedge^{\mathbf{A}} b) \wedge^{\mathbf{A}} c = a \wedge^{\mathbf{A}} c = 0,$$
  $$a \wedge^{\mathbf{A}} (b \wedge^{\mathbf{A}} c) = M^{\mathbf{A}}(0, a, M^{\mathbf{A}}(0, b, c)) = M^{\mathbf{A}}(0, a, 0) = 0.$$
  3. If $a = c \neq b$, then
  $$(a \wedge^{\mathbf{A}} b) \wedge^{\mathbf{A}} c = M^{\mathbf{A}}(0, M^{\mathbf{A}}(0, a, b), a) = M^{\mathbf{A}}(0, 0, a) = 0,$$
  $$a \wedge^{\mathbf{A}} (b \wedge^{\mathbf{A}} c) = M^{\mathbf{A}}(0, a, M^{\mathbf{A}}(0, b, a)) = M^{\mathbf{A}}(0, a, 0) = 0.$$
  4. If $b = c \neq a$, then
  $$(a \wedge^{\mathbf{A}} b) \wedge^{\mathbf{A}} c = M^{\mathbf{A}}(0, M^{\mathbf{A}}(0, a, b), b) = M^{\mathbf{A}}(0, 0, b) = 0,$$
  $$a \wedge^{\mathbf{A}} (b \wedge^{\mathbf{A}} c) = a \wedge^{\mathbf{A}} (b \wedge^{\mathbf{A}} b) = a \wedge^{\mathbf{A}} b = 0.$$
  5. If $a \neq b, b \neq c, c \neq a$, then
  $$(a \wedge^{\mathbf{A}} b) \wedge^{\mathbf{A}} c = M^{\mathbf{A}}(0, M^{\mathbf{A}}(0, a, b), c) = M^{\mathbf{A}}(0, 0, c) = 0,$$
  $$a \wedge^{\mathbf{A}} (b \wedge^{\mathbf{A}} c) = M^{\mathbf{A}}(0, a, M^{\mathbf{A}}(0, b, c)) = M^{\mathbf{A}}(0, a, 0) = 0.$$

Let g be a majority algebra homomorphism $g : \mathbf{X} \to \mathbf{A}$. Then according to Definition 1.1.4 of a homomorphism for each two elements x, y and element p in X we get: $f(M^{\mathbf{X}}(p, x, y)) = M^{\mathbf{A}}(f(p), f(x), f(y))$. We can rewrite this equality: $f(x \wedge^{\mathbf{X}} y) = f(x) \wedge^{\mathbf{A}} f(y)$, therefore g is the semilattice homomorphism $g : \mathbf{X}' = \langle X, \wedge^{\mathbf{X}} \rangle \to \mathbf{A}' = \langle A', \wedge^{\mathbf{A}'} \rangle$.

We have proven that each homomorphism f from $\mathbf{X}$ to $\mathbf{A}$ such that $f(p) = 0$ is also a homomorphism from $\mathbf{X}'$ to $\mathbf{A}'$. Using the same argument we can prove the similar statements for homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ such that the image of p is 1 or 2. According to Corollary 2.1.3 the number of homomorphisms to the semilattice $\mathbf{A}'$ is polynomial, therefore the number of homomorphisms to the majority algebra $\mathbf{A}$ is also polynomial.

□

2.3 2-semilattices

An important generalization of semilattices is the class of 2-semilattices. Those are algebras with a binary operation which is idempotent, commutative, and satisfies the associative law for x, y, z with $|\{x, y, z\}| \leq 2$. In this section we consider the smallest 2-semilattice which is not a semilattice – the three-element rock-paper-scissors algebra introduced in Definition 2.3.2. It turns out this algebra also admits polynomially many homomorphisms. We will prove this fact with the help of the result for semilattices we obtained in Corollary 2.1.3. At first in Theorem 2.3.1 we will look at homomorphisms from conservative algebras to rock-paper-scissors algebras. Then we will consider homomorphisms from general algebras to the rock-paper-scissor algebra in Theorem 2.3.2. But at first we need to define the types of algebras mentioned above.

Definition 2.3.1. An $n-$ary operation f on a set A is called *conservative* if, for all elements $a_1, ..., a_n$ in A, we have $f(a_1, ..., a_n) \in \{a_1, ..., a_n\}$. We say than an algebra is *conservative*, if all the operations in its signature are conservative.

Definition 2.3.2. Let $\mathbf{A} = \langle \{0, 1, 2\}, \wedge^{\mathbf{A}} \rangle$ be the algebra whose binary operation $\wedge^{\mathbf{A}}$ is defined as follows.

