DECIDABILITY IN ALGEBRA

by

Miklós Maróti

Adviser:

Prof. Ágnes Szendrei

Ph.D. Dissertation

Bolyai Institute

University of Szeged

June, 2006.

dedicated to the memory
of Kevin Blount

Acknowledgments

This dissertation would have been impossible without the encouragement and support of many people at different times and places. I cannot possibly thank everyone individually, but would like to express my gratitude to them all.

I would first and foremost like to thank my adviser, Ágnes Szendrei, for nursing my initial steps and encouraging my voyage into the wonders of algebra. Her academic rigor, deep knowledge and clear explanations are unsurpassed. She has formed my interest and brought me in touch with the best researchers and research topics. Among all people I learned from, she had the most profound influence on my academic writing. I apologize to her, and to my readers, that my style does not seem to converge to that of hers, in spite of her continuing efforts.

Secondly, I owe a huge debt of gratitude to my co-adviser, Ralph McKenzie, for his unforgettable seminars and endless source of superb mathematical problems. We often worked together, or raced against each other, where he proved to be many times quicker and younger than me in almost all cases.

Many thanks to Petar Marković for his friendship and intellectual stimulation. I have fond memories of the cheerful and sometimes very difficult days and months when we shared an apartment in Nashville. I am very grateful to Gábor Kun for reminding me of the chromatic number of Kneser graphs, and then for listening to my first disorganized explanation of my main result. Last, but not least, special thanks to the members of the Bolyai Institute for their continuing trust in my abilities and understanding of my limitations.

Table of contents

Introduction

Algebras with a semilattice operation, which commutes with all other operations, have been studied in various forms. In many respects these algebras behave similarly to modules. For example, it is proved in [15] that if a locally finite variety of type-set $\{\mathbf{5}\}$ satisfies a term-condition similar to the term-condition for abelian algebras, then it has a semilattice term that commutes with all other term operations.

Within the class of modes—that is, idempotent algebras whose basic operations commute with each other—those having a semilattice term operation play an important role (see [28, 29]); these algebras are called semilattice modes. The structure of locally finite varieties of semilattice modes is described in [14].

An interesting class of algebras with a commuting semilattice operation arises if we add automorphisms, as basic operations, to a semilattice. This is a special case of the construction studied in [3]. In general, one can expand any variety $\mathcal{V}$ by a fixed monoid $\mathbf{F}$ of endomorphisms in a natural way. The expanded variety is the variety of $\mathcal{V}$-algebras $\mathbf{A}$ equipped with new unary basic operations, acting as endomorphisms on $\mathbf{A}$. In this construction we keep $\mathbf{F}$ fixed, and do the same when $\mathbf{F}$ is a group. We remark that there is a different approach, when the group $\mathbf{F}$ is not kept fixed; what one gets then is the theory of varieties of group representations, where the objects are groups acting on some semilattices (see [1]).

In a number of different cases the simple and subdirectly irreducible algebras of the expanded variety have been determined. In [11] J. Ježek described all simple algebras in the variety of semilattices expanded by two commuting automorphisms. In this case the monoid $\mathbf{F}$ is the free commutative group with two generators. In [12] he also described all subdirectly irreducible semilattices with a single distinguished automorphism.

In Chapter 1 we generalize the main result of [11] to arbitrary commutative group $\mathbf{F}$, that is, we describe all simple algebras in the variety of semilattices expanded by an abelian group of automorphisms (published in [18]). The same results were discovered independently by R. El Basher and T. Kepka in [7]. In fact, their results are slightly more general: they study simple semimodules over commutative semirings, where addition is a semilattice operation.

General duality theory is capable of describing various well-known dualities—for example Pontryagin's, Stone's and Priestley's—between a category $\mathcal{A}$ of algebras with homomorphisms and a category $\mathcal{X}$ of topological structures with continuous structure preserving maps. In all these cases the class $\mathcal{A}$ is a quasi-variety generated by a single algebra $\mathbf{P} \in \mathcal{A}$, and $\mathcal{X}$ is the class of closed substructures of powers of an object $\underset{\sim}{\mathbf{P}} \in \mathcal{X}$ having the same underlying set as $\mathbf{P}$. By this theory, not every quasi-variety admits a natural duality. Therefore, to leverage the power of duality, it is natural to ask which finitely generated quasi-varieties admit a natural duality. Is this characterization possible? Is it decidable of a finite algebra $\mathbf{P}$ whether the quasi-variety generated by $\mathbf{P}$ admits a natural duality? This second question is known as the *natural duality problem*. Currently, we do not know the answer to this problem, but many expect it to be undecidable.

The natural duality problem was partially reduced to a pure algebraic problem in the following way. We call a term t of an algebra $\mathbf{P}$ a *near-unanimity term* if it satisfies the following identities:

$$t(y, x, \dots, x) \approx t(x, y, x, \dots, x) \approx \dots \approx t(x, \dots, x, y) \approx x.$$

Near-unanimity term operations come up naturally in the study of algebras. For example, all lattices have a ternary near-unanimity term $t(x, y, z) = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$. From E. L. Post's classification [26] we know that almost all clones on a two element set contain a near-unanimity operation; the exceptions are those that are contained in $\langle \wedge, 0, 1 \rangle$, $\langle +, 0, 1 \rangle$, $\langle \rightarrow \rangle$ or in their duals. It is also well known that an algebra having a near-unanimity term lies in a congruence distributive variety, and has a finite base of identities provided it is of finite signature (see [30]).

B. A. Davey and H. Werner proved in [6] that in the presence of a near-unanimity term of $\mathbf{P}$, the quasi-variety $\mathcal{A}$ generated by $\mathbf{P}$ admits a natural duality. The converse was proved in [5] under the assumption that $\mathcal{A}$ is congruence join-semi-distributive: if $\mathcal{A}$ admits a natural duality and is congruence join-semi-distributive then $\mathbf{P}$ has a (finitary) near-unanimity term. This theorem, known as the near-unanimity obstacle theorem, implies that if it were undecidable of a finite algebra whether it has a near-unanimity term, then the natural duality problem would also be undecidable. We call the premise of this implication the *near-unanimity problem*, which was posed in [5] over ten years ago.

Clearly, the algebra $\mathbf{P}$ has a near-unanimity term operation t if and only if the equations

$$t(y, x, \dots, x) = t(x, y, x, \dots, x) = \dots = t(x, \dots, x, y) = x$$

hold for the generator elements x, y of the two-generated free algebra in the quasi-variety $\mathcal{A}$ generated by $\mathbf{P}$. Probably this observation motivated R. McKenzie's unpublished result [22] where he proves that it is undecidable of a finite algebra $\mathbf{P}$ and a pair $x, y \in P$ of fixed elements whether $\mathbf{P}$ has a term t that behaves as a near-unanimity term on $\{x, y\}$. This result does not imply the undecidability of the near-unanimity problem because the algebras used in his construction are not freely generated by the elements x, y in the quasi-variety they generate.

The key result presented in Chapter 2 is the improvement of R. McKenzie's result to a fixed $|P| - 2$ element subset, and the simplification of his elaborate construction (to appear in [19]). The basic idea, however, is intact: the use of Minsky machines—which are equivalent to Turing machines—and the encoding of their computations in the terms of $\mathbf{P}$. The method used in the proof relies on an absorbing element as the indicator of defects. An improvement of this method to $|P| - 1$ elements might be possible, which could be formulated, analogously to the results in [13], as the undecidability of the near-unanimity problem for partial algebras:

Problem 1. *Given a finite partial algebra, decide whether it has a term that is defined on all near-unanimous evaluations and satisfies the near-unanimity identities.*

In Chapter 3 we show that the near-unanimity problem is decidable, which is a rather surprising development after the negative partial results (unpublished, see [20]). As an immediate consequence of the decidability of the near-unanimity problem and the near-unanimity obstacle theorem, the natural duality problem for finite algebras that generate a congruence join-semi-distributive variety is also decidable. However, the decidability of the natural duality problem in general is still open.

The proof of the decidability of the near-unanimity problem relies on the study of the following special fragment of clones. Given an operation t, we consider those binary operations—called polymers—with their multiplicities that arise as $t(x, \ldots, x, y, x, \ldots, x)$ where the lone y is at a fixed coordinate. Clearly, near-unanimity operations are characterized by their binary polymers; namely they all must be equal to x. By studying the polymers of composite operations, we arrive to a notion of composition for binary polymers, which we use to solve the near-unanimity problem.

Since there are only finitely many algebras on a fixed n-element set whose basic operations are at most r-ary, by the decidability of the near-unanimity problem, there exists a recursive function $N(n, r)$ that puts an upper limit on the minimum arity of a near-unanimity term operation for those algebras that have one. Consequently, given an algebra $\mathbf{P}$ whose operations are at most r-ary, one can decide the near-unanimity problem by simply constructing all at most $N(|P|, r)$-ary terms and checking if one of them yields a near-unanimity operation. If no such is found, then $\mathbf{P}$ has no near-unanimity term operation. We know that such recursive function $N(n, r)$ exists, but currently we do not have a formula for one.

A very interesting group of open problems is related to the *constraint satisfaction problem*, which we do not define here and refer the reader to [8] for details. It is proved in [10] that if a set Γ of relations on a set admits a compatible near-unanimity operation, then the corresponding constraint satisfaction problem $\mathrm{CSP}(\Gamma)$ is solvable in polynomial time. Therefore, it is natural to consider the *near-unanimity problem for relations*:

Problem 2. *Given a finite set Γ of relations on a set, decide whether there exists a near-unanimity operation that is compatible with each member of Γ.*

Currently we are unable to solve this problem, even in the light of our result. We know that if a clone has a near-unanimity operation, then both the clone and its dual relational clone are finitely generated (see [30]). Inspired by this fact, we ask the following:

Problem 3. *Given a finite set of operations and a finite set of relations on the same underlying set, decide if the functional and relational clones they generate are duals of each other.*

The three chapters of the dissertation are self contained, independent of each other, and are based on the essential parts of [18, 19] and [20], respectively. We assume basic knowledge of universal algebra and direct the reader to either [2] or [23] for reference. Although the study of the near-unanimity problem stems from the study of natural dualities (see [4, 5]), the reader is not required to know this theory.

1 F-semilattices

In [3] one can find the definition of the expansion of a variety by a fixed monoid of endomorphisms, and also some basic properties of this construction. In this section we need only the following special case.

Definition 1.1. An algebra $\mathbf{S} = \langle S; \wedge, F \rangle$ with a binary operation $\wedge$ and a set F of unary operations is an $\mathbf{F}$-*semilattice*, if $\mathbf{F} = \langle F; \cdot, ^{-1}, \mathrm{id} \rangle$ is a group and $\mathbf{S}$ satisfies the following identities:

(1) the operation $\wedge$ is a semilattice operation,

(2) $\mathrm{id}(x) \approx x$,

(3) $f(g(x)) \approx (f \cdot g)(x)$ for all $f, g \in F$, and

(4) $f(x \wedge y) \approx f(x) \wedge f(y)$ for all $f \in F$.

In other words, an $\mathbf{F}$-semilattice is a semilattice expanded with a set F of new operations which forms an automorphism group of the semilattice. Usually the group $\mathbf{F}$ will be fixed. Note that every semilattice can be considered as an $\mathbf{F}$-semilattice in a trivial way: every unary operation of F acts as the identity function. Now we give a much more typical example of an $\mathbf{F}$-semilattice.

Definition 1.2. Let $\mathbf{P}(F) = \langle P(F); \wedge, F \rangle$ be the $\mathbf{F}$-semilattice which is defined on the set $P(F)$ of all subsets of F by setting

(1) $A \wedge B = A \cap B$ for all $A, B \subseteq F$, and

(2) $f(A) = A \cdot f^{-1}$ for all $f \in F$ and $A \subseteq F$.

Thus the meet operation is intersection, and every unary operation $f \in F$ acts by taking complex product with f^{-1} on the right hand side. We show that $\mathbf{P}(F)$ contains all subdirectly irreducible $\mathbf{F}$-semilattices.

Proposition 1.3. *Every subdirectly irreducible* $\mathbf{F}$*-semilattice can be embedded in* $\mathbf{P}(F)$.

Proof. Let $\mathbf{S}$ be a subdirectly irreducible $\mathbf{F}$-semilattice. For every element $s \in S$ we define a homomorphism φ_s from $\mathbf{S}$ to $\mathbf{P}(F)$ as follows:

$$\varphi_s \colon S \to P(F); \quad \varphi_s(x) = \{\, f \in F \mid f(x) \geq s \,\}. \tag{1.3a}$$

This function is indeed a homomorphism, since

$$\begin{aligned} \varphi_s(x \wedge y) &= \{\, f \in F \mid f(x \wedge y) \geq s \,\} \\ &= \{\, f \in F \mid f(x) \wedge f(y) \geq s \,\} \\ &= \{\, f \in F \mid f(x) \geq s \text{ and } f(y) \geq s \,\} \\ &= \{\, f \in F \mid f(x) \geq s \,\} \cap \{\, f \in F \mid f(y) \geq s \,\} \\ &= \varphi_s(x) \wedge \varphi_s(y), \end{aligned}$$

and for any unary operation $g \in F$ we have

$$\begin{aligned}
\varphi_s(g(x)) &= \{\, f \in F \mid f(g(x)) \geq s \,\} \\
&= \{\, f \in F \mid (f \cdot g)(x) \geq s \,\} \\
&= \{\, h \cdot g^{-1} \in F \mid h(x) \geq s \,\} \\
&= \{\, h \in F \mid h(x) \geq s \,\} \cdot g^{-1} \\
&= \varphi_s(x) \cdot g^{-1} \\
&= g(\varphi_s(x)).
\end{aligned}$$

Now we show that at least one of these homomorphisms is an embedding from $\mathbf{S}$ to $\mathbf{P}(F)$. Let $\langle x, y \rangle \in \bigcap_{s \in S} \ker \varphi_s$ be an arbitrary pair of elements. Since $\langle x, y \rangle \in \ker \varphi_x$, therefore $\varphi_x(x) = \varphi_x(y)$. We have $\mathrm{id} \in \varphi_x(x)$ by equation (1.3a), so $\mathrm{id} \in \varphi_x(y)$, thus again by equation (1.3a) we conclude that $y \geq x$. A similar argument shows that $x \geq y$, thus $x = y$. This proves that the congruence $\bigcap_{s \in S} \ker \varphi_s$ is the equality relation on $\mathbf{S}$. But $\mathbf{S}$ is subdirectly irreducible, therefore for at least one element $s \in S$ the kernel of φ_s is the equality relation. Hence φ_s is an embedding. $\square$

We have seen that every subdirectly irreducible $\mathbf{F}$-semilattice is isomorphic to some subalgebra of $\mathbf{P}(F)$. So it is natural to ask which subalgebras of $\mathbf{P}(F)$ are in fact subdirectly irreducible. The following corollary states that all finite subalgebras of $\mathbf{P}(F)$ are subdirectly irreducible. However, it is not hard to construct an example showing that the infinite subalgebras of $\mathbf{P}(F)$ are not necessarily subdirectly irreducible.

Proposition 1.4. *The finite subdirectly irreducible* $\mathbf{F}$*-semilattices are exactly the nontrivial finite subalgebras of* $\mathbf{P}(F)$.

Proof. We already know from Proposition 1.3 that the finite subdirectly irreducible $\mathbf{F}$-semilattices are subalgebras of $\mathbf{P}(F)$. Conversely, we must show that each nontrivial finite subalgebra of $\mathbf{P}(F)$ is indeed subdirectly irreducible. Let $\mathbf{U}$ be a finite subalgebra of $\mathbf{P}(F)$, and suppose that $\mathbf{U}$ has more than one element. First we will define a pair of elements in U, and subsequently we will show that every nontrivial congruence of $\mathbf{U}$ contains this pair. Clearly, this is enough to ensure that $\mathbf{U}$ is subdirectly irreducible.

Consider the pair $\langle M, \emptyset \rangle$ where

$$M = \bigcap \{\, A \in U \mid \mathrm{id} \in A \,\}. \tag{1.4a}$$

The set on the right hand side of equation (1.4a) is not empty. In order to verify this, we choose an element A of U different from the empty set. This can be done, since U has more than one element. Let a be an arbitrary element of A. From Definition 1.2 we see that $a(A) = A \cdot a^{-1}$, and since $\mathrm{id} \in A \cdot a^{-1}$, we conclude that $\mathrm{id} \in a(A)$. Therefore the set on the right hand side of equation (1.4a) contains the element $a(A)$ of U, thus it is nonempty. Furthermore, this set is finite, since U is finite. Finally, if we use the meet operation of $\mathbf{P}(F)$, we get that the set M is in U. With a similar argument it is easy to verify that the empty set is also in U. To this end we need to take the intersection of all elements of U.

Now we show that M is a subgroup of $\mathbf{F}$. It is obvious that $\mathrm{id} \in M$. Let m be an arbitrary element of M. Then $\mathrm{id} \in M \cdot m^{-1} = m(M)$, so by equation (1.4a) we get $M \cdot m^{-1} \supseteq M$. If we multiply this inclusion by m on the right, we conclude that $M \supseteq M \cdot m$ for every element m of M. Therefore M is closed under the multiplication of $\mathbf{F}$. To prove that M is closed under taking inverses also, consider the sets $M \cdot m^k$ where k is a nonnegative integer. Since $M \in U$ and $M \cdot m^k = m^{-k}(M)$, we see that these sets are elements of U. But U is finite, so there exist two distinct integers k and l, such that $M \cdot m^k = M \cdot m^l$. We can assume without loss of generality that $k > l$. Since $k - l - 1 \geq 0$ and M is a monoid, we get $m^{k-1} = m^{k-l-1} \cdot m^l \in M \cdot m^l = M \cdot m^k$, that is, $m^{-1} \in M$. Now we are ready to complete our proof.

Let ϑ be a congruence of $\mathbf{U}$ different from the equality relation. Hence we can choose a pair $\langle A, B\rangle \in \vartheta$ with $A \neq B$. Without loss of generality we can assume that $A \not\subseteq B$, thus we can choose an element $a \in A \setminus B$. For this element a we have $\mathrm{id} \in a(A)$, but $\mathrm{id} \notin a(B)$. Let

$$\langle C, D\rangle = \langle a(A) \cap M, a(B) \cap M\rangle.$$

Clearly, this pair belongs to ϑ. Furthermore, we have $\mathrm{id} \in C$ and $C \subseteq M$, thus by equation (1.4a) we conclude that C equals M. On the other hand, $\mathrm{id} \notin D$ and $D \subseteq M$. We show that D must be equal to the empty set. In order to verify this suppose that d is an arbitrary element of D. Then $\mathrm{id} \in d(D)$, and since M is a subgroup of $\mathbf{F}$, $d(D)$ is also a subset of M. In view of equation (1.4a) this means that $d(D) = M$, thus D equals M. Hence $\mathrm{id} \in D$, a contradiction. So we have shown that $\langle C, D\rangle = \langle M, \emptyset\rangle$. $\square$

We remark that we have proved more than what we stated in Proposition 1.4. Namely, in the last paragraph of the proof we have also shown that M is an atom of $\mathbf{U}$. Since the unary operations of $\mathbf{U}$ are automorphisms of the semilattice reduct of $\mathbf{U}$, we conclude that the atoms of $\mathbf{U}$ are exactly the right cosets of M. So the above proof yields also a proof for the following lemma.

Lemma 1.5. *If a subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$ contains the empty set and the set*

$$M = \bigcap\{\, A \in U \mid \mathrm{id} \in A \,\},$$

where M is a subgroup of $\mathbf{F}$, then $\mathbf{U}$ is subdirectly irreducible, and the atoms in $\mathbf{U}$ are exactly the right cosets of M. $\square$

In view of equation (1.4a) one can define the set M for each subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$, but in general M will be neither a subgroup of $\mathbf{F}$ nor an element of U. However, if $\mathbf{U}$ is the image of a subdirectly irreducible $\mathbf{F}$-semilattice under the embedding described in the proof of Proposition 1.3, then M does enjoy similar properties. Later on we will need these technical properties which are summarized in the following lemma.

Lemma 1.6. *If* $\mathbf{S}$ *is a subdirectly irreducible* $\mathbf{F}$*-semilattice, then* $\mathbf{S}$ *is isomorphic to a subalgebra* $\mathbf{U}$ *of* $\mathbf{P}(F)$*. The algebra* $\mathbf{U}$ *can be selected so that it has a unique element* $M \subseteq F$ *with the following properties:*

(1) $\mathrm{id} \in M$ *and* $M \cdot M = M$*,*

(2) $A = M \cdot A$ *for all* $A \in U$*, and*

(3) $M = \bigcap\{\, A \in U \mid \mathrm{id} \in A \,\}$.

This means that the element M of $\mathbf{U}$—considered as a subset of F—is a submonoid of $\mathbf{F}$, and every element in $\mathbf{U}$ is closed with respect to taking complex product with M. Furthermore, the element M is the least element in $\mathbf{U}$ which contains the element $\mathrm{id} \in \mathbf{F}$.

Proof. We will use the embedding φ_s which was defined in the proof of Proposition 1.3. So suppose that $\mathbf{S}$ is a subdirectly irreducible $\mathbf{F}$-semilattice, s is a fixed element of S, and φ_s is an embedding of $\mathbf{S}$ into $\mathbf{P}(F)$. Let $\mathbf{U} = \varphi_s(\mathbf{S})$ and $M = \varphi_s(s)$. Now we show that for any element $A \in U$ the equality

$$A = \{\, f \in F \mid A \supseteq M \cdot f \,\} \tag{1.6a}$$

holds. To verify this, let $a \in S$ be an element such that $\varphi_s(a) = A$. Since φ_s is an isomorphism from $\mathbf{S}$ to $\mathbf{U}$, we have

$$\begin{aligned} A &= \varphi_s(a) \\ &= \{\, f \in F \mid f(a) \geq s \,\} \\ &= \{\, f \in F \mid \varphi_s(f(a)) \supseteq \varphi_s(s) \,\} \\ &= \{\, f \in F \mid f(\varphi_s(a)) \supseteq \varphi_s(s) \,\} \\ &= \{\, f \in F \mid f(A) \supseteq M \,\} \\ &= \{\, f \in F \mid A \cdot f^{-1} \supseteq M \,\} \\ &= \{\, f \in F \mid A \supseteq M \cdot f \,\}. \end{aligned}$$

Since $M \supseteq M \cdot \mathrm{id}$, it follows from equation (1.6a) that $\mathrm{id} \in M$. Again by equation (1.6a) it is easy to see that $A \supseteq M \cdot A$ for every element $A \in U$. Finally, since $\mathrm{id} \in M$, we conclude that $A = M \cdot A$. In particular, for the element $M \in U$ this means that $M = M \cdot M$. In order to prove (3), let A be an element of U containing the element id. Then we have $A = M \cdot A \supseteq M \cdot \mathrm{id} = M$. This proves the inclusion $\subseteq$. The reverse inclusion is obvious, as M is one of the sets that are intersected on the right hand side. ☐

Corollary 1.7. *If* $\mathbf{F}$ *is a locally finite group, then, up to isomorphism, the subdirectly irreducible* $\mathbf{F}$*-semilattices are exactly those nontrivial subalgebras* $\mathbf{U}$ *of* $\mathbf{P}(F)$ *for which the set* $M = \bigcap\{\, A \in U \mid \mathrm{id} \in A \,\}$ *is an element of* $\mathbf{U}$*. Furthermore, if* $\mathbf{U}$ *satisfies this condition, then it also has the following properties:*

(1) $\emptyset \in U$,

(2) *M is a subgroup of* $\mathbf{F}$*, and*

(3) *the atoms of* $\mathbf{U}$ *are exactly the right cosets of* M*.*

Proof. In Lemma 1.6 we have proved that each subdirectly irreducible $\mathbf{F}$-semilattice is isomorphic to a subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$ such that $M \in \mathbf{U}$.

For the converse statement let $\mathbf{U}$ be a nontrivial subalgebra of $\mathbf{P}(F)$ such that $M \in \mathbf{U}$. We must show that $\mathbf{U}$ is subdirectly irreducible. From now on we will use similar ideas as in the proof of Proposition 1.4. In the same way as in that proof, we see that M is a submonoid of $\mathbf{F}$. But $\mathbf{F}$ is locally finite, therefore M must be a subgroup of $\mathbf{F}$.

Now we show that U contains the empty set. We will repeatedly use the fact that M and the elements generated by M in $\mathbf{P}(F)$ are in $\mathbf{U}$. Suppose first that $M = F$. Then for any element A of U different from the empty set and for any element $a \in A$, the set $a(A)$ is in U and $\mathrm{id} \in a(A)$. By the definition of M this means that $A = F$. But U contains more than one element, so in this case we conclude that $U = \{F, \emptyset\}$. Now let us consider the case where M is a proper subgroup of $\mathbf{F}$. Then for any element $f \in F \setminus M$ we have $f^{-1}(M) \wedge M = \emptyset$, that is, the empty set is again in U.

So far we have verified the properties (1) and (2). Now we can apply Lemma 1.5 to obtain that $\mathbf{U}$ is subdirectly irreducible and has property (3) as well. $\square$

Up to this point we have proved that every subdirectly irreducible $\mathbf{F}$-semilattice is isomorphic to some subalgebra of $\mathbf{P}(F)$. Furthermore, we have seen that the nontrivial finite subalgebras of $\mathbf{P}(F)$ are subdirectly irreducible, and if $\mathbf{F}$ is locally finite, then we have described a family of subalgebras of $\mathbf{P}(F)$ which represents all subdirectly irreducible $\mathbf{F}$-semilattices. In both of these special cases it turned out that these subdirectly irreducible subalgebras of $\mathbf{P}(F)$ contain the empty set and some subgroup M of $\mathbf{F}$. Now we will show that such an algebra is simple if and only if it consists of the empty set and the right cosets of M.