- $\wedge^{\mathbf{A}}$ is idempotent, i.e. for all $x \in \{0, 1, 2\} : x \wedge^{\mathbf{A}} x = x$
- $\wedge^{\mathbf{A}}$ is commutative, i.e. for all $x, y \in \{0, 1, 2\} : x \wedge^{\mathbf{A}} y = y \wedge^{\mathbf{A}} x$
- $0 \wedge^{\mathbf{A}} 1 = 0, 0 \wedge^{\mathbf{A}} 2 = 2, 2 \wedge^{\mathbf{A}} 1 = 2$

We will call this algebra $\mathbf{A}$ the *rock-paper-scissors* algebra.

Now we are ready to estimate the number homomorphisms from a conservative algebra to the rock-paper-scissors algebra. Although a more general theorem will be proved afterwards, the presented proof gives additional information about homomorphisms in this special case.

Theorem 2.3.1. *Let $\mathbf{A} = \langle A, \wedge^{\mathbf{A}} \rangle$ be the rock-paper-scissors algebra. Then there exists a polynomial p such that for each conservative algebra $\mathbf{X} = \langle X, \wedge^{\mathbf{X}} \rangle$ the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is not greater than $p(|X|)$.*

Proof. Take an arbitrary conservative algebra $\mathbf{X}$. Assume that there exists at least one homomorphism from $\mathbf{X}$ to $\mathbf{A}$, otherwise the proof would be trivial. Let g and f be homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ and assume that g is surjective. Let's take two arbitrary elements x_1, x_2 from the set $g^{-1}(0)$. We will prove that the images of x_1 and x_2 under f are equal.

Let's define a relation $\leq^{\mathbf{X}}$ on the set X in the following way:

$$u \leq^{\mathbf{X}} v \iff u \wedge^{\mathbf{X}} v = u.$$

Define a relation $\leq^{\mathbf{A}}$ on the set A in a similar way:

$$d \leq^{\mathbf{A}} e \iff d \wedge^{\mathbf{A}} e = d.$$

Note that from definition of $\mathbf{A}$ we obtain:

$$0 \leq^{\mathbf{A}} 1 \leq^{\mathbf{A}} 2 \leq^{\mathbf{A}} 0.$$

Then as $f(u \wedge^{\mathbf{X}} v) = f(u) \wedge^{\mathbf{A}} f(v)$ we can conclude that if $u \leq^{\mathbf{X}} v$ in X, then $f(u) \leq^{\mathbf{A}} f(v)$ in A.

Take an element y from $g^{-1}(1)$ and an element z from $g^{-1}(2)$. As $g(x_1) = 0,\ g(y) = 1$, then

$$g(x_1 \wedge^{\mathbf{X}} y) = g(x_1) \wedge^{\mathbf{A}} g(y) = 0 \wedge^{\mathbf{A}} 1 = 0.$$

Since the algebra $\mathbf{X}$ is conservative, then either $x_1 \wedge^{\mathbf{X}} y = x_1$ or $x_1 \wedge^{\mathbf{X}} y = y$. But $g(y) = 1$, therefore $x_1 \wedge^{\mathbf{X}} y = x_1$, or equivalently $x_1 \leq^{\mathbf{X}} y$.

Similar calculation can be made for the element z:

$$g(z \wedge^{\mathbf{X}} x_1) = g(z) \wedge^{\mathbf{A}} g(x_1) = 2 \wedge^{\mathbf{A}} 0 = 2.$$

Conservativity of $\mathbf{X}$ then yields that $z \wedge^{\mathbf{X}} x_1 = z$, therefore $z \leq^{\mathbf{X}} x_1$.

Using the same argument we can also show that $y \leq^{\mathbf{X}} z$ (as $1 \leq^{\mathbf{A}} 2$).

We can rewrite the statements we obtained for x_1, y, z as a chain:

$$x_1 \leq^{\mathbf{X}} y \leq^{\mathbf{X}} z \leq^{\mathbf{X}} x_1.$$

This implies that

$$f(x_1) \leq^{\mathbf{A}} f(y) \leq^{\mathbf{A}} f(z) \leq^{\mathbf{A}} f(x_1) \tag{2.2}$$

What are the possibilities for the images of y and z under f in this case?