Definition 1.8. If $\mathbf{F}$ is a fixed group and M is a subgroup of $\mathbf{F}$, then let $\mathbf{S}_M$ denote the subalgebra of $\mathbf{P}(F)$, the elements of which are the empty set and the right cosets of M.

Thus the empty set is the least element in $\mathbf{S}_M$, and all the right cosets of M are atoms. The set F of unary operations of $\mathbf{S}_M$ acts as a transitive permutation group on the set of atoms. It is easy to see that each $\mathbf{S}_M$ is a simple subalgebra of $\mathbf{P}(F)$ which has a least element and some atoms. The following lemma shows that the converse statement is also true.

Lemma 1.9. *The subalgebras* $\mathbf{S}_M$ *of* $\mathbf{P}(F)$ *are, up to isomorphism, exactly those simple* $\mathbf{F}$*-semilattices that have a least element and some atoms.*

Proof. It is easy to verify that each subalgebra $\mathbf{S}_M$ is simple, and clearly contains a least element and some atoms. For the converse, let $\mathbf{S}$ be a simple $\mathbf{F}$-semilattice with a least element 0 and an atom a. By Lemma 1.6, $\mathbf{S}$ is isomorphic to some subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$. From the definition of this embedding we see that the image of 0 is the empty set. Let us denote the image of a by A. We can assume that $\mathrm{id} \in A$, because A is nonempty and for any element $f \in A$ the element $f(A)$ of $\mathbf{U}$ is an atom containing the identity. On the other hand, we also know from 1.6 that in $\mathbf{U}$ there exists a unique element M with properties (1)–(3). In particular, M is a submonoid of $\mathbf{F}$. Since $\mathrm{id} \in A$, we have $M \subseteq A$ by Lemma 1.6 (3). But A is an atom, therefore A must be equal to M, so the submonoid M is an atom in $\mathbf{U}$. Now we show that this submonoid M is actually a subgroup.

For every element $m \in M$, the set $m^{-1}(M) = M \cdot m$ is an element of $\mathbf{U}$ and a subset of M. But it cannot be a proper subset of M, because M is an atom, so $M \cdot m = M$. Therefore M is a subgroup of $\mathbf{F}$. The right cosets of M are the atoms of $\mathbf{U}$, and together with the empty set they form a subalgebra of $\mathbf{U}$ which is exactly the algebra $\mathbf{S}_M$. Our last task is now to show that $\mathbf{S}_M$ coincides with $\mathbf{U}$.

Consider the equivalence relation ϑ on U which has only one nontrivial equivalence class, namely the set S_M. We check that ϑ is a congruence relation of $\mathbf{U}$. It is clear that every unary operation of $\mathbf{U}$ preserves this relation, since S_M is a subuniverse of $\mathbf{U}$. On the other hand, we know that the elements of S_M are the least element and the atoms in $\mathbf{U}$, therefore the meet operation also preserves ϑ. Since $\mathbf{U}$ is simple, we conclude that ϑ must be the full relation on $\mathbf{U}$, so U must be equal to S_M. ☐

We have characterized the subdirectly irreducible $\mathbf{F}$-semilattices in two special cases in Proposition 1.4 and Corollary 1.7. In view of the previous lemma we can now easily characterize the simple $\mathbf{F}$-semilattices in these cases. It is enough to observe that in these cases the simple $\mathbf{F}$-semilattices contain a least element and some atoms. But this is trivial in the first case, and in the second case it follows from Corollary 1.7.

Corollary 1.10. *The finite simple* $\mathbf{F}$*-semilattices are, up to isomorphism, exactly the subalgebras* $\mathbf{S}_M$ *of* $\mathbf{P}(F)$ *where* M *runs over the subgroups of finite index of* $\mathbf{F}$. ☐

Corollary 1.11. *If* $\mathbf{F}$ *is a locally finite group, then the simple* $\mathbf{F}$*-semilattices are, up to isomorphism, exactly the subalgebras* $\mathbf{S}_M$ *of* $\mathbf{P}(F)$. ☐

The rest of this section is devoted to the description of all simple $\mathbf{F}$-semilattices in the case when $\mathbf{F}$ is a fixed commutative group. We will see that there are two types of simple $\mathbf{F}$-semilattices in this case. One of the types consists of the algebras isomorphic to $\mathbf{S}_M$, as in Corollaries 1.10 and 1.11. The other type of simple $\mathbf{F}$-semilattices will turn out to be representable by an $\mathbf{F}$-semilattice of real numbers where the unary operations act as translations. First we consider the simple $\mathbf{F}$-semilattices which have a least element.

Proposition 1.12. *If* $\mathbf{F}$ *is a commutative group, then the simple* $\mathbf{F}$*-semilattices containing a least element are, up to isomorphism, exactly the subalgebras* $\mathbf{S}_M$ *of* $\mathbf{P}(F)$.

Proof. Let $\mathbf{S}$ be a simple $\mathbf{F}$-semilattice which contains a least element. We have to prove that $\mathbf{S}$ is isomorphic to some subalgebra $\mathbf{S}_M$ of $\mathbf{P}(F)$. By Lemma 1.6, $\mathbf{S}$ is isomorphic to some subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$. Moreover, we know that $\mathbf{U}$ can be selected in such a way that it contains the empty set and a unique element M with properties (1)–(3). In particular, the element M is a submonoid of $\mathbf{F}$. Our aim is to prove that M is not only a submonoid of $\mathbf{F}$ but also a subgroup of $\mathbf{F}$. Once this is done, we can use Lemma 1.5 to show that M is actually an atom of $\mathbf{U}$, and we can complete the proof using the same argument as in the last paragraph of Lemma 1.9.

In order to prove that M is a subgroup of $\mathbf{F}$, let us introduce the notation M^{-1} for the set of inverses of the elements in M. We define a homomorphism φ from $\mathbf{U}$ to $\mathbf{P}(F)$ as follows:

$$\varphi\colon U \to P(F); \quad \varphi(A) = M^{-1} \cdot A. \tag{1.12a}$$

This mapping is compatible with all unary operations, because

$$\begin{aligned} \varphi(f(A)) &= M^{-1} \cdot f(A) \\ &= M^{-1} \cdot A \cdot f^{-1} \\ &= \varphi(A) \cdot f^{-1} \\ &= f(\varphi(A)). \end{aligned}$$

Now we have to show that

$$M^{-1} \cdot (A \cap B) = (M^{-1} \cdot A) \cap (M^{-1} \cdot B).$$

The inclusion $\subseteq$ is trivial. To prove the reverse inclusion, let us choose an element from the right hand side. So there exist elements $a \in A$, $b \in B$, $m, n \in M$ such that $m^{-1} \cdot a = n^{-1} \cdot b$. Since $\mathbf{F}$ is commutative this is equivalent to the equality $n \cdot a = m \cdot b$. But by Lemma 1.6 (2) we know that $A = M \cdot A$ and $B = M \cdot B$, hence both A and B contain the element $n \cdot a = m \cdot b$. Therefore our original element $m^{-1} \cdot a$ can be expressed in the way of $(m^{-1} \cdot n^{-1}) \cdot (n \cdot a) \in M^{-1} \cdot (A \cap B)$. So we have shown that φ is a homomorphism from $\mathbf{U}$ to $\mathbf{P}(F)$.

Clearly, $\varphi(\emptyset) = \emptyset$ and $\varphi(M) = M^{-1} \cdot M$. Since $M^{-1} \cdot M \neq \emptyset$, the kernel of the homomorphism φ cannot be the full relation. But $\mathbf{U}$ is simple, hence φ must be an embedding. Now let m be an arbitrary element of M. Since M is a submonoid, we have $M^{-1} \cdot M \cdot m = M^{-1} \cdot M$, that is, $\varphi(M \cdot m) = \varphi(M)$. However, φ is an embedding, hence $M \cdot m = M$. This means that M is a subgroup of $\mathbf{F}$, so the proof is complete. ☐

From now on we will discuss simple $\mathbf{F}$-semilattices that have no least element. We will see that they can be embedded in a special algebra which we define now.

Definition 1.13. Let $\mathbf{F}$ be a fixed commutative group. Then for every nonconstant homomorphism β from $\mathbf{F}$ to the additive group $\langle \mathbb{R}; + \rangle$ of the real numbers let us define an $\mathbf{F}$-semilattice $\mathbf{R}_\beta = \langle \mathbb{R}; \min, F \rangle$ on the set of real numbers as follows:

(1) $\min(a, b)$ is taken with respect to the natural order of $\mathbb{R}$, and

(2) $f(a) = a - \beta(f)$ for all $f \in F$ and $a, b \in \mathbb{R}$.

As we will see later, not every subalgebra of this algebra is simple; however the algebras $\mathbf{R}_\beta$ contain, up to isomorphism, all the simple $\mathbf{F}$-semilattices without least element.

Lemma 1.14. *If $\mathbf{F}$ is a fixed commutative group then every simple $\mathbf{F}$-semilattice without least element can be embedded in $\mathbf{R}_\beta$ for an appropriate nonconstant homomorphism β.*

Proof. The first step of the proof is to represent the given simple $\mathbf{F}$-semilattice, according to Lemma 1.6, as a subalgebra of $\mathbf{P}(F)$. So we have a simple subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$ without least element. Furthermore, $\mathbf{U}$ has an element M, which is actually a submonoid of $\mathbf{F}$, and in addition M has the properties described in Lemma 1.6. We will see that in this situation M must have $M \cup M^{-1} = F$. This will lead us to the proof that the semilattice order of $\mathbf{U}$ is linear, and that any two distinct element of U can be separated by a shifted image $f(M) = M \cdot f^{-1}$ of M. At this point we will choose a unit shift $e \in F$. The number $0 \in \mathbf{R}_\beta$ will correspond to M, and the integers $k \in \mathbf{R}_\beta$ to $M \cdot e^k$. After this, we will extend this correspondence to the rational numbers and then to the real numbers. Meanwhile the homomorphism β will also be discovered.

Now let us see the details.

Claim 1. $\emptyset, F \notin U$.

Since $\mathbf{U}$ has no least element, $\mathbf{U}$ cannot contain the empty set. In order to prove that $F \notin U$, suppose the contrary. To this end let ϑ be the equivalence relation on U which has only two blocks $\{F\}$ and $U \setminus \{F\}$. Clearly, ϑ is compatible with the unary operations as well as with intersection, so it is a congruence relation. Since $\mathbf{U}$ has no least element, U must be infinite. So the block $U \setminus \{F\}$ contains more than one element, and hence the congruence relation ϑ is not trivial. But this contradicts the assumption that $\mathbf{U}$ is simple.

Claim 2. *The submonoid M of $\mathbf{F}$ is not a subgroup.*

In the second last paragraph of Corollary 1.7 we have shown that if M were a subgroup of $\mathbf{F}$, then $\mathbf{U}$ would contain the empty set. But the empty set would be a least element in $\mathbf{U}$, and we know that $\mathbf{U}$ has none, therefore M cannot be a subgroup of $\mathbf{F}$.

Claim 3. $M^{-1} \cdot M = F$.

We will use the homomorphism φ defined in equation (1.12a) (the proof that φ is indeed a homomorphism works here, as well). Here the kernel of φ is not the equality relation. This is because of the fact that the submonoid M is not a subgroup. To see this, choose an element m from $M \setminus M^{-1}$. We will examine the images of M and $M \cdot m^{-1}$ under φ. Since $m^{-1} \notin M$ and $m^{-1} \in M \cdot m^{-1}$, we have $M \neq M \cdot m^{-1}$. On the other hand, the images under φ are $\varphi(M) = M^{-1} \cdot M$ and $\varphi(M \cdot m^{-1}) = M^{-1} \cdot M \cdot m^{-1}$, respectively. But the set $M^{-1} \cdot M$ is a subgroup of $\mathbf{F}$, because $\mathbf{F}$ is commutative and M is a submonoid. Therefore $\varphi(M) = \varphi(M \cdot m^{-1})$. This shows that φ cannot be an embedding, hence it must be a constant homomorphism, since its domain is the simple algebra $\mathbf{U}$.

If f is an arbitrary element of F, the sets M and $f(M) = M \cdot f^{-1}$ are elements of U, so their images under φ are equal. This means that $M^{-1} \cdot M = M^{-1} \cdot M \cdot f^{-1}$ for every element $f \in F$. Since $M^{-1} \cdot M$ is a subgroup of $\mathbf{F}$, $f^{-1} \in M^{-1} \cdot M$ for every element $f \in F$, that is, $M^{-1} \cdot M = F$.

Claim 4. $F = M \cup M^{-1}$.

Let us suppose the contrary. So, we can take an element $r \in F$ such that neither r nor r^{-1} is in M. This will lead to a contradiction. First of all we will define a sequence a_i $(i = 1, 2, \dots)$ in M. Since $M^{-1} \cdot M = F$, we know that for an arbitrary element $f \in F$ there exist elements $a, b \in M$ such that $f = a^{-1} \cdot b$. In other words, for every element $f \in F$ there exists an element $a \in M$ such that $f \cdot a \in M$. We can apply this argument several times to define the elements a_i $(i = 1, 2, \dots)$ in such a way that

$$\begin{array}{lcr} a_1 \in M & \text{with} & r \cdot a_1 \in M, \\ a_2 \in M & \text{with} & r^2 \cdot a_1 \cdot a_2 \in M, \\ \vdots & & \vdots \\ a_i \in M & \text{with} & r^i \cdot a_1 \cdot \ldots \cdot a_i \in M, \end{array}$$

Furthermore, we require that the choice $a_i = \mathrm{id}$ has to be made whenever $r^i \cdot a_1 \cdot \ldots \cdot a_{i-1} \in M$.

Now we define a homomorphism $\psi \colon \mathbf{U} \to \mathbf{P}(F)$ by setting

$$\psi(A) = \{\, f \in F \mid f \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) \in A \text{ for almost all natural numbers } i \,\}.$$

It is easy to see that this mapping is compatible with the unary operations as well as with intersection. Now we show that this mapping is not injective; namely, we have

$$\psi(M) = \psi(M \cap M \cdot r).$$

The sets M and $M \cap M \cdot r$ are distinct elements of U, because the first one contains id, while the other one does not, since $r^{-1} \notin M$.

In order to see that the images are equal, take an element f from $\psi(M)$. This means that $f \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) \in M$ for almost all i. Therefore there exists a natural number k such that this condition holds for every $i \geq k$. If $f \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) \in M$, then let us multiply each side by $r \cdot a_{i+1}$, and we get

$f \cdot (r^{i+1} \cdot a_1 \cdot \ldots \cdot a_i \cdot a_{i+1}) \in M \cdot a_{i+1} \cdot r$. But we know that $a_{i+1} \in M$ and M is a submonoid, so we get $M \cdot a_{i+1} \subseteq M$. Therefore $f \cdot (r^{i+1} \cdot a_1 \cdot \ldots \cdot a_{i+1}) \in M \cdot r$. To sum it up, we know that $f \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) \in M \cdot r$ if $i > k$. But the element $f \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i)$ is in M, hence it is in $M \cap M \cdot r$, too. This proves the inclusion $\psi(M) \subseteq \psi(M \cap M \cdot r)$. The reverse inclusion is trivial, since $M \cap M \cdot r$ is a subset of M.

So far we have proved that ψ is a homomorphism from $\mathbf{U}$ to $\mathbf{P}(F)$, and it is not an embedding. Since the algebra $\mathbf{U}$ is simple, we conclude that ψ must be a constant mapping. The question is which element of $\mathbf{P}(F)$ is assigned by ψ to the elements of U. Since ψ is a homomorphism, this element must form a one element subalgebra of $\mathbf{P}(F)$. But because of the unary operations, there are only two such subalgebras of $\mathbf{P}(F)$, namely $\{\emptyset\}$ and $\{F\}$. From the definition of ψ we see that $\psi(M)$ contains id, hence we conclude that $\psi(M) = F$.

In particular, the element r is in $\psi(M)$. This means that there exists a natural number k such that $r \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) \in M$ for every $i \geq k$. But this shows that we have chosen id when we defined the element a_{i+1}. Therefore we conclude that $a_{k+1} = a_{k+2} = \cdots = \mathrm{id}$. Since $\psi(M) = F$, the element $(a_1 \cdot a_2 \cdot \ldots \cdot a_k)^{-1}$ is also in $\psi(M)$. This means that there exists a natural number l such that $(a_1 \cdot a_2 \cdot \ldots \cdot a_k)^{-1} \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) \in M$ for every $i \geq l$. We can assume without loss of generality that $l > k$. This shows that $M \ni (a_1 \cdot a_2 \cdot \ldots \cdot a_k)^{-1} \cdot (r^i \cdot a_1 \cdot \ldots \cdot a_i) = r^i \cdot a_{k+1} \cdot \ldots \cdot a_i = r^i$ for every $i \geq l$.

Up to this point we have proved the following statement. If neither r nor r^{-1} is in M, then there exists a natural number l such that $r^l, r^{l+1}, \dots \in M$. If we switch the role of r and r^{-1}, we get in the same way another natural number j such that $r^{-j}, r^{-j-1}, \dots \in M$. Now choose a natural number i greater than both k and l. Then r^{i+1} and r^{-i} are elements of M, and since M is a submonoid of $\mathbf{F}$, we get $r = r^{i+1} \cdot r^{-i} \in M$. But this contradicts our assumption that M contains neither r nor r^{-1}.

Claim 5. *Set inclusion yields a linear order on $\mathbf{U}$. Furthermore if A and B are two elements of U such that $A \not\subseteq B$, then for any element $a \in A \setminus B$ we have $B \subseteq M \cdot a \subseteq A$.*

Clearly, the second statement implies the first. In order to prove the second statement, consider elements $A, B \in U$ and $a \in A \setminus B$. From Lemma 1.6 we know that $M \cdot A = A$, so $M \cdot a \subseteq A$. Now suppose that the other inclusion does not hold, that is, there exists an element $b \in B \setminus M \cdot a$. Thus $b \cdot a^{-1} \in B \cdot a^{-1} \setminus M$. By Claim 4 we get that the element $b \cdot a^{-1}$ must be in M^{-1}, so $a \cdot b^{-1} \in M$. Thus $a = (a \cdot b^{-1}) \cdot b \in M \cdot B = B$, and this is a contradiction. So we conclude that $B \subseteq M \cdot a$.

At this stage of the proof we can indicate how the homomorphism $\beta \colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ will be defined. We have the subset M of F which divides F into two parts. Those elements of F which lie in M will be mapped by β to nonpositive real numbers; and those which lie in M^{-1}, to the positive ones. The kernel of β will be the subgroup $M \cap M^{-1}$ of $\mathbf{F}$. Now we take an element e which will be mapped by β to the number 1. So let us choose and fix an element e from $M^{-1} \setminus M$. This can be done, since M is not a subgroup of F. Since β is to be a homomorphism, for any integer k the elements of $M \cdot e^k$ must correspond to real numbers not greater than k. This suggests the conjecture that every element of F will be an element of $M \cdot e^k$ for some integer k.

Claim 6. $\bigcup_{k\in\mathbb{Z}} M \cdot e^k = F.$

We will define again a homomorphism η from $\mathbf{U}$ to $\mathbf{P}(F)$. For any element $A \in U$ let

$$\eta(A) = \bigcup_{k\in\mathbb{Z}} A \cdot e^k.$$

It is easy to see that this mapping is compatible with the unary operations, since $\mathbf{F}$ is commutative. To prove that η is compatible with the intersection as well, we have to show that

$$\bigcup_{k\in\mathbb{Z}} (A \cap B) \cdot e^k = \left(\bigcup_{k\in\mathbb{Z}} A \cdot e^k\right) \cap \left(\bigcup_{k\in\mathbb{Z}} B \cdot e^k\right).$$

The inclusion $\subseteq$ is trivial. To prove the reverse inclusion, take an arbitrary element from the right hand side. So there exist elements $a \in A, b \in B$ and integers $k, l \in \mathbb{Z}$ such that $a \cdot e^k = b \cdot e^l$. We can assume that $k \leq l$. Since $e \in M^{-1}$, we get that $e^{k-l} \in M$. From Lemma 1.6 we know that $A = M \cdot A$, hence the element $a \cdot e^{k-l}$ belongs to A. But from the equality $a \cdot e^{k-l} \cdot e^l = a \cdot e^k = b \cdot e^l$ we get $a \cdot e^{k-l} = b \in A \cap B$, therefore the element $a \cdot e^{k-l} \cdot e^l = b \cdot e^l$ is in $(A \cap B) \cdot e^l$.

The homomorphism η cannot be injective, since $\eta(M) = \eta(M \cdot e)$ but $M \neq M \cdot e$ (as $e \in M \cdot e \setminus M$). But $\mathbf{U}$ is simple, therefore η is a constant mapping. The same argument as before for ψ yields that η maps each element of U to F. In particular, $\eta(M) = F$, which is what we wanted to prove.

Claim 7. *For any integer k we have* $\mathrm{id} \in M \cdot e^k$ *iff* $k \geq 0$.

This claim is an immediate consequence of the facts that $e \in M^{-1} \setminus M$ and that M is a submonoid of $\mathbf{F}$.

Now we can define the homomorphism $\beta \colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$. For any element $a \in F$ let

$$\beta(a) = \inf\left\{ \frac{k}{l} \in \mathbb{Q} \,\middle|\, k \in \mathbb{Z},\, l \in \mathbb{N} \text{ and } a^l \in M \cdot e^k \right\}. \tag{1.14a}$$

Claim 8. *The mapping β is a nonconstant homomorphism from* $\mathbf{F}$ *to* $\langle \mathbb{R}; + \rangle$. *Furthermore,*

(1) *$\beta(e^i) = i$ for any integer i, and*

(2) *$\beta(m) \leq 0$ for every element $m \in M$.*

To see that β is well defined, we have to check that for every element $a \in F$ the set on the right hand side of equation (1.14a) is nonempty, and has a lower bound. So let a be an arbitrary element of F. By Claim 6 we get an integer k such that $a \in M \cdot e^k$, therefore the set on the right hand side of equation (1.14a) contains k. Again by Claim 6 we get another integer i such that $a^{-1} \in M \cdot e^i$. Since M is closed under multiplication, we get $a^{-l} \in M \cdot e^{il}$ for any natural number l. If for some integer k we have $a^l \in M \cdot e^k$, then $\mathrm{id} = a^l \cdot a^{-l} \in M \cdot e^k \cdot M \cdot e^{il} = M \cdot e^{k+il}$, hence by Claim 7 the exponent $k + il$ is nonnegative. This implies that $k/l \geq -i$, therefore the integer $-i$ is a lower bound for the rational numbers belonging to the set in equation (1.14a).

Now we show that $\beta(e^i) = i$ for any integer i. It is clear that $e^i \in M \cdot e^i$, hence from equation (1.14a) we get $\beta(e^i) \leq i/1 = i$. Now suppose that $(e^i)^l \in M \cdot e^k$ for some integer k and natural number l. Thus $\mathrm{id} \in M \cdot e^{k-il}$, and by Claim 7 we get $k/l \geq i$. This shows that $\beta(e^i) = i$.

From the definition of β it is clear that $\beta(m) \leq 0$ for every element $m \in M$, since we can choose 0 for k and 1 for l.

Now we prove that $\beta(a^{-1}) \leq -\beta(a)$ for every element $a \in F$. To this end let ε be an arbitrary small positive real number, and let us choose the numbers k and l such that $\beta(a) - \varepsilon \leq k/l < \beta(a)$. From $k/l < \beta(a)$ we know that $a^l \notin M \cdot e^k$. Using the facts that M is a submonoid of the commutative group F and that $M \cup M^{-1} = F$, we get

$$\begin{aligned}
a^l \notin M \cdot e^k &\Rightarrow a^l \cdot e^{-k} \notin M \\
&\Rightarrow a^l \cdot e^{-k} \in M^{-1} \\
&\Rightarrow a^{-l} \cdot e^{k} \in M \\
&\Rightarrow a^{-l} \in M \cdot e^{-k} \\
&\Rightarrow (a^{-1})^l \in M \cdot e^{-k}.
\end{aligned}$$

But according to equation (1.14a) this means that $\beta(a^{-1}) \leq -k/l$. Since we have chosen the numbers k and l such that $-k/l \leq -\beta(a) + \varepsilon$, we get $\beta(a^{-1}) \leq -\beta(a) + \varepsilon$. But this holds for every positive real number ε, therefore it must hold for zero, that is, $\beta(a^{-1}) \leq -\beta(a)$.

To prove that β is compatible with multiplication, let $a, b \in F$ and let ε be an arbitrary small positive real number. From the definition of β we get two pairs k_1, l_1 and k_2, l_2 of integers such that $l_1, l_2 > 0$ and

$$\begin{aligned}
\beta(a) \leq \frac{k_1}{l_1} \leq \beta(a) + \varepsilon \quad &\text{where} \quad a^{l_1} \in M \cdot e^{k_1}, \text{ and} \\
\beta(b) \leq \frac{k_2}{l_2} \leq \beta(b) + \varepsilon \quad &\text{where} \quad b^{l_2} \in M \cdot e^{k_2}.
\end{aligned}$$

Since M is a submonoid, raising $a^{l_1} \in M \cdot e^{k_1}$ to the l_2th power yields $a^{l_1 l_2} \in M \cdot e^{k_1 l_2}$. Similarly $b^{l_1 l_2} \in M \cdot e^{l_1 k_2}$, and by multiplication we conclude that $(a \cdot b)^{l_1 l_2} \in M \cdot e^{k_1 l_2 + l_1 k_2}$. By the definition of β this means that

$$\beta(a \cdot b) \leq \frac{k_1 l_2 + l_1 k_2}{l_1 l_2} = \frac{k_1}{l_1} + \frac{k_2}{l_2} \leq \beta(a) + \beta(b) + 2\varepsilon.$$

But ε was again an arbitrary positive real number, hence it follows that $\beta(a \cdot b) \le \beta(a) + \beta(b)$. Finally, the inequalities below prove that $\beta(a \cdot b) = \beta(a) + \beta(b)$ and $\beta(a^{-1}) = -\beta(a)$:

$$\begin{aligned}\beta(a \cdot b) &\le \beta(a) + \beta(b)\\ &= \beta(a) + \beta(a^{-1} \cdot a \cdot b)\\ &\le \beta(a) + \beta(a^{-1}) + \beta(a \cdot b)\\ &\le \beta(a) - \beta(a) + \beta(a \cdot b)\\ &= \beta(a \cdot b).\end{aligned}$$

Now we can define an embedding $\xi \colon \mathbf{U} \to \mathbf{R}_\beta$ which will complete the proof of the lemma. For any element $A \in U$ let

$$\xi(A) = \sup\{\, \beta(a) \mid a \in A \,\}. \tag{1.14b}$$

Claim 9. *The mapping ξ is an embedding of $\mathbf{U}$ in $\mathbf{R}_\beta$. Furthermore, $\xi(M \cdot f) = \beta(f)$ for every element $f \in F$.*

To see that ξ is well defined, we have to check that for every element $A \in U$ the set on the right hand side of equation (1.14b) has an upper bound. By Claim 1 we have $A \neq \emptyset$, and we can choose an element $f \in F \setminus A$ for every element $A \in U$. Since $f \in M \cdot f \setminus A$, by Claim 5 we get $A \subseteq M \cdot f$. So we conclude that if $\xi(M \cdot f)$ exists, then $\xi(A)$ also exists, by the definition of ξ, and $\xi(A) \le \xi(M \cdot f)$.

Now we prove that $\xi(M \cdot f) = \beta(f)$. From Claim 8 we know that β is a homomorphism, and $\beta(m) \le 0$ for every element $m \in M$. Hence for every element $m \cdot f$ of $M \cdot f$ we have

$$\beta(m \cdot f) = \beta(m) + \beta(f) \le 0 + \beta(f) = \beta(f).$$

Therefore $\xi(M \cdot f) \le \beta(f)$. But $f \in M \cdot f$, so $\xi(M \cdot f) \ge \beta(f)$, hence $\xi(M \cdot f) = \beta(f)$.

In order to prove that ξ is compatible with the semilattice operation, let A, B be arbitrary elements in U. By Claim 5 we can assume that $A \subseteq B$. But from this we get $\xi(A) \le \xi(B)$, and hence

$$\xi(A \cap B) = \xi(A) = \min(\xi(A), \xi(B)).$$

Now we are going to show that ξ is compatible with the unary operations as well. For arbitrary elements $A \in U$ and $f \in F$ we have

$$\begin{aligned}\xi(f(A)) &= \xi(A \cdot f^{-1})\\ &= \sup\{\, \beta(b) \mid b \in A \cdot f^{-1} \,\}\\ &= \sup\{\, \beta(a \cdot f^{-1}) \mid a \in A \,\}\\ &= \sup\{\, \beta(a) + \beta(f^{-1}) \mid a \in A \,\}\\ &= \sup\{\, \beta(a) \mid a \in A \,\} + \beta(f^{-1})\\ &= \xi(A) + \beta(f^{-1})\\ &= \xi(A) - \beta(f)\\ &= f(\xi(A)).\end{aligned}$$

So we conclude that ξ is a homomorphism from $\mathbf{U}$ to $\mathbf{R}_\beta$. Since $\xi(M \cdot e^k) = \beta(e^k) = k$ for every integer k, ξ cannot be a constant mapping. But $\mathbf{U}$ is simple, hence ξ is an embedding. $\square$

The next example shows that for a homomorphism $\beta\colon \mathbf{F} \to \mathbb{R}$, a subalgebra $\mathbf{S}$ of $\mathbf{R}_\beta$ is not necessarily simple. This will help us to describe the simple subalgebras of $\mathbf{R}_\beta$.

Example 1.15. *Let* $\mathbf{F}$ *be the additive group* $\langle \mathbb{Z}; + \rangle$ *of the integers and* $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ *be the identical embedding. Then the subalgebra* $\mathbf{S}$ *of* $\mathbf{R}_\beta$ *with the underlying set*

$$S = \left\{ \frac{a}{2} \in \mathbb{R} \mid a \in \mathbb{Z} \right\}$$

is not simple.

Proof. Clearly, the subset S of $\mathbb{R}$ is closed under the operation of subtracting any integer $\beta(i) = i$ ($i \in \mathbb{Z}$), that is, it is closed under the unary operations of $\mathbf{R}_\beta$. In addition, S is also closed under the binary operation of taking the minimum. Therefore $\mathbf{S}$ is a subalgebra of $\mathbf{R}_\beta$.

Now we construct a nontrivial congruence relation ϑ on S which will yield that $\mathbf{S}$ is not simple. Let ϑ be the equivalence relation on S whose blocks are the two-element sets $\{i, i + 1/2\}$, where $i \in \mathbb{Z}$. Clearly, this relation is compatible with the operations of $\mathbf{S}$. $\square$

Now we will show that if the image of β contains arbitrary small positive real numbers, then every subalgebra of $\mathbf{R}_\beta$ is simple. Let us define this property of β exactly.

Definition 1.16. A homomorphism $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ is called *dense* if for each real number $\varepsilon > 0$ there exists an element $f \in F$ such that $0 < \beta(f) \le \varepsilon$.

Lemma 1.17. *If* $\mathbf{F}$ *is a commutative group and* $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ *is a dense homomorphism, then every subalgebra of* $\mathbf{R}_\beta$ *is simple.*

Proof. Let $\mathbf{S}$ be a subalgebra of $\mathbf{R}_\beta$. We will prove that every pair of two distinct real numbers x, y in $\mathbf{S}$ generates the full congruence of $\mathbf{S}$. Clearly, this ensures that $\mathbf{S}$ is simple. So let ϑ denote the congruence relation on $\mathbf{S}$ generated by the pair $\langle x, y \rangle$. We may assume that $x < y$. Since β is dense, there exists an element $e \in F$ such that $0 < \beta(e) \le y - x$. Let $\varepsilon = \beta(e) > 0$, and $z = x + \varepsilon$. The number z is in S, because

$$z = x + \varepsilon = x + \beta(e) = x - \beta(e^{-1}) = e^{-1}(x) \in S.$$

Since the pairs $\langle x, y \rangle$ and $\langle z, z \rangle$ are in ϑ, we have

$$\vartheta \ni \langle \min(x, z), \min(y, z) \rangle = \langle x, z \rangle = \langle x, x + \varepsilon \rangle.$$

If we apply the unary operation $e^{-k} \in F$ to the pair $\langle x, x+\varepsilon\rangle$ for some integer k, we get

$$\begin{aligned}\vartheta &\ni \langle e^{-k}(x), e^{-k}(x+\varepsilon)\rangle \\ &= \langle x - \beta(e^{-k}), x+\varepsilon-\beta(e^{-k})\rangle \\ &= \langle x + \beta(e^{k}), x+\varepsilon+\beta(e^{k})\rangle \\ &= \langle x + k\varepsilon, x+\varepsilon+k\varepsilon\rangle \\ &= \langle x + k\varepsilon, x+(k+1)\varepsilon\rangle.\end{aligned}$$

Since ϑ is transitive, we conclude that $\langle x+k\varepsilon, x+l\varepsilon\rangle \in \vartheta$ for any two integers k, l.

Now we prove that every pair $\langle r, s\rangle \in S\times S$ belongs to ϑ. Since $\varepsilon > 0$, we can choose two integers k, l such that $x+k\varepsilon < r, s < x+l\varepsilon$. Hence we have

$$\begin{aligned}\vartheta &\ni \langle \min(x+k\varepsilon, r), \min(x+l\varepsilon, r)\rangle = \langle x+k\varepsilon, r\rangle, \text{ and} \\ \vartheta &\ni \langle \min(x+k\varepsilon, s), \min(x+l\varepsilon, s)\rangle = \langle x+k\varepsilon, s\rangle.\end{aligned}$$

Finally, the symmetry and the transitivity of ϑ yields $\langle r, s\rangle \in \vartheta$. □

Let us examine the case when β is not dense. It turns out that in this case $\mathbf{R}_\beta$ contains, up to isomorphism, only one simple subalgebra, which has the following structure.

Definition 1.18. Let $\mathbf{F}$ be a fixed commutative group. Then for every surjective homomorphism α from $\mathbf{F}$ onto the additive group $\langle \mathbb{Z}; +\rangle$ of the integers let $\mathbf{Z}_\alpha = \langle \mathbb{Z}; \min, F\rangle$ be the $\mathbf{F}$-semilattice defined on the set of integers as follows:

(1) $\min(a, b)$ is taken with respect to the natural order of $\mathbb{Z}$, and

(2) $f(a) = a - \alpha(f)$ for all $f \in F$ and $a, b \in \mathbb{Z}$.

Lemma 1.19. *If $\mathbf{F}$ is a commutative group and $\alpha\colon \mathbf{F} \to \langle \mathbb{Z}; +\rangle$ is a surjective homomorphism, then the $\mathbf{F}$-semilattice $\mathbf{Z}_\alpha$ is simple.*

Proof. The proof is the same as that of Lemma 1.17, except that the role of ε should be now played by 1. Since α is surjective, we can find an element $e \in F$ such that $\alpha(e) = \varepsilon = 1$. □

Lemma 1.20. *If $\beta\colon \mathbf{F} \to \langle \mathbb{R}; +\rangle$ is a nonconstant and nondense homomorphism, then there exists a positive real number ε such that the mapping $\alpha\colon f \mapsto \beta(f)/\varepsilon$ is a surjective homomorphism of $\mathbf{F}$ onto $\langle \mathbb{Z}; +\rangle$. Furthermore, every simple subalgebra of $\mathbf{R}_\beta$ is isomorphic to $\mathbf{Z}_\alpha$.*

Proof. Since β is not constant, the real number

$$\varepsilon = \inf\{\, \beta(f) \mid f \in F \text{ and } \beta(f) > 0\,\} \tag{1.20a}$$

is well defined. The homomorphism β is not dense, thus $\varepsilon > 0$.

Now we show that there exists an element $e \in F$ such that $\beta(e) = \varepsilon$. Since $\varepsilon > 0$, by equation (1.20a) we can choose an element $e \in F$ such that $\varepsilon \leq \beta(e) < 2\varepsilon$. If $\beta(e) \neq \varepsilon$, then we can again find an element $f \in F$ such that $\varepsilon \leq \beta(f) < \beta(e) < 2\varepsilon$. Hence $0 < \beta(e) - \beta(f) < \varepsilon$. But β is a homomorphism, therefore $\beta(e \cdot f^{-1}) = \beta(f) - \beta(e)$. So we have found an element $e \cdot f^{-1} \in F$ such that $0 < \beta(e \cdot f^{-1}) < \varepsilon$, which contradicts the definition of ε. Therefore we conclude that $\beta(e) = \varepsilon$.

Now we prove that $\beta(f)/\varepsilon \in \mathbb{Z}$ for every element $f \in F$. This will ensure that α assigns integers to the elements of F. Let $f \in F$ be an arbitrary element. Since $\varepsilon > 0$, we can choose an integer k such that $k\varepsilon \leq \beta(f) < (k+1)\varepsilon$. But $\beta(e^k) = k\beta(e) = k\varepsilon$, therefore $0 \leq \beta(f) - k\varepsilon = \beta(a \cdot e^{-k}) < \varepsilon$. By the definition of ε we get $0 = \beta(f) - k\varepsilon$, that is, $\beta(f)/\varepsilon \in \mathbb{Z}$. Since $\beta(e^k) = k\varepsilon$ for every integer k, we conclude that the mapping α of F into $\mathbb{Z}$ is surjective. Finally, since β is a homomorphism, α is also a homomorphism.

To complete the proof, it remains to be checked that if $\mathbf{S}$ is a simple subalgebra of $\mathbf{R}_\beta$, then it is isomorphic to $\mathbf{Z}_\alpha$. To this end let us choose an arbitrary element $s \in S$. Now we define a mapping φ of $\mathbf{S}$ into $\mathbf{Z}_\alpha$, and subsequently we show that φ is a surjective homomorphism. For any number $a \in S$ let

$$\varphi(a) = \lfloor (a-s)/\varepsilon \rfloor.$$

Clearly, this mapping is order preserving, and for any integer k we have

$$\begin{aligned}
\varphi(e^k(a)) &= \varphi(a - \beta(e^k)) \\
&= \varphi(a - k\varepsilon) \\
&= \lfloor (a - k\varepsilon - s)/\varepsilon \rfloor \\
&= \lfloor (a-s)/\varepsilon - k \rfloor \\
&= \lfloor (a-s)/\varepsilon \rfloor - k.
\end{aligned}$$

Thus φ is surjective. Since $\alpha(f) \in \mathbb{Z}$ for any unary operation $f \in F$,

$$\begin{aligned}
f(\varphi(a)) &= f(\lfloor (a-s)/\varepsilon \rfloor) \\
&= \lfloor (a-s)/\varepsilon \rfloor - \alpha(f) \\
&= \lfloor (a-s)/\varepsilon - \alpha(f) \rfloor \\
&= \lfloor (a-s)/\varepsilon - \beta(f)/\varepsilon \rfloor \\
&= \lfloor (a - \beta(f) - s)/\varepsilon \rfloor \\
&= \lfloor (f(a) - s)/\varepsilon \rfloor \\
&= \varphi(f(a)).
\end{aligned}$$

Hence φ is a surjective homomorphism of $\mathbf{S}$ onto $\mathbf{Z}_\alpha$. But $\mathbf{S}$ is simple, therefore φ is an isomorphism. □

Now we can summarize the results in Proposition 1.12 and Lemmas 1.14 through 1.20 to give a characterization of all simple $\mathbf{F}$-semilattices for a commutative group $\mathbf{F}$.

Theorem 1.21. *If* $\mathbf{F}$ *is a commutative group, then every simple* $\mathbf{F}$*-semilattice is isomorphic to one of the following algebras:*

(1) $\mathbf{S}_M$*, where* M *is a subgroup of* $\mathbf{F}$*,*

(2) $\mathbf{Z}_\alpha$*, where* $\alpha\colon \mathbf{F} \to \langle \mathbb{Z}; + \rangle$ *is a surjective group homomorphism, and*

(3) *the subalgebras of* $\mathbf{R}_\beta$*, where* $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ *is a dense group homomorphism.*

Furthermore, these simple $\mathbf{F}$*-semilattices are pairwise nonisomorphic, except for the case when* β_1, β_2 *are dense homomorphisms,* $\mathbf{S}_1, \mathbf{S}_2$ *are subalgebras of* $\mathbf{R}_{\beta_1}, \mathbf{R}_{\beta_2}$ *respectively, and there exist real numbers* $t > 0$ *and* d *such that* $\beta_2 = t\beta_1$ *and* $S_2 = tS_1 + d$*.*

Proof. Let $\mathbf{F}$ be a fixed commutative group. First of all we know that the $\mathbf{F}$-semilattices listed in (1), (2) and (3) are simple (use Lemmas 1.9, 1.19 and 1.17, respectively). Our task is now to prove that each simple $\mathbf{F}$-semilattice $\mathbf{S}$ is isomorphic to one of these.

If $\mathbf{S}$ has a least element, then according to Proposition 1.12, $\mathbf{S}$ is isomorphic to some algebra listed in (1). Now suppose that $\mathbf{S}$ has no least element. By Lemma 1.14 we can assume that $\mathbf{S}$ is a subalgebra of $\mathbf{R}_\beta$ for an appropriate nonconstant homomorphism $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$. If β is dense, then $\mathbf{S}$ is one of the algebras listed in (3). If β is not dense, then by Lemma 1.20, $\mathbf{S}$ is isomorphic to some algebra listed in (2). So we have proved the first part of the theorem.

In the rest of the proof we will show that the given algebras in (1), (2) and (3) are pairwise nonisomorphic, except for the special cases indicated above. Since the algebras in (a) have a least element, while the algebras in (2) and (3) have not, the algebras in (1) cannot be isomorphic to any algebra in (2) or (3). Now we show that distinct algebras in (1) are nonisomorphic; that is, if M_1 and M_2 are distinct subgroups of $\mathbf{F}$, then $\mathbf{S}_{M_1} \not\cong \mathbf{S}_{M_2}$. We can assume that $M_2 \not\subseteq M_1$, so we can choose an element $f \in M_1 \setminus M_2$. We recall that if two algebras are isomorphic then the same identities hold in them. The identity $x \wedge f(x) = x$ holds in $\mathbf{S}_{M_1}$, since $\emptyset \cap f(\emptyset) = \emptyset$, and for each element $M_1 \cdot a \in S_{M_1}$ we have

$$\begin{aligned} M_1 \cdot a \cap f(M_1 \cdot a) &= M_1 \cdot a \cap M_1 \cdot a \cdot f^{-1} \\ &= M_1 \cdot a \cap M_1 \cdot f^{-1} \cdot a \\ &= M_1 \cdot a \cap M_1 \cdot a \\ &= M_1 \cdot a. \end{aligned}$$

On the other hand, the identity $x \wedge f(x) = x$ does not hold in $\mathbf{S}_{M_2}$, since $M_2 \neq M_2 \cdot f^{-1}$ and $M_2 \cap f(M_2) = M_2 \cap M_2 \cdot f^{-1} = \emptyset$. Hence we conclude that $\mathbf{S}_{M_1}$ and $\mathbf{S}_{M_2}$ are nonisomorphic.

Let $\mathbf{Z}_\alpha$ be an arbitrary algebra from (2). Then for any two integers $a, b \in Z_\alpha$ there are only finitely many elements in Z_α that are between a and

b with respect to the natural order induced by the meet operation. However, if $\mathbf{S}$ is a subalgebra of $\mathbf{R}_\beta$, that is, if $\mathbf{S}$ is an algebra from (3), then for any two different real numbers $a, b \in R_\beta$ there are infinitely many elements in R_β that are between a and b, because β is dense. This implies that the algebras in (2) are not isomorphic to any algebra in (3).

Now we will show that if α_1 and α_2 are distinct surjective homomorphisms of $\mathbf{F}$ onto $\langle \mathbb{Z}; + \rangle$, then $\mathbf{Z}_{\alpha_1} \not\cong \mathbf{Z}_{\alpha_2}$. Since $\alpha_1 \neq \alpha_2$, we can choose an element $f \in F$ such that $\alpha_1(f) \neq \alpha_2(f)$. If either $\alpha_1(f)$ or $\alpha_2(f)$ is zero, then we can assume that $\alpha_1(f) = 0 \neq \alpha_2(f)$, and we will examine the identity $f(x) = x$. If $\alpha_1(f)$ and $\alpha_2(f)$ have opposite signs, then we can assume that $\alpha_1(f) < 0 < \alpha_2(f)$, and we examine the identity $x \wedge f(x) = x$. It is easy to check that in these cases the identities hold in $\mathbf{Z}_{\alpha_1}$ but they fail in $\mathbf{Z}_{\alpha_2}$, thus $\mathbf{Z}_{\alpha_1} \not\cong \mathbf{Z}_{\alpha_2}$. For example the identity $x \wedge f(x) = x$ holds in $\mathbf{Z}_{\alpha_1}$, because $\alpha_1(f) < 0$ and $f(x) = x - \alpha_1(f) > x$.

Now let us examine the case when $\alpha_1(f)$ and $\alpha_2(f)$ have the same sign. We can assume that $|\alpha_1(f)| > |\alpha_2(f)| > 0$. Since α_1 is surjective, we can choose an element $e \in F$ such that $\alpha_1(e) = 1$. We know that $\alpha_1(f)$ is an integer, so let $g = f \cdot e^{-\alpha_1(f)} \in F$. Hence we have

$$\begin{aligned}
\alpha_1(g) &= \alpha_1(f \cdot e^{-\alpha_1(f)}) \\
&= \alpha_1(f) + \alpha_1(e^{-\alpha_1(f)}) \\
&= \alpha_1(f) + (-\alpha_1(f))\alpha_1(e) \\
&= \alpha_1(f) - \alpha_1(f)\alpha_1(e) \\
&= \alpha_1(f) - \alpha_1(f) \\
&= 0,
\end{aligned}$$

and similarly

$$\alpha_2(g) = \alpha_2(f) - \alpha_1(f)\alpha_2(e).$$

It is easy to see that $\alpha_2(g) \neq 0$, since $|\alpha_1(f)| > |\alpha_2(f)| > 0$ and $\alpha_2(e)$ is an integer. So we have found again an element $g \in F$ such that $\alpha_1(g) = 0 \neq \alpha_2(g)$. Hence the identity $g(x) = x$ holds in $\mathbf{Z}_{\alpha_1}$ but fails in $\mathbf{Z}_{\alpha_2}$. Thus we conclude that the algebras listed in (2) are pairwise nonisomorphic.

In order to complete the proof, we have to show that the only possibility for two algebras from (3) to be isomorphic is the case indicated in the statement of the theorem. Let β_1, β_2 be dense homomorphisms from $\mathbf{F}$ to $\langle \mathbb{R}; + \rangle$, and $\mathbf{S}_1$, $\mathbf{S}_2$ be subalgebras of $\mathbf{R}_{\beta_1}$, $\mathbf{R}_{\beta_1}$, respectively. If $t > 0$ and d are real numbers such that $\beta_2 = t\beta_1$ and $S_2 = tS_1 + d$, then let us define an isomorphism $\tau \colon \mathbf{R}_{\beta_1} \to \mathbf{R}_{\beta_2}$ by

$$\tau(x) = tx + d.$$

This mapping is indeed an isomorphism, since it is bijective, it preserves the natural order, and for any unary operation $f \in F$ and real number x we have

$$\begin{aligned}
f(\tau(x)) &= \tau(x) - \beta_2(f) \\
&= tx + d - t\beta_1(f) \\
&= t(x - \beta_1(f)) + d \\
&= t \cdot f(x) + d \\
&= \tau(f(x)).
\end{aligned}$$

Now it is easy to see that the restriction of τ to $\mathbf{S}_1$ is an isomorphism between $\mathbf{S}_1$ and $\mathbf{S}_2$.

Conversely, let $\iota\colon \mathbf{S}_1 \to \mathbf{S}_2$ be an isomorphism. Since β_1 is dense, we can choose an element $f \in F$ such that $\beta_1(f) > 0$. If $\beta_2(f) \leq 0$, then in $\mathbf{S}_2$ we have $f(x) = x - \beta_2(f) \geq x$, thus the identity $x \wedge f(x) = x$ holds in $\mathbf{S}_2$. However, this identity does not hold in $\mathbf{S}_1$, since in $\mathbf{S}_1$ we have $f(x) = x - \beta_1(x) < x$. This contradicts our assumption $\mathbf{S}_1 \cong \mathbf{S}_2$, hence we conclude that $\beta_2(f) > 0$. Put

$$t = \frac{\beta_2(f)}{\beta_1(f)},$$

thus $t > 0$. If $\beta_2 \neq t\beta_1$ then we have an element $g \in F$ such that $\beta_2(g) \neq t\beta_2(g)$. Suppose $\beta_2(g) < t\beta_1(g)$. Since $\beta_2(f) > 0$, we can choose integers $p, q \in \mathbb{Z}$ such that $q > 0$ and

$$\beta_2(g) < \frac{p}{q}\beta_2(f) < t\beta_1(g).$$

Multiplying by $q > 0$ and using $\beta_2(f) = t\beta_1(f)$, we get

$$q\beta_2(g) < p\beta_2(f) = tp\beta_1(f) < tq\beta_1(g).$$

Since β_1, β_2 are homomorphisms and $t > 0$, we get

$$\beta_2(g^q) < \beta_2(f^p) \quad \text{and} \quad \beta_1(f^p) < \beta_1(g^q).$$

This implies that the identity $f^p(x) \wedge g^q(x) = f^p(x)$ holds in $\mathbf{S}_2$, but fails in $\mathbf{S}_1$. It is not hard to see that this method works also for the other case when $\beta_2(g) > t\beta_1(g)$. Thus we get a contradiction, which shows that $\beta_2 = t\beta_1$.

Now let us choose an arbitrary real number $s_1 \in S_1$, and put $s_2 = \iota(s_1) \in S_2$ and $d = s_2 - ts_1$. Furthermore, let

$$Q_i = \{\, f(s_i) \mid f \in F \,\} = \{\, s_i - \beta_i(f) \mid f \in F \,\} \quad \text{for } i = 1, 2.$$

Clearly $Q_i \subseteq S_i$ for $i = 1, 2$, and since β_i is a dense homomorphism, Q_i is a dense subset of $\mathbb{R}$, and hence of S_i, too. Now we will show that the isomorphisms $\tau\colon \mathbf{R}_{\beta_1} \to \mathbf{R}_{\beta_2}$ and ι coincide on the set $Q_1 \subseteq \mathbb{R}$. For each element $f(s_1) \in Q_1$ we have $\iota(f(s_1)) = f(\iota(s_1)) = f(s_2)$ and $\tau(f(s_1)) = f(\tau(s_1)) = f(ts_1 + d) = f(s_2)$. Thus τ yields a bijection between Q_1 and Q_2.