- If $f(y) = f(z)$, then we can shorten the chain (2.2) for $f(y)$: $f(x_1) \leq^{\mathbf{A}} f(y) \leq^{\mathbf{A}} f(x_1)$. Then the images of x_1 and y must be equal, otherwise one of the inequalities would not be true. Therefore in this case the images of all these elements are equal: $f(y) = f(z) = f(x_1)$.

- If $f(y) \neq f(z)$, then also $f(y) \neq f(x_1)$ and $f(z) \neq f(x_1)$, otherwise if $f(y) = f(x_1)$, we can rewrite the chain (2.2) as $f(y) \leq^{\mathbf{A}} f(z) \leq^{\mathbf{A}} f(y)$ and this is a contradiction, similarly if $f(z) = f(x_1)$, we get a contradiction as well. So $f(y) \neq f(z) \neq f(x_1) \neq f(y)$, i.e. the images of all these elements are not equal.

Analogically we get the same chain of inequalities for x_2:

$$x_2 \leq^{\mathbf{X}} y \leq^{\mathbf{X}} z \leq^{\mathbf{X}} x_2$$

as the images of x_1 and x_2 under g are equal. Again this implies that

$$f(x_2) \leq f(y) \leq f(z) \leq f(x_2) \tag{2.3}$$

Now let's look at the image of x_2 under f in these two cases:

- If $f(y) = f(z) = f(x_1)$, then (2.3) gives us that $f(x_2) \leq f(y) \leq f(x_2)$. Then $f(x_2) = f(y)$, otherwise one of the inequalities would not be true. So the images of all these four elements are equal in this case, i.e. $f(y) = f(z) = f(x_1) = f(x_2)$.
- If $f(y) \neq f(z) \neq f(x_1) \neq f(y)$ and using the chain (2.2) we can see that if $f(y) = 0$, $f(z) = 1$, then $f(x_1) = 2$. The chain (2.3) then gives us that $f(x_2) = 2$, otherwise one of the inequalities would be false. The same argument leads us to a conclusion the if $f(y) = 1, f(z) = 2$, then $f(x_1) = f(x_2) = 0$ and if $f(y) = 2, f(z) = 0$, then $f(x_1) = f(x_2) = 1$. So in this case we also get that $f(x_1) = f(x_2)$.

Therefore we can conclude that $f(x_1) = f(x_2)$ for all elements x_1, x_2 in $g^{-1}(0)$. This means that all the elements from $g^{-1}(0)$ have the same image under the homomorphism f. Using the same argument as before it can be proven that the similar statements are true for the elements in $g^{-1}(1)$ and $g^{-1}(2)$. Altogether, all the sets $f(g^{-1}(0)), f(g^{-1}(1)), f(g^{-1}(2))$ contain just one element: $0, 1$ or 2. We assumed that the homomorphism g was surjective, so f is determined by the choice of these elements. There are $3 \cdot 3 \cdot 3 = 27$ ways to choose the images of $g^{-1}(0)$, $g^{-1}(1)$, $g^{-1}(2)$ under f, so there are at most 27 homomorphisms f from $\mathbf{X}$ to $\mathbf{A}$.

In the previous case we assumed that g was surjective. Now let g be a homomorphism from X to A which is not surjective, i.e. at least one of the sets $g^{-1}(0)$, $g^{-1}(1)$, $g^{-1}(2)$ is empty. Take $g^{-1}(2) = \emptyset$. Then the image of each element in X is either 0 or 1. It can be easily checked that $\wedge^{\mathbf{A}}$ is a semilattice operation on the set $\{0,\ 1\}$. This means that homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ are homomorphisms from $\mathbf{X}$ to the two-element subalgebra $\langle\{0, 1\}, \wedge^{\mathbf{A}}\rangle$, which is also a semilattice. We have proven in Corollary 2.1.3 that a semilattice admits polynomially many homomorphisms. Using the equivalent definition from Remark 1.2.1 we can conclude that there exist a real number c and a positive integer k such that for each algebra $\mathbf{X}$ the number of homomorphisms to $\langle\{0, 1\}, \wedge^{\mathbf{A}}\rangle$ is not greater than $c|X|^k$.

So far we have considered only homomorphisms such that $g^{-1}(2) = \emptyset$. Using the same argument we obtain that the numbers of homomorphisms such that $g^{-1}(0) = \emptyset$ and $g^{-1}(1) = \emptyset$ are not greater than $c|X|^k$.

Altogether, we have computed that if there exists at least one surjective homomorphism from $\mathbf{X}$ to $\mathbf{A}$, then there are at most 27 homomorphisms from $\mathbf{X}$ to $\mathbf{A}$. The number of homomorphisms which are not surjective is not greater than $3c|X|^k$. Therefore a total number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is not greater than $3c|X|^k + 27$, which proves the theorem.

□

Now let's look at a more general case: what if the algebra $\mathbf{A}$ remains the same, but the algebra $\mathbf{X}$ is some general algebra, not necessary conservative? We will show that the number of homomorphisms is also polynomial in this case.

In this proof we will use the equivalent definition of an algebra which admits polynomially many homomorphisms mentioned in Remark 1.2.1.

Theorem 2.3.2. *Let* $\mathbf{A}$ *be the rock-paper-scissors algebra. Then* $\mathbf{A}$ *admits polynomially many homomorphisms.*

Proof. We will show that the number of homomorphisms to $\mathbf{A}$ is polynomial in a few steps. We will look at an arbitrary algebra $\mathbf{X}$. At first we will consider homomorphisms from a specific subalgebra $\mathbf{C}$ of $\mathbf{X}$ and show that their number is polynomial. Then we will notice that there only polynomially many ways to extend homomorphisms from $\mathbf{C}$ to $\mathbf{A}$ to homomorphisms from the whole algebra $\mathbf{X}$ to $\mathbf{A}$. Combining these two facts we obtain that the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is polynomial. Now let us prove this in detail.

Let $\mathbf{X} = \langle X, \wedge^{\mathbf{X}} \rangle$ be an algebra and let n be the cardinality of X. We also fix an arbitrary element b in X. We concentrate on homomorphisms f from $\mathbf{X}$ to $\mathbf{A}$ such that $f(b) = 0$. Since the mapping $0 \mapsto 1 \mapsto 2 \mapsto 0$ is a homomorphism from $\mathbf{A}$ to $\mathbf{A}$, the upper bound will hold for the number of homomorphisms with $f(b) = 1$ and with $f(b) = 2$.

Consider the set $C' = \{b \wedge^{\mathbf{X}} c, c \in X\}$. At first notice that the image of all the elements in C' under f is either 0 or 2:

$$f(b \wedge^{\mathbf{X}} c) = f(b) \wedge^{\mathbf{A}} f(c) = 0 \wedge^{\mathbf{A}} f(c)$$

If $f(c) = 0$ or $f(c) = 1$, then $f(b \wedge^{\mathbf{X}} c) = 0 \wedge^{\mathbf{A}} f(c) = 0$. If $f(c) = 2$, then $f(b \wedge^{\mathbf{X}} c) = 2 \wedge^{\mathbf{A}} f(c) = 2$.

Let $\mathbf{C}$ be the subalgebra of $\mathbf{X}$ generated by C'. Since $\mathbf{S} = \langle \{0, 2\}, \wedge^{\mathbf{A}} \rangle$ is a subalgebra of $\mathbf{A}$ and the preimage of a subalgebra (of the target algebra) under a homomorphism is a subalgebra (of the source algebra), the preimage of a $\{0, 2\}$ under f contains C. In other words, f maps C into $\{0, 2\}$.

Moreover, $\mathbf{S}$ is a two-element semilattice. We have proven in Corollary 2.1.3, that the number of homomorphisms to the two-element semilattice is polynomial. Since the restriction of f to C is a homomorphism from $\mathbf{C}$ to $\mathbf{S}$, the number of such restrictions is less than or equal to the number of homomorphisms from $\mathbf{C}$ to $\mathbf{S}$ which is bounded from above by some specific polynomial $d|C|^k$, where d is a real number and k is a positive integer that do not depend on $\mathbf{X}$. As $\mathbf{C}$ is a subalgebra of $\mathbf{X}$, then certainly $|C| \leq n$, therefore $d|C|^k \leq dn^k$. If we summarize the last estimations, we obtain that the number of homomorphisms f' from $\mathbf{C}$ to $\mathbf{S}$ is bounded from above by dn^k (and the same bound applies to the number of restrictions to C of homomorphisms $f : \mathbf{X} \to \mathbf{A}$ with $f(b) = 0$).

Now we consider homomorphisms f from $\mathbf{X}$ to $\mathbf{A}$ such that $f(b) = 0$ that extend a fixed restriction $f' : \mathbf{C} \to \mathbf{S}$. We have shown in the previous paragraph that either $f'(b \wedge^{\mathbf{X}} x) = 0$ or $f'(b \wedge^{\mathbf{X}} x) = 2$. If we denote these sets of elements by D' and E' respectively, i.e. $D' = \{x \in X; f'(b \wedge^{\mathbf{X}} x) = 0\}$ and $E' = \{x \in X; f'(b \wedge^{\mathbf{X}} x) = 2\}$, then $X = D' \cup E'$. We will consider possible restrictions of f to D' and E' separately.