Since both τ and ι preserve the natural order of the real numbers, and they coincide on Q_1, and the sets Q_1, Q_2 are dense in S_1, S_2, respectively, the isomorphisms τ and ι coincide on the whole set S_1. Thus $\tau(S_1) = S_2$, that is, $tS_1 + d = S_2$. $\square$

Up to this point we have seen two types of simple **F**-semilattices. The first type consists of the algebras $\mathbf{S}_M$, while the other type contains the algebras $\mathbf{Z}_\alpha$ and $\mathbf{R}_\beta$. The simple **F**-semilattices of the first type have a least element and some atoms, while the algebras of the second type are linear. It is possible to construct an example of a simple **F**-semilattice which has a least element but no atoms and its semilattice order is not linear. From Corollary 1.11 we know that the group **F** cannot be locally finite in this example. By Lemma 1.14 we also know that **F** cannot be commutative. Therefore it is natural to let **F** to be an appropriate infinite subgroup of the symmetric group $\mathrm{Sym}\,\mathbb{Z}$ of the set of integers. We refer the reader to [18] where the construction of this example is carried out in detail.

2 The undecidability of a partial near-unanimity term

The *near-unanimity problem* is to decide of a finite algebra if it has a near-unanimity term. In an attempt to prove the undecidability of this problem the following approach was taken by R. McKenzie.

Definition 2.1. Let $\mathbf{A}$ be a fixed finite algebra, $t(x_1, \ldots, x_n)$ be a term of $\mathbf{A}$, and S be a subset of A. We say that t is a *partial near-unanimity term on S* if

$$t(y, x, \ldots, x) = t(x, y, x, \ldots, x) = \cdots = t(x, \ldots, x, y) = x$$

for all $x, y \in S$.

Clearly, a term t of $\mathbf{A}$ is a near-unanimity term if and only if it is a partial near-unanimity term on A, but more interestingly, if and only if t is a partial near-unanimity term of the two-generated free algebra in the variety generated by $\mathbf{A}$ on the set $\{x, y\}$ of generators. Thus it is natural to study the decidability of the partial near-unanimity problem on some fixed subset of a finite algebra. It is proved in [22] that the existence of a partial near-unanimity term on a fixed two-element subset is undecidable. We will extend this result to a subset excluding two fixed elements, which is our main result in this chapter.

Theorem 2.2. *There exists no algorithm that can decide of a finite algebra $\mathbf{A}$ and two fixed elements $r, w \in A$ if $\mathbf{A}$ has a partial near-unanimity term on the set $A \setminus \{r, w\}$.*

Following the proof of R. McKenzie, our work is based on the undecidability of the halting problem for Minsky machines. The Minsky machine was invented by M. Minsky in 1961 (see [24, 25]), but he writes that the concept was inspired by some ideas of M. O. Rabin and D. Scott [27]. The "hardware" of a Minsky machine $\mathcal{M}$ consists of two *registers* A and B, which can contain arbitrary natural numbers. The "software" is a finite set S of *states* together with a list of *commands*. There are two special states: the *initial state* $q_1 \in S$, and the *halting state* $q_0 \in S$. The machine starts in the initial state, stops at the halting state, and at any given time it is in one of the states. For each state $i \in S \setminus \{q_0\}$ there is a unique command which is either of the form

- $i : \text{inc } R, j$ or
- $i : \text{dec } R, j, k$

where $R \in \{A, B\}$ and $j, k \in S$. The first command instructs the machine to increase the value stored in register R by one, and then to go to state j. The second command first checks the value stored in register R; if it is zero, then the machine goes to state j; otherwise the value stored in register R is decremented by one and the machine goes to state k. Now we give the formal definition.

Definition 2.3. A *Minsky machine* $\mathcal{M} = \langle S, q_0, q_1, M\rangle$ is a finite set S of *states* with two distinguished elements $q_0, q_1 \in S$ together with a mapping

$$M\colon S \setminus \{q_0\} \to \{\, \langle R, j\rangle, \langle R, j, k\rangle \mid R \in \{A, B\} \text{ and } j, k \in S\,\}.$$

We call q_0 the *halting state*, and q_1 the *initial state*. The symbols A and B represent the registers.

The mapping M describes the commands of $\mathcal{M}$ in the following way. For any given state $i \in S \setminus \{q_0\}$ the tuple $M(i)$ is either of the form $\langle R, j\rangle$ or $\langle R, j, k\rangle$, which correspond to the two types of commands described earlier.

Definition 2.4. A *configuration* $\langle i, a, b\rangle$ of $\mathcal{M}$ is an element of $S \times \mathbb{N} \times \mathbb{N}$, which specifies the current state and the values of the registers. We call $\langle i, a, b\rangle$ an *initial configuration* (*halting configuration*) if $i = q_1$ (or $i = q_0$, respectively).

For any configuration the Minsky machine $\mathcal{M}$ uniquely determines (computes) the next configuration. By iteration, starting from the initial configuration with zero registers, we obtain a sequence of configurations, which will be called the computation of $\mathcal{M}$.

Definition 2.5. The *processor* for $\mathcal{M}$ is a partial mapping of the set of configurations into itself denoted by $\bar{\mathcal{M}}$ and defined as

$$\bar{\mathcal{M}}(\langle i, a, b\rangle) = \begin{cases} \text{undefined} & \text{if } i = q_0, \\ \langle j, a+1, b\rangle & \text{if } M(i) = \langle A, j\rangle, \\ \langle j, 0, b\rangle & \text{if } M(i) = \langle A, j, k\rangle \text{ and } a = 0, \\ \langle k, a-1, b\rangle & \text{if } M(i) = \langle A, j, k\rangle \text{ and } a > 0, \\ \langle j, a, b+1\rangle & \text{if } M(i) = \langle B, j\rangle, \\ \langle j, a, 0\rangle & \text{if } M(i) = \langle B, j, k\rangle \text{ and } b = 0, \\ \langle k, a, b-1\rangle & \text{if } M(i) = \langle B, j, k\rangle \text{ and } b > 0. \end{cases}$$

We will use iterative applications of the processor $\bar{\mathcal{M}}$ and adopt the power notation defined as $\bar{\mathcal{M}}^0(\langle i, a, b\rangle) = \langle i, a, b\rangle$ and $\bar{\mathcal{M}}^{n+1}(\langle i, a, b\rangle) = \bar{\mathcal{M}}(\bar{\mathcal{M}}^n(\langle i, a, b\rangle))$. We consider $\bar{\mathcal{M}}^n(\langle i, a, b\rangle)$ to be undefined if $\bar{\mathcal{M}}^m(\langle i, a, b\rangle)$ is a halting configuration for some $m < n$.

Definition 2.6. We say that $\mathcal{M}$ *halts* if it halts on the $\langle 0, 0\rangle$ input, that is, if $\bar{\mathcal{M}}^n(\langle q_1, 0, 0\rangle)$ is a halting configuration for some $n > 0$.

It is proved in [24] that Minsky machines are equivalent to Turing machines in the following sense. Given a Minsky machine $\mathcal{M}$ (or Turing machine $\mathcal{T}$), we can algorithmically construct a Turing machine $\mathcal{T}(\mathcal{M})$ (or Minsky machine $\mathcal{M}(\mathcal{T})$) which halts if and only if the original machine halts. This means that the *halting problem* for Minsky machines is as difficult as for Turing machines; that is, undecidable. Thus a new path opens for proving the undecidability of algebraic problems by interpreting Minsky machines. For example this route was taken in [16] to prove the undecidability of various kinds of word problems.

In the rest of this chapter we are going to prove Theorem 2.2 in the following way. For any Minsky machine $\mathcal{M}$ we define an algebra $\mathbf{A}(\mathcal{M})$ with two special elements $r, w \in A(\mathcal{M})$ such that $\mathbf{A}(\mathcal{M})$ will have a partial near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$ if and only if $\mathcal{M}$ halts. This is clearly enough since the halting problem for Minsky machines is undecidable.

By $\operatorname{maj}(x, y, z)$ we denote the majority element of $\{x, y, z\}$ if it exists, i.e., when $|\{x, y, z\}| \leq 2$. We advise the reader to skim through this definition and return to it when reading the subsequent proofs.

Definition 2.7. Let $C = \{0, A, B, 1\}$. We define the algebra $\mathbf{A}(\mathcal{M})$ on the set $A(\mathcal{M}) = S \times C \cup \{p, r, w\}$ with the following operations

$$I(x) = \begin{cases} w & \text{if } x \in \{r, w\}, \\ \langle q_1, 0\rangle & \text{if } x = p, \\ r & \text{if } x \in S \times C; \end{cases}$$

$$M(x, y, z, u) = \begin{cases} w & \text{if } w \in \{y, z, u\} \text{ or } r \in \{y, z, u\}, \\ \operatorname{maj}(y, z, u) & \text{else if } \operatorname{maj}(y, z, u) \neq p, \\ p & \text{else if } \operatorname{maj}(y, z, u) = p \text{ and} \\ & \quad x \in \{q_0\} \times C \cup \{r\}, \\ w & \text{otherwise;} \end{cases}$$

for each command $i : \text{inc } R, j$ of $\mathcal{M}$ the operation

$$F_i(x, y) = \begin{cases} \langle j, c\rangle & \text{if } x = \langle i, c\rangle \text{ and } y = p, \\ \langle j, R\rangle & \text{if } x = \langle i, 0\rangle \text{ and } y \in S \times C, \\ r & \text{if } x = r \text{ and } y = p, \\ w & \text{otherwise;} \end{cases}$$

and for each command $i : \text{dec } R, j, k$ of $\mathcal{M}$ the operations

$$G_i(x, y) = \begin{cases} \langle k, c\rangle & \text{if } x = \langle i, c\rangle \text{ and } y = p, \\ \langle k, 1\rangle & \text{if } x = \langle i, R\rangle \text{ and } y \in S \times C, \\ r & \text{if } x = r \text{ and } y = p, \\ w & \text{otherwise;} \end{cases}$$

$$H_i(x) = \begin{cases} \langle j, c\rangle & \text{if } x = \langle i, c\rangle \text{ and } c \neq R, \\ r & \text{if } x = r, \\ w & \text{otherwise.} \end{cases}$$

We will investigate this algebra in detail. The first important property of $\mathbf{A}(\mathcal{M})$ is that it almost has an absorbing element.

Definition 2.8. Let A be a set, and $f\colon A^n \to A$. An element $w \in A$ is *absorbing for f* if $f(\bar{a}) = w$ whenever $\bar{a} \in A^n$ and $w \in \{a_1, \ldots, a_n\}$.

Proposition 2.9. *The element w of $\mathbf{A}(\mathcal{M})$ is absorbing for the operations I, F_i, G_i and H_i.*

Proof. One only has to check the definition of $\mathbf{A}(\mathcal{M})$. In the definition of I this is stated explicitly. In the definition of F_i, G_i and H_i only the 'otherwise' case can be applied. □

Note that w is not an absorbing element for the operation M, but almost, except in the first variable. Combining this with the previous proposition one can see that $\mathbf{A}(\mathcal{M})$ cannot have a partial near-unanimity term on a nontrivial subset that includes w. For example plugging in w in the right-most variable of a term always yields w. We will use the element w to indicate some irregularity of a term when plugging in near-unanimous evaluations.

Definition 2.10. Let $\bar{x} = (x_1, x_2, \ldots)$ be a fixed set of variables, and $\bar{p}$ be the constant p evaluation. For each element $e \in A(\mathcal{M})$ let $\bar{p}|_{x_n=e}$ be the evaluation $x_n = e$ and $x_m = p$ if $m \neq n$. We say that a term $t(\bar{x})$ is *regular* if $t(\bar{p}) \neq w$ and $t(\bar{p}|_{x_n=e}) \neq w$ for each $n \in \mathbb{N}$ and $e \in S \times C$.

We ask the reader to check that the terms x_1, $I(x_1)$, and $F_{q_1}(I(x_1), x_2)$ are regular, while the terms $I(I(x_1))$, $F_{q_1}(x_1, x_2)$ and $M(x_1, x_2, x_3, x_4)$ are not.

Definition 2.11. We define *slim* terms inductively. The term $I(x_n)$ is slim for every variable x_n. If t is slim, then so are $F_i(t, y)$, $G_i(t, y)$ and $H_i(t)$ for any state $i \in S$ and variable $y \in \bar{x}$.

Proposition 2.12. *Every regular term t that does not contain the operation M is either slim or a variable. Moreover, if t is regular and slim then there exists an evaluation $\bar{p}|_{x_n=e}$ for some x_n and $e \in S \times C$, such that $t(\bar{p}|_{x_n=e}) = r$.*

Proof. We use induction on the complexity of t. If t is a variable then the statement is void, because variables are not slim by definition.

Suppose that $t(\bar{x}) = I(t_1(\bar{x}))$. Because of Proposition 2.9 we know that t_1 must be regular, as well. If t_1 is not a variable, then according to our assumption we have an evaluation $\bar{p}|_{x_n=e}$ such that $t_1(\bar{p}|_{x_n=e}) = r$. This shows that $t(\bar{p}|_{x_n=e}) = w$, which is a contradiction. Thus t_1 must be a variable, in which case the statement and the existence of the required evaluation are satisfied.

Now suppose that $t(\bar{x}) = F_i(t_1(\bar{x}), t_2(\bar{x}))$ for some $i \in S$. Again, both t_1 and t_2 must be regular. If t_1 is a variable then $t(\bar{p}) = F_i(p, t_2(\bar{p})) = w$. Thus t_1 cannot be a variable. So there exists an evaluation $\bar{p}|_{x_n=e}$ such that $t_1(\bar{p}|_{x_n=e}) = r$, which forces $t_2(\bar{p}|_{x_n=e}) = p$. But p is not in the range of any of the operations I, F_i, G_i and H_i; thus t_2 must be a variable. In this case the statement is clear.

The same argument works if the topmost operation of t is either G_i or H_i. $\square$

Regular slim terms play a very important role in the proof; they essentially encode the computation of the Minsky machine $\mathcal{M}$. To see how this works, we describe the construction of a partial near-unanimity term from a halting computation.

Lemma 2.13. *If $\mathcal{M}$ halts, then there exists a partial near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$.*

Proof. We use the processor $\bar{\mathcal{M}}^n$ from Definition 2.5. Assume that $\mathcal{M}$ halts in n steps, that is, $\bar{\mathcal{M}}^n(\langle q_1, 0, 0\rangle) = \langle q_0, -, -\rangle$. For each natural number $m \leq n$ we define i_m, a_m, and b_m by

$$\bar{\mathcal{M}}^m(\langle q_1, 0, 0\rangle) = \langle i_m, a_m, b_m\rangle.$$

We are going to build a slim term of depth $n+1$ by induction. Put $t_0 = I(x)$. Now suppose that t_m is already defined. At step m the machine is in state i_m. There is a unique command for each state.

If the command for state i_m is of the form i : inc R, j, then put $t_{m+1} = F_{i_m}(t_m, y_m)$ where y_m is a new variable. Now assume that the command for state i_m is of the form i : dec R, j, k where $R = A$. If $a_m = 0$ then put $t_{m+1} = H_{i_m}(t_m)$. If $a_m \neq 0$ then let $m' < m$ be the largest natural number such that $a_{m'} < a_m$, and put $t_{m+1} = G_{i_m}(t_m, y_{m'})$. The case when $R = B$ is handled similarly using b_m and $b_{m'}$ instead of a_m and $a_{m'}$.

Finally, put $t = M(t_n, z_1, z_2, z_3)$ where z_1, z_2 and z_3 are new variables. We claim that t_n is a regular slim term and t is a partial near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$.

Claim 1. *The term t_n is slim.*

This follows from the construction. We have used only variables in the second coordinates of F_i and G_i.

Claim 2. *No variable of t has more than two occurrences. If a variable has exactly two occurrences, then it is $y_{m'}$ for some m and the two occurrences are at $t_{m'+1} = F_{i_{m'}}(t_{m'}, y_{m'})$ and $t_{m+1} = G_{i_m}(t_m, y_{m'})$. If a variable y_m has exactly one occurrence then it is at $t_{m+1} = F_{i_m}(t_m, y_m)$.*

The variables x, z_1, z_2 and z_3 have single occurrences. At each F_i we always introduced a new variable. Now consider the case when $t_{m+1} = G_{i_m}(t_m, y_{m'})$. From the definition we know that $a_{m'} < a_m$ and $a_m \leq a_{m'+1}, \ldots, a_m$ (assuming that $R = A$). Since $a_{m'} < a_m \leq a_{m'+1}$ and the machine cannot increase a register by more than one, $a_{m'} + 1 = a_m = a_{m'+1}$. This implies that the command for state $i_{m'}$ is of the form i : inc R, j and $R = A$. On the other hand, the command for state i_m is of the form

i : dec A, j, k and $a_m \neq 0$, therefore $a_{m+1} = a_m - 1$. To summarize, for each pair $\langle m', m\rangle$

$$a_{m'} + 1 = a_{m'+1} = a_m = a_{m+1} + 1, \text{ and}$$
$$a_m \leq a_{m'+1}, \ldots, a_m.$$

Note that this condition is symmetric. If m' is in pair with some m then m is the least natural number such that $m' < m$ and $a_{m'+1} > a_{m+1}$. Therefore, $y_{m'}$ has at most two occurrences.

Claim 3. *$t_m(\bar{p}) = \langle i_m, 0\rangle$ for all $m \leq n$*

We prove by induction on m. For $m = 0$ this is true by definition: $I(p) = \langle q_1, 0\rangle$. Now we prove it for $m+1$. By definition t_{m+1} is $F_{i_m}(t_m, y_m)$, $H_{i_m}(t_m)$ or $G_{i_m}(t_m, y_{m'})$. Therefore $t_{m+1}(\bar{p})$ is $F_{i_m}(\langle i_m, 0\rangle, p)$, $H_{i_m}(\langle i_m, 0\rangle)$ or $G_{i_m}(\langle i_m, 0\rangle, p)$. Looking up the definition of these operations we conclude that $t_{m+1}(\bar{p}) = \langle i_{m+1}, 0\rangle$.

Claim 4. *$t_m(\bar{p}|_{x=e}) = r$ for all $m \leq n$ and $e \in S \times C$.*

This is clear, using induction.

Claim 5. *Let $h < n$ and $e \in S \times C$ be fixed and assume that y_h has exactly one occurrence in t_n. Let R be the register manipulated in the command for state i_h. Then*

$$t_m(\bar{p}|_{y_h=e}) = \begin{cases} \langle i_m, 0\rangle & \text{if } 0 \leq m \leq h, \\ \langle i_m, R\rangle & \text{if } h < m \leq n. \end{cases}$$

Without loss of generality we can assume that $R = A$. By Claim 2, the single occurrence of y_h is at $t_{h+1} = F_{i_h}(t_h, y_h)$. Therefore, if $m \leq h$ then $t_m(\bar{p}|_{y_h=e}) = t_m(\bar{p}) = \langle i_m, 0\rangle$. We use induction on m to prove the other case. For the base of the induction we have $t_{h+1}(\bar{p}|_{y_h=e}) = F_{i_h}(\langle i_h, 0\rangle, e) = \langle i_{h+1}, A\rangle$.

Now consider the induction step from m to $m+1$. Assume that $t_{m+1} = F_{i_m}(t_m, y_m)$. Since y_h has a single occurrence, $y_h \neq y_m$, and therefore $t_{m+1}(\bar{p}|_{y_h=e}) = F_{i_m}(\langle i_m, A\rangle, p) = \langle i_{m+1}, A\rangle$. A similar argument works when $t_{m+1} = G_{i_m}(t_m, y_{m'})$.

Now assume that $t_{m+1} = H_{i_m}(t_m)$. From the proof of Claim 2 we can see that $a_h < a_{h+1}, \ldots, a_n$. Therefore, $a_m \neq 0$. By the definition of t_{m+1} we know that either a_m or b_m must be zero. Thus it is register B which is manipulated in the command for state i_m. This implies that $t_{m+1}(\bar{p}|_{y_h=e}) = H_{i_m}(\langle i_m, A\rangle) = \langle i_{m+1}, A\rangle$.

Claim 6. *Let $h < n$ and $e \in S \times C$ be fixed and assume that $y_{h'}$ has exactly two occurrences in t_n as described in Claim 2. Let R be the register manipulated in the commands for states $i_{h'}$ and i_h. Then*

$$t_m(\bar{p}|_{y_{h'}=e}) = \begin{cases} \langle i_m, 0\rangle & \text{if } 0 \leq m \leq h', \\ \langle i_m, R\rangle & \text{if } h' < m \leq h, \\ \langle i_m, 1\rangle & \text{if } h < m \leq n. \end{cases}$$

Without loss of generality we can assume that $R = A$. The same argument works for the first two cases as in the previous claim, but using h' instead of h.

We prove the third case by induction on m. For the base of the induction we have $t_{h+1} = G_{i_h}(t_h, y_{h'})$. Hence $t_{h+1}(\bar{p}|_{y_{h'}=e}) = G_{i_h}(\langle i_h, A\rangle, e) = \langle i_{h+1}, 1\rangle$. The induction step is now easy as there are no other occurrences of $y_{h'}$ along the term t_n. Therefore, we always calculate $F_{i_m}(\langle i_m, 1\rangle, p)$, $G_{i_m}(\langle i_m, 1\rangle, p)$, or $H_{i_m}(\langle i_m, 1\rangle)$, which all yield $\langle i_{m+1}, 1\rangle$.

Claim 7. *The term t_n is regular. Moreover, $t_n(\bar{p}|_{u=e}) \in \{q_0\} \times C \cup \{r\}$ for all variables u and all $e \in A(\mathcal{M}) \setminus \{r, w\}$.*

Take any element $e \in S \times C$. By Claims 3 and 4 we have $t_n(\bar{p}) = \langle q_0, 0\rangle$ and $t_n(\bar{p}|_{x=e}) = r$, respectively. Now take a variable y_h. If y_h has no occurrence in t_n then $t_n(\bar{p}|_{y_h=e}) = t_n(\bar{p}) = \langle q_0, 0\rangle$. Otherwise y_h has one or two occurrences by Claim 2. Then by Claims 5 and 6 we have $t_n(\bar{p}|_{y=e}) \in \{q_0\} \times C$.

Claim 8. *t is a partial near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$.*

Take a near-unanimous evaluation $\bar{a}$ on $A(\mathcal{M}) \setminus \{r, w\}$. If the majority element is not p, then $t(\bar{a}) = M(t_n(\bar{a}), z_1, z_2, z_3) = \mathrm{maj}(z_1, z_2, z_3)$. If the majority element is p then $t_n(\bar{a}) \in \{q_0\} \times C \cup \{r\}$ by Claim 7, and hence $t(\bar{a}) = p$. Therefore, t is a partial near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$. ☐

We have seen how to encode the halting computation into the regular slim term t_n. Our goal now is the reverse; to show that the computation of $\mathcal{M}$ can be recovered from a regular slim term.

Lemma 2.14. *Let t_n be a regular slim term of depth $n + 1$. Then $t_n(\bar{p}) = \langle i_n, 0\rangle$ where i_n is the state of the machine $\mathcal{M}$ after the first n steps.*

Proof. We want to show that the term t_n behaves the same way as the one in the proof of the previous lemma. Denote by t_m the unique subterm of t_n of depth $m + 1$. That is, $t_0 = I(-)$, and t_{m+1} is $F_i(t_m, -)$, $G_i(t_m, -)$ or $H_i(t_m)$ for some $i \in S$. Since t_n is regular and the element w is absorbing, $t_m(\bar{p}|_{u=e}) \neq w$ for all $m \leq n$, $e \in S \times C$ and all variables u of t_n.

Claim 1. *$t_m(\bar{p}) \in S \times \{0\}$ for all $m < n$.*

This is clear, using induction.

Claim 2. *Let x be the variable used in t_0. Then x has no other occurrence in t_n. Moreover, $t_m(\bar{p}|_{x=e}) = r$ for all $m \leq n$ and $e \in S \times C$.*

We use induction on m. For $m = 0$ we have $t_0(\bar{p}|_{x=e}) = I(e) = r$. For the induction step from m to $m + 1$ assume that $t_m(\bar{p}|_{x=e}) = r$. Thus $t_{m+1}(\bar{p}|_{x=e})$ is $F_i(r, y)$, $G_i(r, y)$ or $H_i(r)$ for some $i \in S$ and some variable y. We know that this value is not w. Looking up the definition of F_i, G_i and H_i, we can see that the only choice is when the result is r (and $y = p$ for F_i and G_i). This completes the induction step and proves that $x \neq y$ when the operation is F_i or G_i.

Claim 3. *Assume that a variable $y \neq x$ has exactly one occurrence in t_n. Then the occurrence is at $t_{m+1} = F_i(t_m, y)$ for some $m < n$ and $i \in S$. Moreover, there exists no $h > m$ such that $t_{h+1} = H_j(t_h)$ and the command for j manipulates the same register as the one for i.*

Let m be the least natural number such that t_{m+1} has an occurrence of y. Then $t_{m+1} = F_i(t_m, y)$ or $t_{m+1} = G_i(t_m, y)$ for some $i \in S$. Take $e \in S \times C$, and consider $t_{m+1}(\bar{p}|_{y=e})$. By Claim 1, $t_m(\bar{p}|_{y=e}) \in S \times \{0\}$. Checking the definition of G_i we see that $G_i(t_m(\bar{p}|_{y=e}), e) = w$, a contradiction. So $t_{m+1} = F_i(t_m, y)$. Moreover, $t_{m+1}(\bar{p}|_{y=e}) \in S \times \{R\}$ where R is the register manipulated by the command for i. Now we show that $t_h(\bar{p}|_{y=e}) \in S \times \{R\}$ for all $h > m$ by induction. For $m+1$ we already have this. For the induction step consider $a = t_{h+1}(\bar{p}|_{y=e})$. By definition a is $F_j(\langle -, R\rangle, p)$, $G_j(\langle -, R\rangle, p)$ or $H_j(\langle -, R\rangle)$ for some $j \in S$ and $a \neq w$. In the first two cases this shows that $a \in S \times \{R\}$. On the other hand, when $a = H_j(\langle -, R\rangle) \neq w$ then the command for state j cannot manipulate the register R. This concludes the proof of this claim.