Let's begin with D'. Let $\mathbf{D}$ be the subalgebra of $\mathbf{X}$ generated by $D' = \{x \in X; f'(b \wedge^{\mathbf{X}} x) = 0\}$. If $f'(b \wedge^{\mathbf{X}} x) = 0$, then $f(b) \wedge^{\mathbf{A}} f(x) = 0 \wedge^{\mathbf{A}} f(x) = 0$. Therefore $f(x)$ is either 0 or 1, i.e. the image of an element from D' under f is either 0 or 1. It follows as above that the restriction of f to D is a homomorphism from $\mathbf{D}$ to the two element semilattice $\langle \{0, 1\}, \wedge^{\mathbf{A}} \rangle$. The number of such homomorphisms from $\mathbf{D}$ is polynomial as we have shown in Corollary 2.1.3, it is bounded from above by the same polynomial as the number of homomorphisms $\mathbf{C}$ to $\mathbf{S}$ above. We can conclude that the number of restrictions to the set D' of homomorphisms $f : \mathbf{X} \to \mathbf{A}$ with $f(b) = 0$ that extend f' is bounded from above by dn^k.

Now let's take a look at the set $E' = \{x \in X; f'(b \wedge^{\mathbf{X}} x) = 2\}$. If $f'(b \wedge^{\mathbf{X}} x) = 2$, then $f(b) \wedge f(x) = 0 \wedge f(x) = 2$, so $f(x)$ is necessarily 2 in this case. In other words, the value of $f'(b \wedge^{\mathbf{X}} x)$ uniquely determines the value of $f(x)$: $f(x) = 2$.

If we summarize the last two paragraphs, we have shown that for each fixed f': $\mathbf{C} \to \mathbf{S}$ there are only polynomially many possibilities for the images of the elements in D', this number is bounded above by dn^k. The images of the elements in E' are uniquely determined by the restriction f'. As $X = D' \cup E'$, this means that there are no more than dn^k possibilities to extend f': $\mathbf{C} \to \mathbf{S}$ to a homomorphism f: $\mathbf{X} \to \mathbf{A}$ such that $f(b) = 0$. In the first part of our proof we have shown that the restriction to C of a homomorphism $f : \mathbf{X} \to \mathbf{A}$ such that $f(b) = 0$ is a homomorphism from $\mathbf{C} \to \mathbf{S}$ and the number of such restrictions is at most dn^k. This means that the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ with $b \mapsto 0$ is not greater than $dn^k \cdot dn^k = d^2n^{2k}$. Altogether the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is not greater than $3d^2n^{2k}$ and we conclude that $\mathbf{A}$ admits polynomially many homomorphisms. □

2.4 Groups

Now let $\mathbf{A}$ be a group. Is the number of homomorphisms polynomial in this case? The answer is positive and we will prove this later. But first we need a lemma about the number of generators in a minimal generating set of a group. We show that this number cannot be large.

In the following $\langle b_1, \dots \rangle$ denotes the subgroup generated by $b_1, \dots$.

Lemma 2.4.1. *Let $\mathbf{B}$ be a finite group, $|B| = n > 1$, $B' = \{b_1, b_2, ..., b_k\}$ be a minimal generating set of this group, i.e. $b_{i+1} \notin \langle b_1, ...b_i \rangle$. Then $k \le \log_2(n)$.*

Proof. Let's prove this by induction on the number k.

If $k = 1$, then B' contains just one element b. The order of this element is at least 2, otherwise $|B| = 1$. So the set B contains at least 2 elements, $\log_2(n) \ge 1$ and the inequality $k \le \log_2(n)$ holds.

Let's look at the case when $k > 1$. Then the group $\mathbf{B}$ contains the subgroup $\mathbf{C} = \langle b_1, b_2, ..., b_{k-1} \rangle$ and the set b_kC. These sets are disjoint: if $b_kc_1 = c_2$ for some elements $c_1, c_2 \in C$, this means that $b_k = c_2c_1^{-1}$, so $b_k \in C$. But B' is a minimal generating set, so this cannot be true. So $b_kc_1 \ne c_2$ for all $c_1, c_2 \in C$. This means that $n \ge |C| + |b_kC| = 2|C|$. The group $\mathbf{C}$ has a minimal generating set of size $k-1$, so according to the inductive assumption $|C| \ge 2^{k-1}$. Combining the last two inequalities we obtain $n \ge 2|C| \ge 2^k$, so $k \le \log_2(n)$. □

Theorem 2.4.2. *Let $\mathbf{A}$ be a finite group. Then $\mathbf{A}$ admits polynomially many homomorphisms.*

Proof. Let $\mathbf{X}$ be an algebra. As in the previous proofs, due to Lemma 1.3.3 without the loss of generality we can assume that $\mathbf{X}$ is a group.

Let us denote the cardinalities of X and A by n and m respectively. Let k be the least cardinality of the generating set $X' = \{x_1, x_2, ..., x_k\}$ of $\mathbf{X}$ and f be a homomorphism from $\mathbf{X}$ to $\mathbf{A}$. In this proof we will use the notation $C_{\mathbf{A}}(n)$ introduced in Definition 1.2.1.

At first we can observe that each homomorphism is determined by the images of the elements in the generating set X'. There are at most m possibilities for the image of each element and there are k elements in X'. This means that the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is not greater than m^k, i.e. $C_{\mathbf{A}}(n) \leq m^k$.

We have proven in Lemma 2.4.1 that the cardinality k of a minimal generating set is not greater than $\log_2(n)$. Giving these two inequalities together we get $C_{\mathbf{A}}(n) \leq m^k \leq m^{\log_2(n)} = (2^{\log_2(m)})^{\log_2(n)} = 2^{\log_2(n)\log_2(m)} = n^{\log_2(m)}$. $n^{\log_2(m)}$ is less than or equal to a polynomial of degree $\lceil \log_2(m) \rceil$, so $\mathbf{A}$ admits polynomially many homomorphisms.

□

The two-element group and the two-element minority algebra are closely related in that the minority operation can be written in terms of the group operation as $m(x, y, z) = xy^{-1}z$. Similarly, for every group $\mathbf{A}$ we can consider its reduct $\mathbf{A}' = \langle A; m \rangle$, where $m(x, y, z) = xy^{-1}z$. It can be shown by refining the argument above that such algebras also admit polynomially many homomorphisms [2], but we do not give the details here.

2.5 Unary algebras

In this section we consider unary algebras.

Definition 2.5.1. Algebras in which every basic operation is unary are called *unary algebras.*

At first we will look at algebras with only one unary operation, and then we will generalize this case for algebras with more operations. We will prove that the number of homomorphisms is exponential in both cases.

Theorem 2.5.1. *Let* $\mathbf{A} = \langle \{0, 1\}, f^{\mathbf{A}} \rangle$ *be a two-element algebra with a unary operation* $f^{\mathbf{A}}$. *Then* $\mathbf{A}$ *admits exponentially many homomorphisms.*

Proof. Let's look at the algebra $\mathbf{A}$. There are four possibilities for the results of operation $f^{\mathbf{A}}$ on the elements of $A = \{0, 1\}$:

(a) $f^{\mathbf{A}}(0) = 0, f^{\mathbf{A}}(1) = 1$

(b) $f^{\mathbf{A}}(0) = 1, f^{\mathbf{A}}(1) = 0$

(c) $f^{\mathbf{A}}(0) = 0, f^{\mathbf{A}}(1) = 0$

(d) $f^{\mathbf{A}}(0) = 1, f^{\mathbf{A}}(1) = 1$

We will consider all the possibilities and show that in each case, for every even n, there exists an algebra $\mathbf{X}$ of size n such that the number of homomorphisms from $\mathbf{X}$ to $\mathbf{A}$ is at least $(\sqrt{2})^n$. It follows that $\mathbf{X}$ admits exponentially many homomorphisms (see the end of the proof of Theorem 2.5.2 for details).

We notice that in each case there are at least two different homomorphisms from $\mathbf{A}$ to $\mathbf{A}$. The cases (c) and (d) are symmetric, so without the loss of generality we can look just on of them.

(a) $f^{\mathbf{A}}(0) = 0, f^{\mathbf{A}}(1) = 1$

The image of 0 under homomorphism from $\mathbf{A}$ to $\mathbf{A}$ can be either 0 or 1 independently, the same statement is true for the image of 1. Therefore there are $2^2 = 4$ homomorphisms from $\mathbf{A}$ to $\mathbf{A}$.