Claim 4. *Assume that a variable $y \neq x$ has at least two occurrences in t_n. Then there exist $m' < m$ such that $t_{m'+1} = F_i(t_{m'}, y)$, $t_{m+1} = G_j(t_m, y)$ for some $i, j \in S$, the commands for i and j manipulate the same register R, and y has no other occurrences than these two. Moreover, there exists no $m' < h < m$ such that $t_{h+1} = H_k(t_h)$ and the command for k manipulates the register R.*

Let m' and m be the least natural numbers such that $t_{m'+1}$ has exactly one and t_{m+1} has exactly two occurrences of y. The term t_m has exactly one occurrence of y, so we can apply the previous claim. This proves half of the claim. It remains to be shown that $t_{m+1} = G_j(t_m, y)$ for some $j \in S$, that the command for j manipulates the register R, and that there are no other occurrences of y.

Fix $e \in S \times C$. From the proof of the previous claim we know that $t_m(\bar{p}|_{y=e}) \in S \times \{R\}$ where R is the register manipulated by the command for i. Consider $a = t_{m+1}(\bar{p}|_{y=e})$. This element is either $F_j(\langle -, R\rangle, e)$ or $G_j(\langle -, R\rangle, e)$ for some j. Since $a \neq w$, we must have $t_{m+1} = G_j(t_m, y)$, and the command for j must manipulate R. Therefore, $t_{m+1}(\bar{p}|_{y=e}) \in S \times \{1\}$.

Finally, we show that $t_h(\bar{p}|_{y=e}) \in S \times \{1\}$ for all $h > m$ by induction. We have already the basis of the induction. To show the induction step, consider t_{h+1}. If $t_{h+1} = H_k(t_h)$ for some k then we get $t_{h+1}(\bar{p}|_{y=e}) \in S \times \{1\}$ by the definition of H_k. Now assume that $t_{h+1} = F_k(t_h, z)$. Since $t_{h+1}(\bar{p}|_{y=e}) \neq w$ we must have $z \neq y$ and $t_{h+1}(\bar{p}|_{y=e}) \in S \times \{1\}$. The same argument works for G_k, as well.

Claim 5. *Let i_m, a_m and b_m be defined by $\bar{\mathcal{M}}^m(\langle q_1, 0, 0\rangle) = \langle i_m, a_m, b_m\rangle$. Then the following hold for all $0 \leq m < n$.*

(1) *If the command of $\mathcal{M}$ for i_m is of the form $i : \mathrm{inc}\ R, j$, then $t_{m+1} = F_{i_m}(t_m, -)$.*

(2) *If the command for i_m is of the form $i : \mathrm{dec}\ R, j, k$, and if $a_m \neq 0$ for $R = A$ while $b_m \neq 0$ for $R = B$, then $t_{m+1} = G_{i_m}(t_m, -)$.*

(3) *If the command for i_m is of the form $i : \mathrm{dec}\ R, j, k$, and if $a_m = 0$ for $R = A$ while $b_m = 0$ for $R = B$, then $t_{m+1} = H_{i_m}(t_m, -)$.*

Moreover, $t_m(\bar{p}) = \langle i_m, 0\rangle$ for all $0 \leq m \leq n$.

We prove this by induction on m. For $m = 0$ we have $t_0(\bar{p}) = I(p) = \langle q_1, 0\rangle = \langle i_0, 0\rangle$. For the induction step assume that (1)–(3) hold for all $m' < m$, a condition which is void if $m = 0$, and $t_m(\bar{p}) = \langle i_m, 0\rangle$. We have to show that (1)–(3) hold for m and $t_{m+1}(\bar{p}) = \langle i_{m+1}, 0\rangle$.

Assume that $t_{m+1} = F_i(t_m, y)$ for some $i \in S$ and some variable y. We have to show that $i = i_m$ and $t_{m+1}(\bar{p}) = \langle i_{m+1}, 0\rangle$. Since the operation F_i is defined, the command for state i is $i : \mathrm{inc}\ R, j$ for some $R \in \{A, B\}$ and $j \in S$. From the induction hypothesis, $t_m(\bar{p}) = \langle i_m, 0\rangle$. Consider the element $e = t_{m+1}(\bar{p}) = F_i(\langle i_m, 0\rangle, p)$. Since $e \neq w$, we must have $i = i_m$ and $e = \langle j, 0\rangle$. As $i_m = i$ and the command is $i : \mathrm{inc}\ R, j$, we have $i_{m+1} = j$. So, $t_{m+1}(\bar{p}) = \langle i_{m+1}, 0\rangle$.

Assume that $t_{m+1} = G_i(t_m, y)$ for some $i \in S$ and variable y. We have to show that $i = i_m$ and $t_{m+1}(\bar{p}) = \langle i_{m+1}, 0\rangle$. Since the operation G_i is defined, the command for state i is $i : \mathrm{dec}\ R, j, k$ for some $R \in \{A, B\}$ and $j, k \in S$. Without loss of generality we can assume that $R = A$. Consider $e = t_{m+1}(\bar{p}) = G_i(\langle i_m, 0\rangle, p)$. Since $e \neq w$, we must have $i = i_m$ and $e = \langle k, 0\rangle$. What remains to be shown is that $i_{m+1} = k$. We know that i_{m+1} is either j or k depending on whether $a_m = 0$ or $a_m \neq 0$. We claim that $a_m \neq 0$. By the definition of the Minsky machine,

$$\begin{aligned} a_m = {} & |\{\, h < m : \mathcal{M} \text{ has increased register } A \text{ at step } h \,\}| \\ & - |\{\, h < m : \mathcal{M} \text{ has decreased register } A \text{ at step } h \,\}|. \end{aligned}$$

Now using the induction hypothesis we get that $a_m = |S^+| - |S^-|$ where

$$\begin{aligned} S^+ = \{\, h < m : {} & t_{h+1} = F_{i_h}(t_h, -) \text{ and} \\ & \text{the command for } i_h \text{ manipulates register } A \,\}, \text{ and} \\ S^- = \{\, h < m : {} & t_{h+1} = G_{i_h}(t_h, -) \text{ and} \\ & \text{the command for } i_h \text{ manipulates register } A \,\}. \end{aligned}$$

Take a number h from the second set S^-, so $t_{h+1} = G_{i_h}(t_h, z)$ for some variable z, and the command for i_h manipulates register A. By Claim 2, 3 and 4, the variable z has exactly two occurrences; the other being at $t_{h'+1} = F_{i_{h'}}(t'_h, z)$ for some $h' < h$. Moreover, the command for $i_{h'}$ manipulates the same register A. Thus h' belongs to the first set S^+. This only shows that $a_m \geq 0$. But the same argument works for $t_{m+1} = G_i(t_m, y)$, showing that there exists an $m' < m$ which belongs to S^+, while $m \notin \mathrm{S}^-$. Therefore, $a_m > 0$ and $i_{m+1} = k$.

Finally, assume that $t_{m+1} = H_i(t_m)$ for some $i \in S$. We have to show that $i = i_m$ and $t_{m+1}(\bar{p}) = \langle i_{m+1}, 0\rangle$. Since the operation H_i is defined, the command for state i is i : dec R, j, k for some $R \in \{A, B\}$ and $j, k \in S$. Without loss of generality we can assume that $R = A$. Consider $e = t_{m+1}(\bar{p}) = H_i(\langle i_m, 0\rangle)$. Since $e \neq w$, we must have $i = i_m$ and $e = \langle j, 0\rangle$. What remains to be shown is that $i_{m+1} = j$. We know that i_{m+1} is either j or k depending on whether $a_m = 0$ or $a_m \neq 0$. To get a contradiction, suppose that $a_m \neq 0$, i.e., the set S^+, defined in the previous subsection, has more elements than S^-. We know that each element of S^- is in pair with a unique element of S^+. So there exists an $h < m$ such that $t_{h+1} = F_{i_h}(t_h, z)$ for some variable z, the command for i_h manipulates register A, and h is not in S^-. Therefore, z has exactly one occurrence in t_m. If z has two occurrences then the other one must appear after t_{m+1}. In any case, either by Case 3 or 4, the command for i at $t_{m+1} = H_i(t_m)$ cannot manipulate register A. But according to our assumption it does, which is a contradiction. This shows that $a_m = 0$, therefore $i_{m+1} = j$.

This finishes the proof of the last claim, which includes the statement $t_n(\bar{p}) = \langle i_n, 0\rangle$ of the lemma. $\square$

The previous two lemmas give the connection between regular slim terms and halting computations. What remains to be shown is that a regular slim term can be found as a subterm of a partial near-unanimity term on $A(\mathcal{M})\setminus\{r, w\}$, or at least as a subterm of a "minimal" partial near-unanimity term.

Definition 2.15. Two terms t_1 and t_2 are *p-equivalent* iff $t_1(\bar{p}) = t_2(\bar{p})$ and $t_1(\bar{p}|_{x_n=e}) = t_2(\bar{p}|_{x_n=e})$ for each $n \in \mathbb{N}$ and $e \in S \times C$. A term is *p-minimal* iff there is no p-equivalent term of smaller complexity.

Lemma 2.16. *Let t be a regular p-minimal term which contains the operation M. Then $\mathbf{A}(\mathcal{M})$ halts.*

Proof. We use induction on the complexity of t. If $t = F_{i,c}(t_1, t_2)$ then both t_1 and t_2 must be regular (and p-minimal) by Proposition 2.9. So at least one of them contains the operation M and by induction we are done. The same argument works for the operations $G_{i,c}$, $H_{i,c}$ and I, as well.

Now suppose that $t = M(t_1, t_2, t_3, t_4)$. If t_2,t_3 or t_4 is not regular then we have some near p-unanimous evaluation $\bar{f}$ such that $w \in \{t_2(\bar{f}), t_3(\bar{f}), t_4(\bar{f})\}$. This forces $t(\bar{f}) = w$, which is a contradiction. So t_2, t_3 and t_4 are regular. If one of them contains the operation M, then we use induction on that subterm. So assume that M does not occur in t_2,t_3 and t_4. By Proposition 2.12, each of them is either a slim term or a variable. If t_k is slim ($k \in \{2, 3, 4\}$), then we have an evaluation $\bar{p}|_{x_n=e}$ such that $t_k(\bar{p}|_{x_n=e}) = r$. This forces a contradiction $t(\bar{p}|_{x_n=e}) = w$. Thus t_2,t_3 and t_4 must be variables. If two of them are the same variable y then it is not hard to check that t is p-equivalent to y, a contradiction to the p-minimality. Thus the terms t_2,t_3 and t_4 are distinct variables. If t_1 is not regular then we have an evaluation $\bar{p}|_{x_n=e}$ such that $t_1(\bar{p}|_{x_n=e}) = w$. But this forces $t(\bar{p}|_{x_n=e}) = w$, a contradiction. So t_1 must be regular. If t_1 contains M then we use the induction. If t_1 does not contain M then by Proposition 2.12 it is either a slim term or a variable. It cannot be a variable because $t(\bar{p}) \neq w$. So t_1 is regular and slim term. Now by Lemma 2.14 the value $t_1(\bar{p})$ contains the last state of the correct piece of the computation. But $t(\bar{p}) \neq w$, which proves that we have reached the halting state. $\square$

Theorem 2.17. *Let $\mathcal{M}$ be a Minsky machine. The algebra $\mathbf{A}(\mathcal{M})$ has a partial near-unanimity term on the set $A(\mathcal{M}) \setminus \{r, w\}$ iff $\mathcal{M}$ halts.*

Proof. Suppose that t is a partial near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$. Then t is regular. Let t' be a term p-equivalent to t and p-minimal. Then t' is not a variable; moreover, $t'(\bar{p}) = p$ implies that the topmost operation of t' is M. Now by Lemma 2.16, $\mathcal{M}$ halts. The other direction is proved in Lemma 2.13. $\square$

This finishes the proof of Theorem 2.2, as it is undecidable of a Minsky machine if it halts.

3 The decidability of a near-unanimity term

Let ω and ω^+ be the set of all finite and countable cardinals, respectively. For a nonempty set A we denote by $\mathcal{O}_A$ the set of all operations on A. In general we do not assume that the underlying set A is finite. For $\mathcal{F} \subseteq \mathcal{O}_A$ and $n \in \omega$ put $\mathcal{F}^{(n)} = \mathcal{F} \cap A^{A^n}$, which is the set of all n-ary operations contained in $\mathcal{F}$. Binary operations will play a crucial role in our arguments, therefore we put $\mathcal{B}_A = \mathcal{O}_A^{(2)}$. The clone generated by a set $\mathcal{F} \subseteq \mathcal{O}_A$ will be denoted by $\langle \mathcal{F} \rangle$. All indices in this chapter start from zero.

An operation $f \in \mathcal{O}_A^{(n)}$ is a *near-unanimity operation* if

$$f(y, x, \dots, x) = f(x, y, x, \dots, x) = \dots = f(x, \dots, x, y) = x$$

for all $x, y \in A$. It is customary to assume that $n \geq 3$, but we will not make this restriction to avoid considering special cases in some of our arguments. However, this does not weaken our results, because no operation of arity less than three can satisfy this definition whenever the underlying set has at least two elements. The problem of deciding whether a finite algebra has a near-unanimity term operation is called the *near-unanimity problem.*

Instead of working with operations and their composition, we introduce an equivalence relation on the set of operations in such a way that

(1) the near-unanimity operations form an equivalence class of the relation,

(2) a new notion of composition can be introduced on the equivalence classes, and

(3) it is possible to algorithmically compute the closure of equivalence classes under this new notion of composition.

We start the proof with the study of the binary operations that arise as $f(x, \dots, x, y, x, \dots, x)$ from another operation $f \in \mathcal{O}_A$.

Definition 3.1. For $f \in \mathcal{O}_A^{(n)}$ and $i \in \omega$, the ith *polymer* of f is $f|_i \in \mathcal{B}_A$ defined as

$$f|_i(x, y) = \begin{cases} f(x, \dots, x, \overset{i\text{th}}{\overbrace{y}}, x, \dots, x) & \text{if } i < n, \\ f(x, \dots, x) & \text{if } i \geq n, \end{cases}$$

where y occurs at the ith coordinate of f in the first case. The collection of polymers of f together with their multiplicities is the *characteristic function* of f, which is formally defined as the map $\chi_f : \mathcal{B}_A \to \omega^+$ where

$$\chi_f(b) = |\{\, i \in \omega : f|_i = b \,\}| .$$

By the set of characteristic functions on a nonempty set A we mean the set $\mathcal{X}_A = \{\, \chi_f : f \in \mathcal{O}_A \,\}$. Note that not every mapping of $\mathcal{B}_A$ to ω^+ is a characteristic function of some operation. In the following lemma we characterize the ones that are.

Lemma 3.2. *A mapping $\chi : \mathcal{B}_A \to \omega^+$ is a characteristic function of some operation if and only if*

(1) *there exists a unique element $b \in \mathcal{B}_A$ such that $\chi(b) = \omega$,*

(2) *there are only finitely many $c \in \mathcal{B}_A$ such that $\chi(c) \neq 0$, and*

(3) *$c(x, x) \approx b(x, y)$ whenever $\chi(c) \neq 0$ and $\chi(b) = \omega$.*

Proof. To show that the given list of conditions are necessary, take an arbitrary operation $f \in \mathcal{O}_A^{(n)}$. Put $b = f|_n$. By Definition 3.1, $b(x, y) \approx f(x, \dots, x)$ and $f|_i = b$ for all $i \geq n$, which proves that $\chi(b) = \omega$. Moreover, for every $c \in \mathcal{B}_A$ other than b, $\chi(c) = |\{\, i < n : f|_i = c \,\}|$ is finite, proving items (1) and (2). Finally, if $\chi(c) \neq 0$, then $c = f|_i$ for some $i \in \omega$, and $c(x, x) \approx f(x, \dots, x) \approx b(x, y)$.

To show the other direction, take a mapping $\chi : \mathcal{B}_A \to \omega^+$ satisfying items (1)–(3). Let $b \in \mathcal{B}_A$ be the unique element for which $\chi(b) = \omega$, and put $C = \{\, c \in \mathcal{B}_A : \chi(c) \notin \{0, \omega\} \,\}$. By conditions (1) and (2), the set C is finite, and $n = \sum_{c \in C} \chi(c)$ is a finite number. Consequently, we can choose a finite list $\xi_0, \dots, \xi_{n-1} \in \mathcal{B}_A$ of elements such that $\chi(c) = |\{\, i < n : \xi_i = c \,\}|$ for all $c \in C$. Because of condition (3), there exists an operation $f \in \mathcal{O}_A^{(n)}$ that satisfies the following list of identities:

$$\begin{aligned} f(y, x, x, \dots, x, x) &\approx \xi_0(x, y), \\ f(x, y, x, \dots, x, x) &\approx \xi_1(x, y), \\ &\vdots \\ f(x, x, x, \dots, x, y) &\approx \xi_{n-1}(x, y), \\ f(x, x, x, \dots, x, x) &\approx b(x, y). \end{aligned}$$

Clearly, $f|_i = \xi_i$ for all $i < n$, and $f|_n = f|_{n+1} = \cdots = b$. Therefore, $\chi_f = \chi$, which concludes the proof. ☐

We leave it to the reader to prove the following result that characterizes near-unanimity operations by their characteristic functions.

Lemma 3.3. *$f \in \mathcal{O}_A$ is a near-unanimity operation if and only if $\chi_f = \chi_{\mathrm{nu}}$ where $\chi_{\mathrm{nu}} \in \mathcal{X}_A$ is defined as*

$$\chi_{\mathrm{nu}}(b) = \begin{cases} \omega & \text{if } b(x, y) \approx x, \\ 0 & \text{otherwise.} \end{cases}$$

Given a set $\mathcal{G} \subseteq \mathcal{O}_A$ of operations, we define $\mathsf{X}(\mathcal{G}) = \{\, \chi_f : f \in \mathcal{G} \,\}$. By the last lemma, the kernel of the operator X satisfies our goal (1) stated at the beginning of the chapter. To establish goal (2), we introduce the notions of composition for operations and characteristic functions, and consequently show that they correspond to one another under taking the characteristic functions of the operations. If for a set $\mathcal{G}$ of operations we can show that the corresponding set $\{\chi_g : g \in \mathcal{G}\}$ of characteristic functions is closed under this new notion of composition and does not include $\chi_{\mathbf{nu}}$, then we will be able to conclude that $\langle \mathcal{G} \rangle$ does not contain a near-unanimity operation, even if $\mathcal{G}$ is not a clone. First, we need the following definition.

Definition 3.4. By an *extension* of $g \in \mathcal{O}_A^{(n)}$ we mean an operation $g' \in \mathcal{O}_A^{(m)}$ satisfying

$$g'(x_0, \dots, x_{m-1}) \approx g(x_{\sigma(0)}, \dots, x_{\sigma(n-1)}),$$

where σ is an arbitrary injection of $\{0, \dots, n-1\}$ into $\{0, \dots, m-1\}$. By a *composition* of $f \in \mathcal{O}_A^{(n)}$ *with extensions* of $g_0, \dots, g_{n-1} \in \mathcal{O}_A$ we mean an operation of the form $f(g'_0, \dots, g'_{n-1})$ where $g'_0, \dots, g'_{n-1} \in \mathcal{O}_A^{(m)}$ are extensions of $g_0, \dots, g_{n-1}$, respectively, and are of the same arity m.

Clearly, the extensions of g are exactly the operations that can be obtained from g by permuting the variables and introducing dummy variables. As an example, all projections are extensions of the unary projection. It is easy to see that if g' is an extension of g, then $\chi_{g'} = \chi_g$.

The next definition is best motivated by a simple example. Take $f \in \mathcal{O}_A^{(2)}$ and $g_0, g_1 \in \mathcal{O}_A^{(m)}$. We would like to describe the characteristic function of $f(g_0, g_1)$ via the characteristic functions of f, g_0 and g_1. Clearly, the ith polymer of $f(g_0, g_1)$ is $f(g_0|_i, g_1|_i)$, which shows that $\chi_{f(g_0,g_1)}$ depends not only on χ_f but also on f. Furthermore, if g'_1 is an m-ary extensions of g_1, then $\chi_{g_1} = \chi_{g'_1}$, but in general $g_1|_i \neq g'_1|_i$, and therefore $\chi_{f(g_0,g_1)} \neq \chi_{f(g_0,g'_1)}$. This shows that besides χ_{g_0} and χ_{g_1} we also need to know which "variables" of χ_{g_0} correspond to the "variables" of χ_{g_1}. What we need is an assignment, denoted as a map μ in the following definition, that with multiplicities assigns the polymers of g_0 to that of g_1.

Definition 3.5. We say that $\chi \in \mathcal{X}_A$ is a *composition* of $f \in \mathcal{O}_A^{(n)}$ with $\chi_0, \dots, \chi_{n-1} \in \mathcal{X}_A$ if there exists a mapping $\mu : (\mathcal{B}_A)^n \to \omega^+$ such that

$$\chi(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b}) = c} \mu(\bar{b})$$

and

$$\chi_i(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_i = c} \mu(\bar{b})$$

for all $c \in \mathcal{B}_A$ and $i < n$.

We introduce the following operators on $\mathcal{O}_A$ and $\mathcal{X}_A$. Given $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$, we denote by $\mathsf{C}_{\mathcal{F}}(\mathcal{G})$ the set of all possible compositions of operations $f \in \mathcal{F}^{(n)}$ with extensions of $g_0, \dots, g_{n-1} \in \mathcal{G}$. We will use the same symbol for the analogous operator for characteristic functions: given $\mathcal{F} \subseteq \mathcal{O}_A$ and $\mathcal{U} \subseteq \mathcal{X}_A$, we denote by $\mathsf{C}_{\mathcal{F}}(\mathcal{U})$ the set of all possible compositions of operations $f \in \mathcal{F}^{(n)}$, for some $n \in \omega$, with characteristic functions $\chi_0, \dots, \chi_{n-1} \in \mathcal{U}$.

Lemma 3.6. $\mathsf{XC}_{\mathcal{F}}(\mathcal{G}) = \mathsf{C}_{\mathcal{F}}\mathsf{X}(\mathcal{G})$ *for all* $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$.

Proof. To prove the inclusion $\subseteq$, take $f \in \mathcal{F}^{(n)}$ and $g_0, \dots, g_{n-1} \in \mathcal{G}$, let $g'_0, \dots, g'_{n-1} \in \mathcal{O}_A^{(m)}$ be extensions of $g_0, \dots, g_{n-1}$, respectively, of the same arity $m \in \omega$, and put $h = f(g'_0, \dots, g'_{n-1}) \in \mathcal{O}_A^{(m)}$. We need to show that χ_h is a composition of f with $\chi_{g_0}, \dots, \chi_{g_{n-1}}$. Define $\mu : (\mathcal{B}_A)^n \to \omega^+$ as

$$\mu(\bar{b}) = \left|\{\, i \in \omega : \langle g'_0|_i, \dots, g'_{n-1}|_i \rangle = \bar{b} \,\}\right|,$$

which describes how many times the tuple $\bar{b} \in (\mathcal{B}_A)^n$ of binary operations appear as the polymers of $g'_0, \dots, g'_{n-1}$ at the same coordinate i.

We check Definition 3.5 now. For each element $c \in \mathcal{B}_A$,

$$\sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b}) = c} \mu(\bar{b}) = \left|\{\, i \in \omega : f(g'_0|_i, \dots, g'_{n-1}|_i) = c \,\}\right| \\ = \left|\{\, i \in \omega : h|_i = c \,\}\right| = \chi_h(c).$$

On the other hand, for each $j < n$ and $c \in \mathcal{B}_A$,

$$\sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_j = c} \mu(\bar{b}) = \left|\{\, i \in \omega : g'_j|_i = c \,\}\right| = \chi_{g'_j}(c).$$

This shows that χ_h is a composition of f with $\chi_{g'_0}, \dots, \chi_{g'_{n-1}}$. Moreover, since g'_j is an extension of g_j, $\chi_{g_j} = \chi_{g'_j}$ for all $j < n$. This completes the proof of $\mathsf{XC}_{\mathcal{F}}(\mathcal{G}) \subseteq \mathsf{C}_{\mathcal{F}}\mathsf{X}(\mathcal{G})$.

To prove the other inclusion, take an arbitrary $\chi \in \mathsf{C}_{\mathcal{F}}\mathsf{X}(\mathcal{G})$. Then there exist $f \in \mathcal{F}^{(n)}$, operations $g_0, \dots, g_{n-1} \in \mathcal{G}$ of arities $m_0, \dots, m_{n-1}$, respectively, and $\mu : (\mathcal{B}_A)^n \to \omega^+$ such that

$$\chi(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b}) = c} \mu(\bar{b}) \tag{3.6a}$$

and

$$\chi_{g_j}(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_j = c} \mu(\bar{b}) \tag{3.6b}$$

for all $c \in \mathcal{B}_A$ and $j < n$. We will argue that χ is the characteristic function of a composition of f with extensions of $g_0, \dots, g_{n-1}$.