(b) $f^{\mathbf{A}}(0) = 1, f^{\mathbf{A}}(1) = 0$

There are two possibilities for the images of 0 and 1 under homomorphism h from $\mathbf{A}$ to $\mathbf{A}$: either $h(0) = 1$, and then $h(1) = h(f^{\mathbf{A}}(0)) = f^{\mathbf{A}}(1) = 0$, or $h(1) = 0$, and then $h(0) = h(f^{\mathbf{A}}(1)) = f^{\mathbf{A}}(0) = 1$. Clearly, both of these mappings h are homomorphisms. Therefore there are two homomorphisms from $\mathbf{A}$ to $\mathbf{A}$ in this case.

(c) $f^{\mathbf{A}}(0) = 0, f^{\mathbf{A}}(1) = 0$

As in the previous case, there are two possibilities for the images of 0 and 1 under $h : \mathbf{A} \to \mathbf{A}$: either $h(1) = 1$, then $h(0) = h(f^{\mathbf{A}}(1)) = f^{\mathbf{A}}(1) = 0$, or $h(1) = 0$, then $h(0) = h(f^{\mathbf{A}}(1)) = f^{\mathbf{A}}(0) = 0$. Again, there are two homomorphisms from $\mathbf{A}$ to $\mathbf{A}$.

Now we fix a number $n \in \mathbb{N}$ and define the set X as $X = A \times \{1, 2, ..., n\}$. So we can look at the set X as n copies of A. We define the operation $f^{\mathbf{X}}$ on X in the following way:

$$f^{\mathbf{X}}(a, i) = (f^{\mathbf{A}}(a), i) \text{ for each } a \in \{0, 1\}, i \leq n.$$

Therefore $\mathbf{X} = \langle X, f^{\mathbf{X}} \rangle$. For each copy $A \times \{i\}$ of $\mathbf{A}$, where $i \leq n$, there are at least two ways to define a partial homomorphism from this copy to $\mathbf{A}$. Moreover, h can be chosen independently on each of these copies. Therefore there are at least 2^n homomorphisms from $\mathbf{X}$ to $\mathbf{A}$. We will define these homomorphisms formally in the next proof of Theorem 2.5.2.

Notice that we have considered only algebras $\mathbf{X}$ which have an even number of elements. This problem will be also solved in the proof of Theorem 2.5.2, where we will generalize the idea used in this proof.

□

Theorem 2.5.2. *Let $\mathbf{A} = \langle A, (f_i^{\mathbf{A}})_{i \in I} \rangle$ be a finite unary algebra and the cardinality of A is at least 2. Then $\mathbf{A}$ admits exponentially many homomorphisms.*

Proof. Let us denote the cardinality of A by m. According to our assumption $m \geq 2$, so A contains at least two elements, denote any of them by 0 and 1.

As in the previous proof we will construct a family of algebras with large number of homomorphisms into $\mathbf{A}$.

We fix a number $n \in \mathbb{N}$ and define the set X as $X = A \times A \times \{1, 2, ..., n\}$. So we can look at the set X as n copies of $A \times A$. Now we take the same signature Σ and define the corresponding operations $f_i^{\mathbf{X}}$ on the algebra $\mathbf{X}$ in the following way: for all $i \in I$ and for all $x = (x_1, x_2, k) \in X$ we set $f_i^{\mathbf{X}}(x_1, x_2, k) = (f_i^{\mathbf{A}}(x_1), f_i^{\mathbf{A}}(x_2), k)$.

Now we can define 2^n different homomorphisms $g_{l_1,...,l_n}$, where $l_j \in \{1, 2\}$, $j \in \{1, 2, ..., n\}$, from $\mathbf{X}$ to $\mathbf{A}$ in the following way: $g_{l_1,...,l_n}(x_1, x_2, k) = x_{l_k}$ for all $x = (x_1, x_2, k) \in X$.

These functions $g_{l_1,...,l_n}$ are indeed homomorphisms, because for all $j \in \{1, ..., n\}$, for all $i \in I$, and for all $x = (x_1, x_2, k) \in X$,

$$g_{l_1,...,l_n}(f_i^{\mathbf{X}}((x_1, x_2, k)) = g_{l_1,...,l_n}(f_i^{\mathbf{A}}(x_1), f_i^{\mathbf{A}}(x_2), k) = f_i^{\mathbf{A}}(x_{l_k}) = f_i^{\mathbf{A}}(g_{l_1,...,l_n}((x_1, x_2, k))).$$

Next we observe that these homomorphisms $g_{l_1,...,l_n}$ are different. Consider two homomorphisms $g_{l_1,...,l_n}, g_{s_1,...,s_n}$ whose indices are different, say $l_i = 1$ and $s_i = 2$, and also consider the element $x = (0, 1, 1)$. The value of $g_{l_1,...,l_n}$ on x is $g_{l_1,...,l_n}((0, 1, 1)) = x_{l_i} = x_1 = 0$, while the value of $g_{s_1,...,s_n}$ is $g_{s_1,...,s_n}((0, 1, 1)) = x_{s_i} = x_2 = 1$, and we are done.

We have found 2^n different homomorphisms from $\mathbf{X}$ to $\mathbf{A}$, this means that there are at least 2^n homomorphisms from $\mathbf{X}$ to $\mathbf{A}$.

Finally, we show that $C_{\mathbf{A}}(N)$ bounded from below by an exponential function. We fix $N > m^2$.

Note that if $N = m^2 n$ for some positive integer n, then we have proven that there are at least $2^n = 2^{\frac{N}{m^2}} = (2^{\frac{1}{m^2}})^N$ homomorphisms from $\mathbf{X}$ to $\mathbf{A}$.

In general, we take the maximal positive integer n' such that $N \geq m^2 n'$. We already know that there exists an algebra $\mathbf{X}'$ such that the cardinality of $\mathbf{X}'$ is $N' = m^2 n'$ and there are at least $(2^{\frac{1}{m^2}})^{N'}$ homomorphisms from $\mathbf{X}'$ to $\mathbf{A}$. According to Definition 1.2.1 of $C_{\mathbf{A}}(N)$ as $N' \leq N$, then $C_{\mathbf{A}}(N) \geq (2^{\frac{1}{m^2}})^{N'}$. At the same time we have taken n' as the maximal positive integer such that $N \geq m^2 n'$, therefore we have an inequality $m^2 n' < N < m^2(n'+1)$. If we rewrite the second inequality using $N' = m^2 n'$, we obtain $N < N' + m^2$, therefore $N' > N - m^2$. Finally using this we can rewrite the estimation of $C_{\mathbf{A}}(N)$ as follows.

$$C_{\mathbf{A}}(N) \geq (2^{\frac{1}{m^2}})^{N'} > (2^{\frac{1}{m^2}})^{N-m^2} = \frac{1}{2}(2^{\frac{1}{m^2}})^N$$

Thus according to Definition 1.2.3 $\mathbf{A}$ admits exponentially many homomorphisms. □

Corollary 2.5.3. *Every finite essentially unary algebra admits exponentially many homomorphisms.*

Proof. As essentially unary algebra is a reduct of a unary algebra, the claim follows from Theorem 2.5.2 and Lemma 1.3.1. □

Conclusion

We have proven that finite unary algebras admit exponentially many homomorphisms, whereas finite semilattices, groups and two specific algebras - three-element majority algebra and three-element 2-semilattice - admit polynomially many homomorphisms. As we have mentioned before, these results have already been superseded in the article [2] with the help of Tame Congruence Theory [3]. Moreover, all algebras which admit polynomially many homomorphisms were recently fully characterized by Barto, Mottet, and DeMeo (unpublished): A finite algebra admits polynomially many homomorphisms if and only if it does not have a nontrivial strongly solvable congruence (see [3] for the definition of strong solvability). The result for the rock-paper-scissors algebra was an important step towards this characterization.

Lemma 2.4.1 in Section 2.4 shows a stronger property of finite groups than admitting polynomially many homomorphisms: each finite group has a generating set of logarthmic cardinality (with respect to the cardinality of the group). This phenomenon can be an interesting topic for further study. One specific question in this direction is, for which sets of identities there exists a real number k such that each finite algebra $\mathbf{A}$ satisfying these identities has the least generating set of cardinality not greater than $k \log(|X|)$.

Bibliography

[1] Libor Barto, William DeMeo, and Antoine Mottet. The complexity of the homomorphism problem for boolean structures. *arXiv*, abs/2010.04958v1, 2020.

[2] Libor Barto, William DeMeo, and Antoine Mottet. Constraint satisfaction problems over finite structures. *arXiv*, abs/2010.04958v2, 2021.

[3] David Charles Hobby and Ralph McKenzie. *The Structure of Finite Algebras*. American Mathematical Society, 1996.

[4] Clifford Bergman. *Universal Algebra: Fundamentals and Selected Topics*. Chapman & Hall Pure and Applied Mathematics. CRC Press, 2011.

[5] Emil Post. *The Two-Valued Iterative Systems of Mathematical Logic. (AM-5)*. Princeton University Press, 1941.