Using equation (3.6a) we obtain

$$\sum_{\bar{b} \in (\mathcal{B}_A)^n} \mu(\bar{b}) = \sum_{c \in \mathcal{B}_A} \chi(c) = \omega,$$

where the second equality holds because χ is a characteristic function. Consequently, we can choose a mapping $\xi : \omega \to (\mathcal{B}_A)^n$ such that

$$\mu(\bar{b}) = \left|\{\, i \in \omega : \xi(i) = \bar{b} \,\}\right|$$

for all $\bar{b} \in (\mathcal{B}_A)^n$. Now, using equation (3.6b), we get that

$$\bigl|\{\, i \in \omega : g_j|_i = c \,\}\bigr| = \chi_{g_j}(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_j = c} \mu(\bar{b}) = \bigl|\{\, i \in \omega : \xi(i)_j = c \,\}\bigr|$$

for all $j < n$ and $c \in \mathcal{B}_A$. The cardinalities of the two sets on the two sides are equal, therefore, for every $j < n$ we can choose a permutation $\sigma_j : \omega \to \omega$ such that

$$g_j|_i = \xi(\sigma_j(i))_j$$

for all $i \in \omega$. Put $m = \max\{\, \sigma_j(i) : j < n, i < m_j \,\}$. Now, for all $j < n$, the restriction of σ_j to the set $\{0, \ldots, m_j - 1\}$ is an injection into the set $\{0, \ldots, m-1\}$. Define the operations $g'_0, \ldots, g'_{n-1} \in \mathcal{O}_A^{(m)}$ as

$$g'_j(x_0, \ldots, x_{m-1}) \approx g_j(x_{\sigma_j(0)}, \ldots, x_{\sigma_j(m_j-1)}).$$

Clearly, each g'_j is an extension of g_j. To complete the proof, we need to show that the characteristic function of $f(g'_0, \ldots, g'_{n-1})$ equals χ.

Observe that

$$g'_j|_i = \begin{cases} g_j|_{\sigma_j^{-1}(i)} & \text{if } \sigma_j^{-1}(i) < m_j, \\ g_j(x, \ldots, x) & \text{otherwise.} \end{cases}$$

As a result, $g'_j|_i = g_j|_{\sigma_j^{-1}(i)}$ for all $i \in \omega$, and therefore

$$g'_j|_i = g_j|_{\sigma_j^{-1}(i)} = \xi(\sigma_j \sigma_j^{-1}(i))_j = \xi(i)_j$$

for all $i \in \omega$ and $j < n$. Then, for an arbitrary element $c \in \mathcal{B}_A$,

$$\begin{aligned}
\chi_{f(g'_0, \ldots, g'_{n-1})}(c) &= \bigl|\{\, i \in \omega : f(g'_0, \ldots, g'_{n-1})|_i = c \,\}\bigr| \\
&= \bigl|\{\, i \in \omega : f(g'_0|_i, \ldots, g'_{n-1}|_i) = c \,\}\bigr| \\
&= \bigl|\{\, i \in \omega : f(\xi(i)_0, \ldots, \xi(i)_{n-1}) = c \,\}\bigr| \\
&= \bigl|\{\, i \in \omega : f(\bar{b}) = c \text{ where } \bar{b} = \xi(i) \,\}\bigr| \\
&= \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b}) = c} \mu(\bar{b}) \\
&= \chi(c).
\end{aligned}$$

□

The following lemma turns the near unanimity problem into a problem about characteristic functions. We will use the power notation for the composition operator. For $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$ we define $\mathsf{C}^0_{\mathcal{F}}(\mathcal{G}) = \mathcal{G}$, and $\mathsf{C}^{n+1}_{\mathcal{F}}(\mathcal{G}) = \mathsf{C}_{\mathcal{F}} \mathsf{C}^n_{\mathcal{F}}(\mathcal{G})$ for all $n \in \omega$. We use the same power notation for the composition of characteristic functions, as well.

Lemma 3.7. *Let $\mathcal{F} \subseteq \mathcal{O}_A$ and $\mathcal{G} \subseteq \langle \mathcal{F} \rangle$, and assume that $\mathcal{G}$ contains an idempotent operation. Then $\langle \mathcal{F} \rangle$ contains a near-unanimity operation if and only if $\chi_{\mathrm{nu}} \in \bigcup_{n \in \omega} \mathsf{C}^n_{\mathcal{F}} \mathsf{X}(\mathcal{G})$.*

Proof. By Lemma 3.6, $\bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}\mathsf{X}(\mathcal{G}) = \mathsf{X}\left(\bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}(\mathcal{G})\right)$. Consequently, by Lemma 3.3, it is enough to show that $\langle\mathcal{F}\rangle$ contains a near-unanimity operation if and only if $\bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}(\mathcal{G})$ does. One direction is trivial because $\bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}(\mathcal{G}) \subseteq \langle\mathcal{F}\rangle$. For the other direction assume that $f \in \langle\mathcal{F}\rangle^{(k)}$ is a near-unanimity operation and $g \in \mathcal{G}^{(m)}$ is an arbitrary idempotent operation. We define $h \in \langle\mathcal{F}\rangle^{(km)}$ as

$$h(x_0,\dots,x_{km-1}) = f(g(x_0,\dots,x_{m-1}),\dots,g(x_{km-m},\dots,x_{km-1})).$$

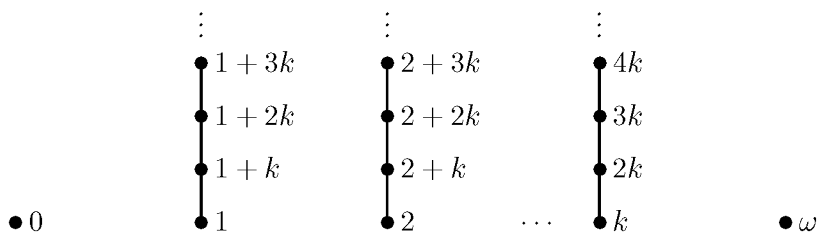
Clearly, h is a near-unanimity operation, and $h \in \bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}(\mathcal{G})$. ☐

If $\mathcal{G}$ is the set of all projections on the set A and $\mathcal{F} \subseteq \mathcal{O}_A$, then $\bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}(\mathcal{G}) = \langle\mathcal{F}\rangle$, and $\mathsf{X}(\mathcal{G}) = \{\chi_{\mathrm{id}}\}$, where χ_{id} is defined as

$$\chi_{\mathrm{id}}(b) = \begin{cases} \omega & \text{if } b(x,y) \approx x, \\ 1 & \text{if } b(x,y) \approx y, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, by the previous lemma, $\langle\mathcal{F}\rangle$ contains a near-unanimity operation if and only if $\chi_{\mathrm{nu}} \in \bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}(\{\chi_{\mathrm{id}}\})$. However, this condition does not seem to be easier to check than the original one. We overcome this problem by carefully choosing $\mathcal{G}$ so that the latter condition can be effectively tested.

Definition 3.8. For an integer $k \geq 1$ we define a partial order $\sqsubseteq_k$ on ω^+ as follows:



Acting coordinate-wise, this defines a partial order on $\mathcal{X}_A$. For a set $\mathcal{U} \subseteq \mathcal{X}_A$ denote by $\mathsf{F}_k(\mathcal{U})$ the order filter generated by $\mathcal{U}$ in $\mathcal{X}_A$, that is,

$$\mathsf{F}_k(\mathcal{U}) = \{\, \chi' \in \mathcal{X}_A : (\exists \chi \in \mathcal{U})(\forall b \in \mathcal{B}_A)(\chi(b) \sqsubseteq_k \chi'(b)) \,\}.$$

Recall that a partially ordered set (or simply poset) is called *well-ordered*, if it has no infinite anti-chains and satisfies the descending chain condition, i.e., contains no strictly decreasing sequence of elements. Clearly, $\langle\omega^+; \sqsubseteq_k\rangle$ is well-ordered. It is known that subposets and finite products of well-ordered posets are well-ordered. Moreover, the set of order filters of a well-ordered poset under the inclusion order satisfies the ascending chain condition. Consequently, $\langle\mathcal{X}_A; \sqsubseteq_k\rangle$ is well-ordered and has no strictly increasing sequence of order filters.

Lemma 3.9. *Let $k \geq 1$, $\mathcal{F} \subseteq \mathcal{O}_A$ and $\mathcal{U} \subseteq \mathcal{X}_A$. Then $\mathsf{F}_k\mathsf{C}_{\mathcal{F}}(\mathcal{U}) \subseteq \mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$. Consequently, $\mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$ is an order filter.*

Proof. Take arbitrary characteristic functions $\chi \in \mathsf{C}_{\mathcal{F}}(\mathcal{U})$ and $\chi' \in \mathcal{X}_A$ such that $\chi \sqsubseteq_k \chi'$. Thus χ is a composition of an operation $f \in \mathcal{F}^{(n)}$ and characteristic functions $\chi_0, \ldots, \chi_{n-1} \in \mathcal{U}$. By Definition 3.5, there exists a map $\mu : (\mathcal{B}_A)^n \to \omega^+$ such that

$$\chi(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b})=c} \mu(\bar{b}) \tag{3.9a}$$

and

$$\chi_i(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_i=c} \mu(\bar{b}) \tag{3.9b}$$

for all $c \in \mathcal{B}_A$ and $i < n$. Let D be the set of binary operations $d \in \mathcal{B}_A$ where $\chi(d) \neq \chi'(d)$. Since neither 0 nor ω is comparable to any other element under $\sqsubseteq_k$, for all $d \in D$, $\chi(d) \notin \{0, \omega\}$ and $\chi'(d) - \chi(d)$ equals to a positive multiple of k. Using equation (3.9a), for each $d \in D$ we can choose an n-tuple $\bar{b}_d \in (\mathcal{B}_A)^n$ such that $\mu(\bar{b}_d) \notin \{0, \omega\}$. Define $\mu' : (\mathcal{B}_A)^n \to \omega^+$ as

$$\mu'(\bar{b}) = \begin{cases} \mu(\bar{b}) + \chi'(d) - \chi(d) & \text{if } \bar{b} = \bar{b}_d \text{ for some } d \in D, \\ \mu(\bar{b}) & \text{otherwise.} \end{cases}$$

Clearly, $\mu(\bar{b}) \sqsubseteq_k \mu'(\bar{b})$ for all $\bar{b} \in (\mathcal{B}_A)^n$. Then by equation (3.9b), $\chi_i \sqsubseteq_k \chi'_i$ for all $i < n$ where $\chi'_i : \mathcal{B}_A \to \omega^+$ is defined as

$$\chi'_i(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_i=c} \mu'(\bar{b})$$

for all $c \in \mathcal{B}_A$. On the other hand, by the choice of μ',

$$\chi'(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b})=c} \mu'(\bar{b})$$

for all $c \in \mathcal{B}_A$. This proves that χ' is a composition of f and the characteristic functions $\chi'_0, \ldots, \chi'_{n-1} \in \mathsf{F}_k(\mathcal{U})$ via the map μ'.

To prove the second assertion of the lemma, consider the containments $\mathsf{F}_k\mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U}) \subseteq \mathsf{C}_{\mathcal{F}}\mathsf{F}_k\mathsf{F}_k(\mathcal{U}) = \mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U}) \subseteq \mathsf{F}_k\mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$ showing that $\mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$ is an order filter. ☐

Lemma 3.10. *Let $k \geq 1$, and let A, $\mathcal{F} \subseteq \mathcal{O}_A$ and $\mathcal{U} \subseteq \mathcal{X}_A$ be finite sets. Then the minimal elements of $\langle \mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U}); \sqsubseteq_k \rangle$ can be effectively computed.*

Proof. Choose an arbitrary minimal element $\chi \in \mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$. Then χ is a composition of an n-ary operation $f \in \mathcal{F}^{(n)}$ with some characteristic functions $\chi_0, \ldots, \chi_{n-1} \in \mathsf{F}_k(\mathcal{U})$ via a mapping $\mu : (\mathcal{B}_A)^n \to \omega^+$. Observe in

Definition 3.5 that f and μ uniquely determine χ and $\chi_0, \dots, \chi_{n-1}$ via the defining equations

$$\chi(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ f(\bar{b})=c} \mu(\bar{b}) \tag{3.10a}$$

and

$$\chi_i(c) = \sum_{\bar{b} \in (\mathcal{B}_A)^n,\ b_i=c} \mu(\bar{b}). \tag{3.10b}$$

Since A is finite, $(\mathcal{B}_A)^n$ is finite, and consequently the poset $\langle (\omega^+)^{(\mathcal{B}_A)^n}; \sqsubseteq_k \rangle$ is well ordered. Clearly, μ is an element of this poset, so we can assume that μ is minimal in this poset among all representations of χ.

By the finiteness of A and $\mathcal{U}$,

$$m = \max\big(\{k\} \cup \{\, \chi'(b) : \chi' \in \mathcal{U}, b \in \mathcal{B}_A \text{ and } \chi'(b) \neq \omega \,\}\big)$$

is a (finite) natural number that depends only on k, A and $\mathcal{U}$. We claim that $\mu(\bar{b}) \in \{0, \dots, m, \omega\}$ for all $\bar{b} \in (\mathcal{B}_A)^n$, which is enough to conclude our proof because then only finitely many operations $f \in \mathcal{F}$ and finitely many mappings $\mu : (\mathcal{B}_A)^n \to \{0, \dots, m, \omega\}$ need to be considered to find all minimal elements of $\mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$.

To get a contradiction, assume that $\mu(\bar{c}) > m$ and $\mu(\bar{c}) \neq \omega$ for some tuple $\bar{c} \in (\mathcal{B}_A)^n$. Define $\mu' : (\mathcal{B}_A)^n \to \omega^+$ as

$$\mu'(\bar{b}) = \begin{cases} \mu(\bar{b}) & \text{if } \bar{b} \neq \bar{c}, \\ \mu(\bar{b}) - k & \text{if } \bar{b} = \bar{c}, \end{cases}$$

and define χ' and $\chi'_0, \dots, \chi'_{n-1}$ using the defining equations (3.10a) and (3.10b) for μ', respectively. Observe that $\mu'(\bar{c}) = \mu(\bar{c}) - k > m - k \geq 0$.

First we argue that $\chi'_i \in \mathsf{F}_k(\mathcal{U})$ for all $i = 0, \dots, n-1$. Clearly, by equation (3.10b), $\chi_i(b) = \chi'_i(b)$ for all $b \neq c_i$. Moreover, either $\chi'_i(c_i) = \chi_i(c_i) = \omega$ or $\chi'_i(c_i) = \chi_i(c_i) - k$. In the former case, $\chi'_i = \chi_i \in \mathsf{F}_k(\mathcal{U})$. In the latter case, $\chi'_i(c_i) = \chi_i(c_i) - k \geq \mu(\bar{c}) - k > m - k \geq 0$, where the first inequality holds by equation (3.10b). Therefore, χ'_i satisfies the conditions of Lemma 3.2, so $\chi'_i \in \mathcal{X}_A$. Since $\chi_i \in \mathsf{F}_k(\mathcal{U})$, there exists a characteristic function $\chi''_i \in \mathcal{U}$ so that $\chi''_i \sqsubseteq_k \chi_i$. By the choice of m, $\chi''_i(c_i) \leq m < \mu(\bar{c}) \leq \chi_i(c_i)$, consequently $\chi''_i(c_i) \leq \chi_i(c_i) - k$. This proves that $\chi''_i \sqsubseteq_k \chi'_i$. As a result, $\chi'_i \in \mathsf{F}_k(\mathcal{U})$.

Analogously, $\chi'(\bar{b}) = \chi(\bar{b})$ for all $\bar{b} \neq \bar{c}$, and either $\chi'(\bar{c}) = \chi(\bar{c}) = \omega$ or $\chi'(\bar{c}) = \chi(\bar{c}) - k > m - k \geq 0$. Consequently, $\chi' \in \mathcal{X}_A$ by Lemma 3.2, and $\chi' \sqsubseteq_k \chi$. Since $\chi'_0, \dots, \chi'_{n-1} \in \mathsf{F}_k(\mathcal{U})$, we get that $\chi' \in \mathsf{C}_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$. From the minimality of χ we see that $\chi' = \chi$. But then μ' contradicts the minimality of μ, which concludes the proof. $\square$

Lemma 3.11. *Let $k \geq 1$, and let A, $\mathcal{F} \subseteq \mathcal{O}_A$ and $\mathcal{U} \subseteq \mathcal{X}_A$ be finite sets. Then $\bigcup_{n \in \omega} \mathsf{C}^n_{\mathcal{F}}\mathsf{F}_k(\mathcal{U})$ is an order filter with respect to $\sqsubseteq_k$, and its minimal elements can be effectively computed.*

Proof. For every $m \in \omega$ define $\mathcal{U}_m = \bigcup_{n \le m} \mathsf{C}^n_{\mathcal{F}} \mathsf{F}_k(\mathcal{U})$, where $\mathcal{U}_0 = \mathsf{F}_k(\mathcal{U})$. For each $m \in \omega$, $\mathcal{U}_m$ is an order filter in $\langle \mathcal{X}_A; \sqsubseteq_k \rangle$ whose minimal elements can be effectively computed by Lemmas 3.9 and 3.10. Since A is finite, $\langle \mathcal{X}_A; \sqsubseteq_k \rangle$ is well-ordered and consequently the set of all its order filters under the inclusion order satisfies the ascending chain condition. Therefore, the ascending chain $\mathcal{U}_0 \subseteq \mathcal{U}_1 \subseteq \mathcal{U}_2 \subseteq \dots$ of order filters cannot be strictly increasing.

Assume that $\mathcal{U}_m = \mathcal{U}_{m+1}$ for some $m \in \omega$. This condition is equivalent to that of $\mathsf{C}^{m+1} \mathsf{F}_k(\mathcal{U}) \subseteq \bigcup_{n \le m} \mathsf{C}^n_{\mathcal{F}} \mathsf{F}_k(\mathcal{U})$. Applying $\mathsf{C}_{\mathcal{F}}$ to both sides we get that

$$\mathsf{C}^{m+2} \mathsf{F}_k(\mathcal{U}) \subseteq \bigcup_{1 \le n \le m+1} \mathsf{C}^n_{\mathcal{F}} \mathsf{F}_k(\mathcal{U}) \subseteq \mathcal{U}_{m+1}.$$

Consequently, $\mathcal{U}_{m+1} = \mathcal{U}_{m+2}$. By induction, we obtain that $\mathcal{U}_m = \mathcal{U}_{m+1} = \mathcal{U}_{m+2} = \dots$, as a result $\mathcal{U}_m = \bigcup_{n \in \omega} \mathsf{C}^n_{\mathcal{F}} \mathsf{F}_k(\mathcal{U})$.

This yields an algorithm to find $\bigcup_{n \in \omega} \mathsf{C}^n_{\mathcal{F}} \mathsf{F}_k(\mathcal{U})$. Calculate $\mathcal{U}_0, \mathcal{U}_1, \dots$ in order using Lemma 3.10. If $\mathcal{U}_m = \mathcal{U}_{m+1}$ for some $m \in \omega$, then we have found $\bigcup_{n \in \omega} \mathsf{C}^n_{\mathcal{F}} \mathsf{F}_k(\mathcal{U})$ and know its minimal elements. This condition must occur and therefore the algorithm stops, because we cannot have a strictly increasing sequence of order filters in $\langle \mathcal{X}_A; \sqsubseteq_k \rangle$. ☐

The previous lemma shows that the minimal elements of the infinite union $\bigcup_{n \in \omega} \mathsf{C}^n_{\mathcal{F}} \mathsf{X}(\mathcal{G})$ of Lemma 3.7 can be effectively calculated provided that $\mathsf{X}(\mathcal{G})$ forms an order filter in $\langle \mathcal{X}_A; \sqsubseteq_k \rangle$ for some $k \ge 1$. We will argue that such integer k and set $\mathcal{G} \subseteq \langle \mathcal{F} \rangle$ can be found if $\langle \mathcal{F} \rangle$ contains a near-unanimity operation. We need the following definition.

Definition 3.12. Let $k \in \omega$ and $f \in \mathcal{O}^{(n)}_A$. We call f a *k-nu operation* if $k \le n$ and

$$\begin{gathered} f(x, \dots, x) \approx x, \\ f|_0(x, y) \approx \dots \approx f|_{k-1}(x, y) \text{ and} \\ f|_k(x, y) \approx \dots \approx f|_{n-1}(x, y) \approx x. \end{gathered}$$

This concept is the generalization of that of near-unanimity and weak near-unanimity operations. The 0-nu operations are precisely the near-unanimity operations, while the k-nu operations of arity k are called weak near-unanimity operations.

Lemma 3.13. *If a clone on an m-element set contains a near-unanimity operation, then it contains a 2-nu operation of arity at most $2 + m^{m^2}$.*

To prove this lemma, we need the following theorem.

Theorem 3.14 (L. Lovász [17]). *Let n, k be natural numbers such that $2 \le 2k \le n$, and $G_{n,k}$ be the graph on the set of all k-element subsets of an n-element set with the disjointness relation. Then the chromatic number of $G_{n,k}$ is $n - 2k + 2$.* ☐

Proof of Lemma 3.13. Let $\mathcal{C}$ be a clone and $f \in \mathcal{C}$ be a near-unanimity operation of arity n. If $n \leq 1 + m^{m^2}$, then we are done as f is a 2-nu operation. Otherwise $n - m^{m^2} \geq 2$. Put

$$k = \left\lfloor \frac{n - m^{m^2} + 1}{2} \right\rfloor.$$

By the choice of k, we have $n - m^{m^2} \leq 2k \leq n - m^{m^2} + 1$, from which it follows that $1 + m^{m^2} \leq n - 2k + 2 \leq 2 + m^{m^2}$ and $2 \leq 2k \leq n$.

We color each k-element subset $I \subseteq \{0, \dots, n-1\}$ by the binary operation $f|_I$ defined as

$$f|_I(x, y) = f(u_0, \dots, u_{n-1}) \quad \text{where} \quad u_i = \begin{cases} x & \text{if } i \notin I, \\ y & \text{if } i \in I. \end{cases}$$

There are m^{m^2} binary operations on an m-element set, thus we colored the graph $G_{n,k}$ with m^{m^2} colors. Since the chromatic number of this graph is $n - 2k + 2$, by Theorem 3.14, and $n - 2k + 2 > m^{m^2}$, there must exist two disjoint k-element subsets $I, J \subset \{0, \dots, n-1\}$ for which $f|_I = f|_J$.

Choose an arbitrary bijection τ from $\{0, \dots, n-1\} \setminus (I \cup J)$ to $\{0, \dots, n-2k-1\}$. We claim that the following operation is a 2-nu operation in $\mathcal{C}$ of arity at most $2 + m^{m^2}$:

$$g(x, y, z_0, \dots, z_{n-2k-1}) = f(u_0, \dots, u_{n-1}) \quad \text{where} \quad u_i = \begin{cases} x & \text{if } i \in I, \\ y & \text{if } i \in J, \\ z_{\tau(i)} & \text{otherwise.} \end{cases}$$

Clearly, $g \in \mathcal{C}$ and its arity is $n - 2k + 2 \leq 2 + m^{m^2}$. Moreover, $g|_0 = f|_I = f|_J = g|_1$, and for all $i \geq 2$, $g|_i = f|_{\tau(i-2)} = x$ because f was a near-unanimity operation. This proves that g is a 2-nu operation. ☐

Lemma 3.15. *Let $\mathcal{C}$ be a clone on an m-element set that contains a k-nu operation of arity $k + n$. Then $\mathcal{C}$ contains a $k^{m!}$-nu operation f of arity $k^{m!} + n$ such that*

$$f|_0(x, f|_0(x, y)) = f|_0(x, y).$$

Proof. Let A be the underlying set of $\mathcal{C}$, and $g \in \mathcal{C}$ be a k-nu operation of arity $k+n$. By induction we define a sequence $g_1, g_2, g_3, \dots \in \mathcal{C}$ of operations of arities $k + n, k^2 + n, k^3 + n, \dots$, respectively. Put $g_1 = g$, and for $i \geq 1$ put

$$\begin{aligned} &g_{i+1}(x_0, \dots, x_{k^{i+1}-1}, y_0, \dots, y_{n-1}) \\ &\qquad = g\big(g_i(x_0, \dots, x_{k^i-1}, y_0, \dots, y_{n-1}), \dots, \\ &\qquad\qquad g_i(x_{(k-1)k^i}, \dots, x_{k^{i+1}-1}, y_0, \dots, y_{n-1}), y_0, \dots, y_{n-1}\big). \end{aligned}$$

Since g is idempotent, i.e. $g(x, \dots, x) = x$, the defined operations $g_1, g_2, \dots$ are idempotent, as well. For each element $x \in A$ define the unary operation $h_x(y) = g|_0(x, y)$. We claim that, for each $i \geq 1$ and $j \in \omega$,

$$g_i|_j(x, y) = \begin{cases} h_x^i(y) & \text{if } j < k^i, \\ x & \text{if } j \geq k^i. \end{cases}$$

This holds for g_1 by definition. Let $i \geq 1$ and $j < k^{i+1}$. Choosing $l < k$ such that $lk^i \leq j < (l+1)k^i$ we get that

$$\begin{aligned} g_{i+1}|_j(x, y) &= g\big(g_i(x, \dots, x), \dots, g_i(x, \dots, x), g_i|_{j-lk^i}(x, y), \\ &\qquad\qquad g_i(x, \dots, x), \dots, g_i(x, \dots, x), x, \dots, x\big) \\ &= g|_l(x, g_i|_{j-lk^i}(x, y)) \\ &= h_x(h_x^i(y) \\ &= h_x^{i+1}(y). \end{aligned}$$

Finally, if $i \geq 1$ and $k^{i+1} \leq j < k^{i+1} + n$, then

$$\begin{aligned} g_{i+1}|_j(x, y) &= g(g_i(x, \dots, x), \dots, g_i(x, \dots, x), x, \dots, x, y, x, \dots, x) \\ &= g|_{j-k^{i+1}+k}(x, y) \\ &= x. \end{aligned}$$

This proves that each g_i is a k^i-nu operation of arity $k^i + n$. We argue that $f = g_{m!}$ is the operation we claimed in the statement of the lemma. Indeed, since h_x is a unary operation on an m-element set, $h_x^{m!}$ is idempotent, that is, $h_x^{m!} = h_x^{2\cdot m!}$. Then,

$$f|_0(x, f|_0(x, y)) = h_x^{m!}(h_x^{m!}(y)) = h_x^{m!}(y) = f|_0(x, y). \qquad \square$$

Lemma 3.16. *Let A be a finite set of size m.*

(1) *If a clone on A contains a near-unanimity operation, then it contains a $2^{m!}$-nu operation g of arity at most $2^{m!} + m^{m^2}$ that satisfies*

$$g|_0(x, g|_0(x, y)) \approx g|_0(x, y).$$

(2) *If $g \in \mathcal{O}_A$ is a $2^{m!}$-nu operation satisfying the above identity, then there exists a set $\mathcal{G} \subseteq \langle \{g\} \rangle$ such that $\mathcal{G}$ contains an idempotent operation and $\mathsf{X}(\mathcal{G}) = \mathsf{F}_{2^{m!}-1}(\{\chi_g\})$.*

Proof. The first statement follows immediately from Lemmas 3.13 and 3.15. To prove the second statement, let g be a $2^{m!}$-nu operation of arity $2^{m!} + k$ that satisfies the identity of the lemma. If g is a near-unanimity operation, then we can choose $\mathcal{G} = \{g\}$. Thus assume that g is not a near-unanimity operation. By induction, we define a sequence of operations $g_i \in \langle \{g\} \rangle$

$(i = 1, 2, \dots)$ of arity $i(2^{m!} - 1) + 1 + k$, respectively. Put $g_1 = g$, and for all positive integers i define

$$\begin{aligned} g_{i+1}(x_0, \dots, x_{(i+1)(2^{m!}-1)}, y_0, \dots, y_{k-1}) \\ = g_i\big(g(x_0, \dots, x_{2^{m!}-1}, y_0, \dots, y_{k-1}), \\ x_{2^{m!}}, \dots, x_{(i+1)(2^{m!}-1)}, y_0, \dots, y_{k-1}\big). \quad (3.16a) \end{aligned}$$

We claim that each g_i is a $(i(2^{m!} - 1) + 1)$-nu operation and $g_i|_0 = g|_0$. This holds trivially for g_1. We prove this by induction, so assume that the claim holds for g_i. Clearly, g_{i+1} is idempotent. If $0 \leq j < 2^{m!}$, then

$$g_{i+1}|_j(x, y) \approx g_i|_0(x, g|_j(x, y)) \approx g|_0(x, g|_0(x, y)) \approx g|_0(x, y),$$

where the first identity follows from (3.16a), $g_i|_0 = g|_0$ by the induction assumption, $g|_j = g|_0$ since g is a $2^{m!}$-nu operation, and finally the last identity was assumed in the statement of the lemma. On the other hand, if $2^{m!} \leq j \leq (i + 1)(2^{m!} - 1)$, then

$$g_{i+1}|_j(x, y) \approx g_i|_{j-(2^{m!}-1)}(x, y) \approx g|_0(x, y),$$

where the first identity holds because the first argument of g_i on the right hand side of equation (3.16a) is $g(x, \dots, x) \approx x$, and the variable x_j is at the $j - (2^{m!} - 1)$-th argument of g_i. Finally, if $(i + 1)(2^{m!} - 1) < j \leq (i + 1)(2^{m!} - 1) + k$, i.e., we plug in y into one of the y coordinates in equation (3.16a) and x everywhere else, then we get $g_{i+1}|_j(x, y) \approx x$, because $g|_{j-i(2^{m!}-1)}(x, y) \approx x$ and $g_i|_{j-(2^{m!}-1)}(x, y) \approx x$. This finishes the proof of the claim.

From the claim it immediately follows that

$$\chi_{g_i}(b) = \begin{cases} \omega & \text{if } b(x, y) \approx x, \\ i(2^{m!} - 1) + 1 & \text{if } b(x, y) \approx g|_0(x, y), \\ 0 & \text{otherwise}, \end{cases}$$

which is well defined, because $g|_0(x, y) \not\approx x$ since we assumed that g is not a near-unanimity operation. Now put $\mathcal{G} = \{g_1, g_2, \dots\}$. Clearly, $\mathsf{X}(\mathcal{G}) = \mathsf{F}_{2^{m!}-1}(\{\chi_g\})$. $\square$

Theorem 3.17. *Given a finite set A and a finite set $\mathcal{F}$ of operations on A, it is decidable whether the clone generated by $\mathcal{F}$ contains a near-unanimity operation.*

Proof. Put $m = |A|$. First we check if $\langle \mathcal{F} \rangle$ contains a $2^{m!}$-nu operation of arity at most $2^{m!} + m^{m^2}$ that satisfies the identity of Lemma 3.16. If such an operation is not found, then $\langle \mathcal{F} \rangle$ cannot have a near-unanimity operation. If $g \in \langle \mathcal{F} \rangle$ is such an operation, then by the same lemma we know that there exists a set $\mathcal{G} \subseteq \langle \{g\} \rangle \subseteq \langle \mathcal{F} \rangle$ of operations such that $\mathcal{G}$ contains an idempotent operation and $\mathsf{X}(\mathcal{G}) = \mathsf{F}_{2^{m!}-1}(\{\chi_g\})$. We do not need to "compute" the set $\mathcal{G}$, in fact it is infinite. Then by Lemma 3.11, the minimal elements of the order filter

$$\mathcal{U} = \bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}\mathsf{F}_{2^{m!}-1}(\{\chi_g\}) = \bigcup_{n\in\omega} \mathsf{C}^n_{\mathcal{F}}\mathsf{X}(\mathcal{G})$$

can be effectively computed. By Lemma 3.7, the clone $\langle\mathcal{F}\rangle$ contains a near-unanimity operation if and only if $\chi_{\mathbf{nu}} \in \mathcal{U}$. But this can be easily checked if we know the minimal elements of $\mathcal{U}$. In fact, $\chi_{\mathbf{nu}}$ is minimal in $\langle\mathcal{X}_A; \sqsubseteq_{2^{m!}-1}\rangle$, and therefore must be among the minimal elements of $\mathcal{U}$. $\square$

References

[1] L. M. Bobek: *Groups Acting on Join Semilattices.* Ph.D. dissertation, Browling Gree State University, 1992.

[2] S. Burris and H. P. Sankappanavar: *A course in universal algebra.* Graduate Texts in Mathematics, Springer-Verlag, New York, 1981.

[3] S. Burris and M. Valeriote: *Expanding varieties by monoids of endomorphisms.* Algebra Universalis **17** (1983), 150–169.

[4] B. A. Davey: *Duality theory on ten dollars a day.* Algebras and Orders (Montreal, 1991), NATO Advanced Study Institute Series, Series C, **389**, 71–111.

[5] B. A. Davey, L. Heindorf and R. McKenzie: *Near unanimity: an obstacle to general duality theory* Algebra Universalis, **33** (1995), 428–439.

[6] B. A. Davey and H. Werner: *Dualities and equivalences for varieties of algebras.* Contributions to lattice theory (Szeged, 1980), Colloq. Math. Soc. János Bolyai, **33** (1983), 101–275.

[7] R. El Bashir and T. Kepka: *Commutative semigroups with few invariant congruences.* Semigroup Forum **64** (2002), 453–471.

[8] T. Feder and M. Y. Vardi: *The computational structure of monotone monadic SNP and constraint satisfaction: A study through Datalog and group theory.* SIAM Journal of Computing **28** (1998), no. 1, 57–104.

[9] D. Hobby and R. McKenzie: *The structure of Finite algebras.* Contemporary Mathematics **76**, American Mathematical Society, Providence, RI, 1988.

[10] P. Jeavons, D. Cohen and M. C. Cooper: *Constraints, consistency and closure.* Artificial Intelligence **101** (1998), 251–265.

[11] J. Ježek: *Simple semilattices with two commuting automorphisms.* Algebra Universalis **15** (1982), 162–175.

[12] J. Ježek: *Subdirectly irreducible semilattices with an automorphism.* Semigroup-Forum **43** (1991), 178–186.

[13] J. Ježek and M. Maróti: *Membership problems for finite entropic groupoids.* (manuscript).

[14] K. A. Kearnes: *Semilattice modes I. The associated semiring, II. The amalgamation property.* Algebra Universalis **34** (1995), 200–303.

[15] K. A. Kearnes and Á. Szendrei: *Self-rectangulating varieties of type* **5**. Int. Journal on Algebra and Computation **7** (1997), 511–540.

[16] O. G. Kharlampovich and M. V. Sapir: *Algorithmic problems in varieties.* Int. Journal of Algebra and Computation **5** (1995), 379–602.

[17] L. Lovász: *Kneser's Conjecture, Chromatic Numbers and Homotopy.* J. Combin. Theory, Series A, **25** (1978), 319–324.

[18] M. Maróti: *Semilattices with a group of automorphisms.* Algebra Universalis, **38** (1997), no. 3, 238–265.

[19] M. Maróti: *On the (un)decidability of a near-unanimity term.* (submitted)

[20] M. Maróti: *The existence of a near-unanimity term in a finite algebra is decidable.* (manuscript)

[21] M. Maróti: *The variety generated by tournaments.* Vanderbilt University, Ph.D. dissertation, 2002.

[22] R. McKenzie: *Is the presence of a nu-term a decidable property of a finite algebra?* October 15, 1997 (manuscript).

[23] R. McKenzie, G. McNulty and W. Taylor: *Algebras, Lattices, Varieties, Volume I.* Wadsworth & Brooks/Cole, Monterey, CA, 1987.

[24] M. L. Minsky: *Recursive unsolvability of Post's problem of "tag" and other topics in the theory of Turing Machines.* Ann. Math. **74** (1961), 437–455.

[25] M. L. Minsky: *Computations: finite and infinite machines.* Prentice-Hall, Englewood Cliffs, N.J., 1967.

[26] E. L. Post: *The two-valued iterative systems of mathematical logic.* Number 5 in Annals of Math. Studies. Princeton Univ. Press, 1941.

[27] M. O. Rabin and D. Scott: *Finite automata and their decision problems.* IBM Journal of Res. and Devel. **3** (1969), no. 2, 114–125.

[28] A. Romanowska: *An introduction to the theory of modes and modals.* Proceedings of the International Conference on Algebra (Novosibirsk, 1989), Contemporary Mathematics **131** (1992), Part 3, 241–262.

[29] A. Romanowska and J. D. H. Smith: *Modal theory: an algebraic approach to order, geometry, and convexity.* Research and Exposition in Mathematics vol. **9**, Heldermann Verlag, Berlin, 1985.

[30] Á. Szendrei: *Clones in universal algebra.* Volume 99 of Séminaire de mathématiques supérieures. Les presses de l'Universit'e de Montréal, Montréal, 1986.

Summary

The three chapters of my dissertation are based on the papers [18, 19] and [20], respectively. The first paper is not related to the main topic of the dissertation—decidability problems—but gives a complete description of the simple algebras in the variety of semilattices expanded by an abelian group of automorphisms. In the second paper we study the decidability of the near-unanimity problem, posed ten years ago in [5], and prove a partial version of it to be undecidable. In the last, unpublished paper we show that the original problem, contrary to expectations, is decidable. As a consequence, we obtain the decidability of the natural duality problem for finitely generated, congruence distributive quasi-varieties.

We assume basic knowledge of universal algebra and direct the reader to either [2] or [23] for reference. Although the study of the near-unanimity problem stems from that of natural dualities (see [4, 5, 6]), the reader is not required to know this theory. For easier reference, we kept the original numbering of definitions and theorems of the dissertation.

F-semilattices

One of the primary goals of universal algebraic investigations is the full description of broad classes of algebras. According to a theorem of G. Birkhoff, in equational classes of algebras, such as in the varieties of groups, rings and lattices, every algebra can be expressed as a subdirect product of subdirectly irreducible members of the class. Therefore, these subdirectly irreducible algebras can be considered as the building blocks of varieties. The description of subdirectly irreducible algebras is particularly important because the study of many algebraic properties can be reduced to that of subdirectly irreducible algebras.

This description is trivial in the variety of semilattices because only the two-element semilattice is subdirectly irreducible. The situation is not this simple in other varieties, e.g., every subdirectly irreducible algebra in the variety generated by tournaments is a tournament, but not every algebra is [21]. There are (residually large) varieties, such as the variety generated by the quaternion group, where the subdirectly irreducible algebras form a proper class, and their full description is practically beyond hope. Therefore, in many cases we restrict ourselves to the study of simple algebras, i.e., subdirectly irreducible algebras that have only trivial congruences. Even this problem is extremely difficult in general, as witnessed by the classification of finite simple groups.

Algebras with a commuting semilattice operation, i.e., satisfying the identity

$$f(x_1 \wedge y_1, \dots, x_n \wedge y_1) \approx f(x_1, \dots, x_n) \wedge f(y_1, \dots, y_n)$$

for all basic operations f, have been studied in various forms. In many respects these algebras behave similarly to modules. For example, it is proved in [15] that if a locally finite variety of type-set $\{\mathbf{5}\}$ satisfies a term-condition similar to the term-condition for abelian algebras, then it has a semilattice term that commutes with all other term operations.

Within the class of modes—that is, idempotent algebras whose basic operations commute with each other—those having a semilattice term operation play an important role (see [28, 29]); these algebras are called semilattice modes. The structure of locally finite varieties of semilattice modes is described in [14].

An interesting class of algebras with a commuting semilattice operation arises if we add automorphisms, as basic operations, to a semilattice. This is a special case of the construction studied in [3]. In general, one can expand any variety $\mathcal{V}$ by a fixed monoid $\mathbf{F}$ of endomorphisms in a natural way. The expanded variety is the variety of $\mathcal{V}$-algebras $\mathbf{A}$ equipped with new unary basic operations, acting as endomorphisms on $\mathbf{A}$. We study only the following special case.

Definition 1.1. An algebra $\mathbf{S} = \langle S; \wedge, F\rangle$ with a binary operation $\wedge$ and a set F of unary operations is an $\mathbf{F}$-*semilattice*, if $\mathbf{F} = \langle F; \cdot, ^{-1}, \mathrm{id}\rangle$ is a group and $\mathbf{S}$ satisfies the following identities:

(1) the operation $\wedge$ is a semilattice operation,

(2) $\mathrm{id}(x) \approx x$,

(3) $f(g(x)) \approx (f \cdot g)(x)$ for all $f, g \in F$, and

(4) $f(x \wedge y) \approx f(x) \wedge f(y)$ for all $f \in F$.

Note that every semilattice can be considered as an $\mathbf{F}$-semilattice in a trivial way: every unary operation of F acts as the identity function. A much more interesting example of an $\mathbf{F}$-semilattice is the following.

Definition 1.2. For a group $\mathbf{F} = \langle F; \cdot, ^{-1}, \mathrm{id}\rangle$ let $\mathbf{P}(F) = \langle P(F); \wedge, F\rangle$ be the $\mathbf{F}$-semilattice which is defined on the set $P(F)$ of all subsets of F by setting

(1) $A \wedge B = A \cap B$ for all $A, B \subseteq F$, and

(2) $f(A) = A \cdot f^{-1}$ for all $f \in F$ and $A \subseteq F$.

Our first important statement reduces the study of subdirectly irreducible $\mathbf{F}$-semilattices to that of the subalgebras of $\mathbf{P}(F)$.

Lemma 1.6. *If $\mathbf{S}$ is a subdirectly irreducible $\mathbf{F}$-semilattice, then $\mathbf{S}$ is isomorphic to a subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$. The algebra $\mathbf{U}$ can be selected so that it has a unique element $M \subseteq F$ with the following properties:*

(1) $\mathrm{id} \in M$ *and* $M \cdot M = M$,

(2) $A = M \cdot A$ *for all* $A \in U$, *and*

(3) $M = \bigcap\{\, A \in U \mid \mathrm{id} \in A \,\}$.

In [12] J. Ježek has described all subdirectly irreducible $\langle \mathbb{Z}; + \rangle$-semilattices. Using our lemma above, we can easily describe the finite subdirectly irreducible $\mathbf{F}$-semilattices (Proposition 1.4), and all subdirectly irreducible $\mathbf{F}$-semilattices when $\mathbf{F}$ is locally finite (Corollary 1.7). In these special cases the subdirectly irreducible subalgebra $\mathbf{U}$ of $\mathbf{P}(F)$ contains the empty set and some subgroup M of $\mathbf{F}$. These elements also play an important role in the following class of simple $\mathbf{F}$-semilattices.

Definition 1.8. If $\mathbf{F}$ is a fixed group and M is a subgroup of $\mathbf{F}$, then let $\mathbf{S}_M$ denote the subalgebra of $\mathbf{P}(F)$, the elements of which are the empty set and the right cosets of M.

Thus the empty set is the least element in $\mathbf{S}_M$, and the right cosets of M are the atoms. The set F of unary operations of $\mathbf{S}_M$ acts as a transitive permutation group on the set of atoms. It is not hard to show that the algebras $\mathbf{S}_M$ are exactly those simple subalgebras of $\mathbf{P}(F)$ that have a least element and some atoms.

In [11] J. Ježek has described all simple algebras in the variety of semilattices expanded by two commuting automorphisms, that is, in the variety of $\langle \mathbb{Z} \times \mathbb{Z}; + \rangle$-semilattices. We generalize this result to arbitrary commutative groups, which is our main result in this chapter.

Definition 1.13. Let $\mathbf{F}$ be a fixed commutative group. Then for every nonconstant homomorphism β from $\mathbf{F}$ to the additive group $\langle \mathbb{R}; + \rangle$ of the real numbers let us define an $\mathbf{F}$-semilattice $\mathbf{R}_\beta = \langle \mathbb{R}; \min, F \rangle$ as follows:

(1) $\min(a, b)$ is taken with respect to the natural order of $\mathbb{R}$, and

(2) $f(a) = a - \beta(f)$ for all $f \in F$ and $a, b \in \mathbb{R}$.

Definition 1.16. A homomorphism $\beta \colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ is called *dense* if for each real number $\varepsilon > 0$ there exists an element $f \in F$ such that $0 < \beta(f) \leq \varepsilon$.

If the homomorphism β in Definition 1.13 is not dense, then the range of β is isomorphic to $\langle \mathbb{Z}; + \rangle$. We will consider this case separately:

Definition 1.18. Let $\mathbf{F}$ be a fixed commutative group. Then for every surjective homomorphism α from $\mathbf{F}$ onto the additive group $\langle \mathbb{Z}; + \rangle$ of the integers let $\mathbf{Z}_\alpha = \langle \mathbb{Z}; \min, F \rangle$ be the $\mathbf{F}$-semilattice defined as follows:

(1) $\min(a, b)$ is taken with respect to the natural order of $\mathbb{Z}$, and

(2) $f(a) = a - \alpha(f)$ for all $f \in F$ and $a, b \in \mathbb{Z}$.

Theorem 1.21. *If* $\mathbf{F}$ *is a commutative group, then every simple* $\mathbf{F}$*-semilattice is isomorphic to one of the following algebras:*

(1) $\mathbf{S}_M$, *where* M *is a subgroup of* $\mathbf{F}$,

(2) $\mathbf{Z}_\alpha$, *where* $\alpha \colon \mathbf{F} \to \langle \mathbb{Z}; + \rangle$ *is a surjective group homomorphism, and*

(3) *the subalgebras of* $\mathbf{R}_\beta$*, where* $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ *is a dense group homomorphism.*

Furthermore, these simple $\mathbf{F}$*-semilattices are pairwise nonisomorphic, except for the case when* β_1, β_2 *are dense homomorphisms,* $\mathbf{S}_1, \mathbf{S}_2$ *are subalgebras of* $\mathbf{R}_{\beta_1}, \mathbf{R}_{\beta_2}$ *respectively, and there exist real numbers* $t > 0$ *and* d *such that* $\beta_2 = t\beta_1$ *and* $S_2 = tS_1 + d$*.*

We conclude this chapter by noting that there exists a simple $\mathbf{F}$-semilattice in the nonabelian case that has a least element but no atom and its semilattice order is not linear.

Duality theory and the near-unanimity problem

General duality theory is capable of describing various well-known dualities—for example Pontryagin's, Stone's and Priestley's—between a category $\mathcal{A}$ of algebras with homomorphisms and a category $\mathcal{X}$ of topological structures with continuous structure preserving maps (see [6]). In these cases the class $\mathcal{A}$ is a quasi-variety generated by a single algebra $\mathbf{P} \in \mathcal{A}$, and $\mathcal{X}$ is the class of closed substructures of powers of an object $\underset{\sim}{\mathbf{P}} \in \mathcal{X}$ having the same underlying set as $\mathbf{P}$. Without getting into the details, we note that the points of the dual $\underset{\sim}{\mathbf{A}} \in \mathcal{X}$ of an algebra $\mathbf{A} \in \mathcal{A}$ are the homomorphisms $\varphi\colon \mathbf{A} \to \mathbf{P}$; while the elements of the dual $\mathbf{X} \in \mathcal{A}$ of a topological structure $\underset{\sim}{\mathbf{X}} \in \mathcal{X}$ are the $f\colon \underset{\sim}{\mathbf{X}} \to \underset{\sim}{\mathbf{P}}$ continuous structure preserving maps.

Example. *For the Pontryagin duality,* $\mathcal{A}$ *is the class of abelian groups,* $\mathbf{P} = \langle P; \cdot, ^{-1}, 1 \rangle$ *is the circle group on the set* $P = \{\, z \in \mathbb{C} : |z| = 1 \,\}$ *of complex numbers with multiplication,* $\mathcal{X}$ *is the category of compact topological abelian groups, and* $\underset{\sim}{\mathbf{P}} = \langle P; \cdot, ^{-1}, 1, \tau \rangle$ *where* τ *is the restriction of the natural topology of the complex plane to* P*.*

Example. *For the Stone duality,* $\mathcal{A}$ *is the category of Boolean algebras,* $\mathbf{P} = \langle \{0,1\}; \wedge, \vee, ', 0, 1 \rangle$ *is the two-element Boolean algebra,* $\mathcal{X}$ *is the category of totally disconnected Hausdorff spaces, and* $\underset{\sim}{\mathbf{P}} = \langle \{0,1\}; \tau \rangle$ *where* τ *is the discrete topology. It is easy to see that the ultra filters of a Boolean algebra* $\mathbf{A} \in \mathcal{A}$ *correspond to the homomorphisms of* $\mathbf{A}$ *onto* $\mathbf{P}$*.*

Example. *For the Priestley duality,* $\mathcal{A}$ *is the category of bounded distributive lattices,* $\mathbf{P} = \langle \{0,1\}; \vee, \wedge, 0, 1 \rangle$ *is the two-element bounded distributive lattice,* $\mathcal{X}$ *is the category of totally order-disconnected spaces, and* $\underset{\sim}{\mathbf{P}} = \langle \{0,1\}; \leq, \tau \rangle$ *where* τ *is the discrete topology. It is easy to see that the prime filters of a distributed lattice* $\mathbf{A} \in \mathcal{A}$ *correspond to the homomorphisms of* $\mathbf{A}$ *to* $\mathbf{P}$*.*

We say that an algebra $\mathbf{P}$ *admits a natural duality*, if there exists a topological structure $\underset{\sim}{\mathbf{P}}$ defined on P such that the quasi-variety generated by $\mathbf{P}$ is dually represented, as defined by duality theory, by the category $\mathcal{X}$ of closed substructures of powers of $\underset{\sim}{\mathbf{P}}$. Therefore, to leverage the power of duality, it is natural to ask which finite algebras admit a natural duality. Is this characterization possible? Is it decidable of a finite algebra $\mathbf{P}$ whether it admits a natural duality? This second question is known as the *natural duality problem*. Currently, we do not know the answer to this problem, but many expect it to be undecidable.

The natural duality problem was partially reduced to a pure algebraic problem in the following way. We call a term t of an algebra $\mathbf{P}$ a *near-unanimity term* if it satisfies the following identities:

$$t(y, x, \ldots, x) \approx t(x, y, x, \ldots, x) \approx \cdots \approx t(x, \ldots, x, y) \approx x.$$

An algebra is congruence join-semi-distributive if its congruence lattice satisfies the quasi-identity

$$x \vee y = x \vee z \implies x \vee (y \wedge z) = x \vee y.$$

B. A. Davey and H. Werner proved in [6] that in the presence of a near-unanimity term of $\mathbf{P}$, the quasi-variety $\mathcal{A}$ generated by $\mathbf{P}$ admits a natural duality. The converse was proved in [5] under the assumption that $\mathcal{A}$ is congruence join-semi-distributive:

Theorem (B. A. Davey, L. Heindorf and R. McKenzie [5]). *Let* $\mathbf{P}$ *be a finite non-trivial algebra and let* $\mathcal{A}$ *be the quasivariety generated by* $\mathbf{P}$. *The following are equivalent:*

(1) $\mathbf{P}$ *has a near-unanimity term;*

(2) $\mathbf{P}$ *admits a natural duality, and every algebra in* $\mathcal{A}$ *is congruence distributive; and*

(3) $\mathbf{P}$ *admits a natural duality, and every finite algebra in* $\mathcal{A}$ *is congruence join-semi-distributive.*

This theorem, known as the *near-unanimity obstacle theorem*, motivates the *near-unanimity problem*, the problem of deciding whether a finite algebra has a near-unanimity term. Clearly, if the arity of the near-unanimity term of $\mathbf{P}$ is known, then finding the near-unanimity term is easy by simply calculating the free algebra in $\mathcal{A}$ generated by the appropriate number of elements. The difficulty lies in the fact that we do not even have an upper bound for the arity of a possible near-unanimity term.

Near-unanimity term operations come up naturally in the study of algebras. For example, all lattices have a ternary near-unanimity term

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x).$$

From E. L. Post's classification [26] we know that almost all clones on a two element set contain a near-unanimity operation. It is also well known that an algebra having a near-unanimity term lies in a congruence distributive variety, and has a finite base of identities provided it is of finite signature (see [30]).

It is easy to decide whether the quasi-variety $\mathcal{A}$ generated by a finite algebra $\mathbf{P}$ is congruence distributive because it is enough to search for Jónsson terms among the finitely many ternary terms of $\mathbf{P}$. Therefore, by the near-unanimity obstacle theorem, if the near-unanimity problem were undecidable, then the natural duality problem would also be undecidable.

The undecidability of a partial near-unanimity term

In an attempt to prove the undecidability of the near-unanimity problem the following approach was taken by R. McKenzie.

Definition 2.1. Let $\mathbf{A}$ be a fixed finite algebra, $t(x_1, \dots, x_n)$ be a term of $\mathbf{A}$, and $S \subseteq A$. We say that t is a *partial near-unanimity term on* S if

$$t(y, x, \dots, x) = t(x, y, x, \dots, x) = \dots = t(x, \dots, x, y) = x$$

for all $x, y \in S$.

Clearly, a term of $\mathbf{A}$ is a near-unanimity term if and only if it is a partial near-unanimity term of the two-generated free algebra in the variety generated by $\mathbf{A}$ on the set $\{x, y\}$ of generators. Thus it is natural to study the decidability of the partial near-unanimity problem on some fixed subset of a finite algebra. It is proved in [22] that the existence of a partial near-unanimity term on a fixed two-element subset is undecidable. In Chapter 2 we extend this result to a subset excluding two fixed elements:

Theorem 2.2. *There exists no algorithm that can decide of a finite algebra* $\mathbf{A}$ *and two fixed elements* $r, w \in A$ *if* $\mathbf{A}$ *has a partial near-unanimity term on the set* $A \setminus \{r, w\}$.

This theorem does not seem to be significant after learning the decidability of the near-unanimity problem. Nevertheless, the methods used in the proof are interesting on their own and may be useful for the study of other decidability problems.

In the proof of this theorem we employ Minsky machines, which are equivalent to Turing machines (see [24, 25]). The "hardware" of a Minsky machine consists of a pair of *registers* that can contain arbitrary natural numbers. The "software" is a finite set of *states* containing an *initial* and a *halting state* together with a list of *commands*. There are two types of commands: the first instructs the machine to increase the value stored in one of the registers by one, and then to go to another state. The second command first checks the value stored in one of the registers; if it is zero, then the machine goes to one state; otherwise the value stored in the register is decremented by one and the machine goes to another state. The *computation* of the machine is a possibly infinite sequence of states together with the values of the registers at each step.

Since the halting problem for Minsky machines is undecidable, it is enough to construct (by an effective algorithm) for each Minsky machine $\mathcal{M}$

an algebra $\mathbf{A}(\mathcal{M})$ with two special elements $r, w \in A(\mathcal{M})$ such that $\mathbf{A}(\mathcal{M})$ has a partial near-unanimity term on the set $A(\mathcal{M}) \setminus \{r, w\}$ if and only if $\mathcal{M}$ halts.

In the construction the universe and the set of basic operations of $\mathbf{A}(\mathcal{M})$ depend on the set of states and commands of $\mathcal{M}$, respectively. Our goal is to encode the halting computation of $\mathcal{M}$ into a partial near-unanimity term. The key step is to show that given a partial near-unanimity term t on $A(\mathcal{M}) \setminus \{r, w\}$ one can reconstruct the halting computation of $\mathcal{M}$ from the term tree of t. The definition of the basic operations forces the shape of the tree to be almost "linear" with the basic operations encoding a sequence of commands of $\mathcal{M}$. With the proper definition of the basic operations, for example making their range pairwise disjoint, we can easily ensure that the sequence of states is correct except possibly those steps where the next state depends whether the content of a register is zero or not. We solve this difficulty by encoding whether the contents of registers are zero at each step together with the states. We cannot encode the actual values of the registers, which can be arbitrary large natural numbers, because $\mathbf{A}(\mathcal{M})$ must be finite. Our final task is to verify whether the sequence of states together with these special markings for zero values correspond to the halting computation of $\mathcal{M}$. We achieve this by forcing an appropriate matching of the variables of t via the known value of t at near-unanimous evaluations.

The element $w \in A(\mathcal{M})$ has (essentially) the *absorbing property*: for all basic operations $f(x_1, \ldots, x_n)$ and elements $x_1, \ldots, x_n \in A(\mathcal{M})$ the implication

$$w \in \{x_1, \ldots, x_n\} \implies f(x_1, \ldots, x_n) = w$$

holds. We use w to indicate that either the shape of t is incorrect, or the sequence of encoded states does not correspond to that of the halting computation. If some local inconsistency is detected, then one of the basic operations in the term tree returns w at an appropriate near-unanimous evaluation $(x, \ldots, x, y, x \ldots, x)$. Then the element w propagates to the root of t by the absorbing property, thus $t(x, \ldots, x, y, x, \ldots, x) = w$, which is a contradiction.

An improvement of this method might be possible to the subset $A(\mathcal{M}) \setminus \{w\}$, which could be formulated, analogously to the results in [13], as the undecidability of the near-unanimity problem for partial algebras:

Problem 1. *Given a finite partial algebra, decide whether it has a term that is defined on all near-unanimous evaluations and satisfies the near-unanimity identities.*

The decidability of a near-unanimity term

In the last chapter of the dissertation we prove the decidability of the near-unanimity problem, a rather surprising development after the negative partial results. We state this theorem in the language of clones:

Theorem 3.17. *Given a finite set A and a finite set $\mathcal{F}$ of operations on A, it is decidable whether the clone generated by $\mathcal{F}$ contains a near-unanimity operation.*

Instead of working with operations and their composition, we introduce an equivalence relation on the set of operations in such a way that

(1) the near-unanimity operations form an equivalence class of the relation,

(2) a new notion of composition can be introduced on the equivalence classes, and

(3) it is possible to algorithmically compute the closure of equivalence classes under this new notion of composition.

Based on these requirements, our next definition might not be so surprising. We will need the following notations. Let ω and ω^+ be the set of all finite and countable cardinals, respectively. Let $\mathcal{O}_A$ be the set of all operations on the set A, and for $n \in \omega$ let $\mathcal{O}_A^{(n)} = A^{A^n}$, that is, the set of all n-ary operations on A. Given an operation $f \in \mathcal{O}_A$, we consider those binary operations—called polymers—with their multiplicities that arise as $f(x, \dots, x, y, x, \dots, x)$ where the lone y is at a fixed coordinate:

Definition 3.1. For $f \in \mathcal{O}_A^{(n)}$ and $i \in \omega$, the ith *polymer* of f is $f|_i \in \mathcal{O}_A^{(2)}$ defined as

$$f|_i(x, y) = \begin{cases} f(x, \dots, x, \overset{i\text{th}}{\overbrace{y}}, x, \dots, x) & \text{if } 0 \leq i < n, \\ f(x, \dots, x) & \text{if } i \geq n, \end{cases}$$

where y occurs at the ith coordinate of f in the first case. The collection of polymers of f together with their multiplicities is the *characteristic function* of f, which is formally defined as the map $\chi_f : \mathcal{O}_A^{(2)} \to \omega^+$ where

$$\chi_f(b) = |\{ i \in \omega : f|_i = b \}| .$$

Clearly, near-unanimity operations are characterized by their polymers; namely all of them must be equal to x. Therefore, the characteristic functions of near-unanimity operations are the same and equal to

$$\chi_{\text{nu}}(b) = \begin{cases} \omega & \text{if } b(x, y) \approx x, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathcal{X}_A$ be the set of characteristic functions of operations on $\mathbf{A}$. Now the kernel of the operator

$$\mathsf{X} \colon \mathcal{O}_A \to \mathcal{X}_A, \qquad \mathsf{X} \colon f \mapsto \chi_f$$

satisfies our condition (1) stated above.

We do not give the technical definition of the composition operator $\mathsf{C}_{\mathcal{F}}$ as the following shall be sufficient. We distinguish the "outer" set $\mathcal{F} \subseteq \mathcal{O}_A$

of operations from the "inner" objects on which we apply the members of $\mathcal{F}$. For $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$ the set $\mathsf{C}_\mathcal{F}(\mathcal{G})$ contains all operations t of the form

$$t(y_1, \ldots, y_k) = f\big(g(x_{11}, \ldots, x_{1n}), \ldots, g(x_{m1}, \ldots, x_{mn})\big),$$

where $f \in \mathcal{F}$ and $g \in \mathcal{G}$ are m and n-ary operations, respectively, and $\{x_{11}, \ldots, x_{mn}\} \subseteq \{y_1, \ldots, y_k\}$. We employ the same operator symbol $\mathsf{C}_\mathcal{F}$ for characteristic functions, thus $\mathsf{C}_\mathcal{F}(\mathcal{U}) \subseteq \mathcal{X}_A$ for every $\mathcal{U} \subseteq \mathcal{X}_A$. The connection between the two composition operators, the real meaning of condition (2), is expressed by the next lemma.

Lemma 3.6. *$\mathsf{X}\mathsf{C}_\mathcal{F}(\mathcal{G}) = \mathsf{C}_\mathcal{F}\mathsf{X}(\mathcal{G})$ for all $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$.*

Up to this point, we showed that the clone $\langle \mathcal{F} \rangle$ generated by $\mathcal{F} \subseteq \mathcal{O}_A$ contains a near-unanimity operation if and only if the characteristic function χ_{nu} can be obtained from the characteristic function χ_{id} of the unary projection by finitely many applications of the composition operator $\mathsf{C}_\mathcal{F}$. However, we are still far from establishing requirement (3), our ultimate goal.

Suppose that the sets A and $\mathcal{F} \subseteq \mathcal{O}_A$ are finite, and that the clone $\langle \mathcal{F} \rangle$ contains a near-unanimity operation. Then, using a theorem of L. Lovász on the chromatic number of Kneser graphs [17], we can show that $\langle \mathcal{F} \rangle$ must contain an operation g of bounded arity (dependent only on $|A|$) that satisfies a set of technical identities similar to that of near-unanimity operations. We can effectively find g since its arity is bounded.

Recall that a partially ordered set is called *well-ordered*, if it has no infinite anti-chains and satisfies the descending chain condition, i.e., contains no strictly decreasing infinite sequence of elements. Using the properties of g, we introduce a well-ordered partial order on a special subset of $\mathcal{X}_A$. By applying the composition operator $\mathsf{C}_\mathcal{F}$ to an order filter of characteristic functions, we get another order filter whose minimal elements can be effectively computed from that of the original filter. If we apply the composition operator iteratively, we get an increasing sequence of order filters under inclusion. However, a well-ordered partially ordered set cannot have a strictly increasing infinite chain of order filters, therefore this process must terminate in finitely many steps. This proves that the closure of characteristic functions under the composition operator can be effectively calculated.

As an immediate consequence of the decidability of the near-unanimity problem and the near-unanimity obstacle theorem from [5], we also obtain the decidability of the natural duality problem for finite algebras in a congruence join-semi-distributive variety.

Since there are only finitely many algebras on a fixed n-element set whose basic operations are at most r-ary, by the decidability of the near-unanimity problem, there exists a recursive function $N(n, r)$ that puts an upper limit on the minimum arity of a near-unanimity term operation for those algebras that have one. Consequently, given an algebra $\mathbf{P}$ whose operations are at most r-ary, one can decide the near-unanimity problem by simply constructing all at most $N(|P|, r)$-ary terms and checking if one of them yields a near-unanimity operation. If no such is found, then $\mathbf{P}$ has no near-unanimity term operation. We know that such recursive function $N(n, r)$ exists, but currently we do not have a formula for one.

A very interesting group of open problems is related to the *constraint satisfaction problem*, which we do not define here and refer the reader to [8] for details. It is proved in [10] that if a set Γ of relations on a set admits a compatible near-unanimity operation, then the corresponding constraint satisfaction problem $\mathrm{CSP}(\Gamma)$ is solvable in polynomial time. Therefore, it is natural to consider the *near-unanimity problem for relations*:

Problem 2. *Given a finite set Γ of relations on a set, decide whether there exists a near-unanimity operation that is compatible with each member of Γ.*

Currently we are unable to solve this problem, even in the light of our result. We know that if a clone has a near-unanimity operation, then both the clone and its dual relational clone are finitely generated (see [30]). Inspired by this fact, we ask the following:

Problem 3. *Given a finite set of operations and a finite set of relations on the same underlying set, decide if the functional and relational clones they generate are duals of each other.*

Összefoglaló

Doktori értekezésemet a [18, 19] és [20] dolgozatok eredményeiből állítottam össze. Az első dolgozat témája nem kapcsolódik szervesen az értekezésem címét adó eldönthetőségi problémák köréhez, hanem egy speciális algebraosztály egyszerű algebráit írja le. A második dolgozatomban egy tíz éve megoldatlan eldönthetőségi problémát, az úgynevezett többségi függvény létezésének problémáját vizsgálom, és annak egy parciális változatának eldönthetetlenségét bizonyítom. A harmadik, még nem publikált dolgozatomban megmutatom, hogy az eredeti probléma a várakozásokkal ellentétben eldönthető. Ennek egyik következménye, hogy fontos algebraosztályokról, a végesen generált kongruenciadisztributív kvázivarietásokról eldönthető, hogy a klasszikus Pontrjagin-, Stone-, illetve Priestley-féle dualitásokhoz hasonlóan, topológiai módszerekkel leírhatók-e.

Doktori értekezésem megértéséhez csak az univerzális algebra alapfogalmainak ismeretére van szükség, melyek mindegyike az egyetemi tanulmányok alatt előfordul, illetve a [2] vagy [23] könyvekben fellelhető. Annak ellenére, hogy a többségi függvény létezésének problémáját a természetes dualitások elmélete motiválta (lásd [4, 5, 6]), ezen elmélet ismeretére nem lesz szükségünk. A hivatkozások megkönnyítése érdekében megtartottam az értekezésben kimondott definíciók és tételek számozását.

F-félhálók

Az univerzális algebrai vizsgálatok egyik fő célja általános algebraosztályok minél teljesebb leírása. G. Birkhoff tétele szerint az azonosságokkal definiálható algebraosztályok, mint például a klasszikus csoportok, gyűrűk, és hálók alkotta varietások minden algebrája az osztály építőköveinek tekinthető szubdirekt irreducibilis algebrák szubdirekt szorzatára bontható. Mivel nagyon sok algebrai tulajdonság vizsgálata visszavezethető szubdirekt irreducibilis algebrák vizsgálatára, fontos kutatási terület ezen algebrák leírása.

A félhálók varietásában például ez a leírás triviális, mivel csak a kételemű félháló szubdirekt irreducibilis. Máshol a helyzet nem ilyen egyszerű, mint például a turnamentek által generált varietásban [21], ahol nem minden algebra turnament, de a szubdirekt irreducibilis algebrák azok. Léteznek olyan (reziduálisan nagy) varietások is, mint például a kvaterniócsoport által generált varietás, ahol a szubdirekt irreducibilis algebrák valódi osztályt alkotnak, és valamilyen értelemben leírásuk reménytelen. Ezért sokszor az egyszerű algebrák vizsgálatára szorítkozunk, azaz olyan szubdirekt irreducibilis algebrákra, melyeknek csak triviális kongruenciái vannak. A véges egyszerű csoportok klasszifikációja mutatja legjobban, hogy még ez a probléma is milyen nehéz általában.

Több probléma vizsgálatában természetes módon kerülnek elő felcserélhető félhálóművelettel rendelkező algebrák, azaz olyan algebrák, melyekben minden $f(x_1, \ldots, x_n)$ műveletre teljesül az

$$f(x_1 \wedge y_1, \ldots, x_n \wedge y_1) \approx f(x_1, \ldots, x_n) \wedge f(y_1, \ldots, y_n)$$

azonosság. Sok tekintetben ezen algebrák nagyon hasonlóan viselkednek a modulusokhoz. Például K. Kearnes és Szendrei Ágnes [15] cikke alapján ha valamely lokálisan véges varietás a szelíd kongruenciák elmélete szerint (lásd [9]) csak **5**-ös típust tartalmaz, és teljesül benne egy speciális term-feltétel, akkor létezik olyan félháló-kifejezésfüggvénye, amely minden művelettel felcserélhető. Az olyan idempotens algebrák vizsgálatában, amelyekben az alapműveletek egymással mind felcserélhetőek, a félhálóművelettel rendelkező algebrák fontos szerepet játszanak, melyeket félhálómódoknak nevezünk. Lokálisan véges félhálómódok varietásaiban a szubdirekt irreducibilis algebrákat K. Kearnes írta le a [14] cikkben.

Érdekes, felcserélhető félhálóművelettel rendelkező algebrát kapunk, ha félhálóhoz automorfizmusokat, mint új egyváltozós műveleteket adunk hozzá. Ezt általában is elvégezhetjük [3]: minden $\mathcal{V}$ varietás természetes módon kibővíthető egy rögzített $\mathbf{F}$ automorfizmus-monoiddal úgy, hogy az $\mathbf{A} \in \mathcal{V}$ algebrákhoz olyan új egyváltozós műveleteket veszünk hozzá, amelyek endomorfizmusként hatnak $\mathbf{A}$-n. Ennek a konstrukciónak mi csak a következő speciális esetével foglalkozunk.

1.1. Definíció. A kétváltozós $\wedge$ műveletet és az F halmaz elemeivel jelölt egyváltozós műveleteket tartalmazó $\mathbf{S} = \langle S; \wedge, F\rangle$ algebrát $\mathbf{F}$-*félhálónak* nevezzük, ha $\mathbf{F} = \langle F; \cdot, ^{-1}, \mathrm{id}\rangle$ csoport, és $\mathbf{S}$-ben teljesülnek az alábbi azonosságok:

(1) a félháló-azonosságok a $\wedge$ műveletre,

(2) $\mathrm{id}(x) \approx x$,

(3) $f(g(x)) \approx (f \cdot g)(x)$ minden $f, g \in F$ műveletre, és

(4) $f(x \wedge y) \approx f(x) \wedge f(y)$ minden $f \in F$ műveletre.

Minden félháló triviális módon $\mathbf{F}$-félhálóként is tekinthető, ha az F-beli egyváltozós műveletek mindegyikét identikus leképezésnek definiáljuk. Ennél egy sokkal érdekesebb példa a következő.

1.2. Definíció. Legyen $\mathbf{F} = \langle F; \cdot, ^{-1}, \mathrm{id}\rangle$ rögzített csoport. Az F halmaz hatványhalmazán definiáljuk a $\mathbf{P}(F) = \langle P(F); \wedge, F\rangle$ $\mathbf{F}$-félhálót a következőképpen:

(1) $A \wedge B = A \cap B$ minden $A, B \subseteq F$ elemre, és

(2) $f(A) = A \cdot f^{-1}$ minden $f \in F$ műveletre és $A \subseteq F$ elemre.

Az első fontos állításunk visszavezeti a szubdirekt irreducibilis $\mathbf{F}$-félhálók vizsgálatát a fent definiált $\mathbf{P}(F)$ algebra részalgebráinak vizsgálatára.

1.6. Segédtétel. *Minden szubdirekt irreducibilis* $\mathbf{F}$*-félháló izomorf* $\mathbf{P}(F)$ *valamely* $\mathbf{U}$ *részalgebrájával, amelynek létezik egy egyértelműen meghatározott* $M \subseteq F$ *eleme, melyre a következők teljesülnek:*

(1) M *monoid, azaz* $\mathrm{id} \in M$ *és* $M \cdot M = M$,

(2) $A = M \cdot A$ *minden* $A \in U$ *elemre, és*

(3) $M = \bigcap \{ A \in U \mid \mathrm{id} \in A \}$.

Ezen segédtétel felhasználásával könnyen adódik a véges szubdirekt irreducibilis **F**-félhálók, illetve a lokálisan véges **F** csoportok esetében az összes szubdirekt irreducibilis **F**-félháló jellemzése (az 1.4. Állítás és 1.7. Következmény). Ezekben a speciális esetekben az **U** algebra tartalmazza az üres halmazt, és M részcsoport **F**-ben. Nem meglepő, hogy ezek az elemek fontos szerepet játszanak az egyszerű **F**-félhálók következő fontos osztályában is.

1.8. Definíció. Az **F** csoport minden M részcsoportjára legyen $\mathbf{S}(M)$ a $\mathbf{P}(F)$ **F**-félháló azon részalgebrája, amelynek elemei az üres halmaz és M jobb oldali mellékosztályai.

$\mathbf{S}(M)$ olyan „lapos" félháló, amelyben az üres halmaz a zéruselem, M jobb oldali mellékosztályai az atomok, és az **F** csoport tranzitív permutációcsoportként hat az atomok halmazán. Az $\mathbf{S}(M)$ algebrák pontosan azokat az egyszerű **F**-félhálókat írják le, amelyeknek a félhálórendezésre nézve van legkisebb eleme és legalább egy atomja.

J. Ježek a [11] cikkében leírta az egyszerű, két egymással is felcserélhető automorfizmussal bővített félhálókat, azaz a $\langle \mathbb{Z} \times \mathbb{Z}; + \rangle$-félhálók varietásában az egyszerű algebrákat. Ennek tetszőleges kommutatív **F** csoportra való kiterjesztése a [18] dolgozat legfontosabb eredménye. Az előző $\mathbf{S}(M)$ egyszerű **F**-félhálókon kívül a lineáris félhálórendezéssel rendelkező következő **F**-félhálók is fontos szerepet játszanak:

1.13. Definíció. A kommutatív **F** csoportnak a valós számok $\langle \mathbb{R}; + \rangle$ additív csoportjába történő minden nemtriviális β homomorfizmusára definiáljuk az $\mathbf{R}_\beta = \langle \mathbb{R}; \min, F \rangle$ **F**-félhálót a következőképpen:

(1) $\min(a, b)$ a valós számok természetes rendezése szerinti kisebbik szám, és

(2) $f(a) = a - \beta(f)$ minden $f \in F$ műveletre és $a, b \in \mathbb{R}$ számokra.

1.16. Definíció. A $\beta \colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ homomorfizmust *sűrűnek* nevezzük, ha minden valós $\varepsilon > 0$ számhoz létezik olyan $f \in F$ elem, hogy $0 < \beta(f) \leq \varepsilon$.

Ha β az 1.13. definícióban nem sűrű, akkor β képe az $\langle \mathbb{R}; + \rangle$ csoportban $\langle \mathbb{Z}; + \rangle$-szal izomorf részcsoportot alkot. Ezt külön esetnek fogjuk tekinteni:

1.18. Definíció. A kommutatív **F** csoportnak az egész számok $\langle \mathbb{Z}; + \rangle$ additív csoportjára történő minden szürjektív α homomorfizmusához definiáljuk a $\mathbf{Z}_\alpha = \langle \mathbb{Z}; \min, F \rangle$ **F**-félhálót a következőképpen:

(1) $\min(a, b)$ az egész számok természetes rendezése szerinti kisebbik szám, és

(2) $f(a) = a - \alpha(f)$ minden $f \in F$ műveletre és $a, b \in \mathbb{Z}$ számokra.

1.21. Tétel. *Ha* $\mathbf{F}$ *kommutatív csoport, akkor minden egyszerű* $\mathbf{F}$*-félháló a következő egyszerű algebrák valamelyikével izomorf:*

(1) $\mathbf{S}_M$*, ahol* M *az* $\mathbf{F}$ *csoport valamely részcsoportja,*

(2) $\mathbf{Z}_\alpha$*, ahol* $\alpha\colon \mathbf{F} \to \langle \mathbb{Z}; + \rangle$ *szürjektív csoport-homomorfizmus, és*

(3) *az* $\mathbf{R}_\beta$ *algebra bármely részalgebrája, ahol* $\beta\colon \mathbf{F} \to \langle \mathbb{R}; + \rangle$ *sűrű csoport-homomorfizmus.*

A felsorolt algebrák páronként nem izomorfak, kivéve azt az esetet, amikor β_1 *és* β_2 *sűrű csoport-homomorfizmusok,* $\mathbf{S}_1$ *és* $\mathbf{S}_2$ *rendre az* $\mathbf{R}_{\beta_1}$ *és* $\mathbf{R}_{\beta_2}$ *algebrák részalgebrái, és léteznek olyan valós* $t > 0$ *és* d *számok, hogy* $\beta_2 = t\beta_1$ *és* $S_2 = tS_1 + d$*.*

Végezetül megemlítjük, hogy a nemkommutatív eset ennél bonyolultabb. A [18] cikkben példát adunk olyan egyszerű $\mathbf{F}$-félhálóra, amelynek van legkisebb eleme, de nincs atomja, és félhálórendezése nem lineáris.

Dualitáselmélet és a többségi függvény probléma

A dualitáselmélet a klasszikus Pontrjagin-, Stone-, illetve Priestley-féle dualitás közös általánosításaként fejlődött ki (lásd [6]). Az elmélet szerint algebrák valamely $\mathcal{A}$ osztálya és a köztük létező homomorfizmusok alkotta kategória duálisan ekvivalens egy megfelelően választott topológiai struktúrák $\mathcal{X}$ osztályának és folytonos, struktúramegőrző függvényeinek kategóriájával. Az $\mathcal{A}$ osztály minden esetben valamely $\mathbf{P} \in \mathcal{A}$ algebra által generált kvázivarietás. Az $\mathcal{X}$ osztály valamely $\underset{\sim}{\mathbf{P}} \in \mathcal{X}$ topológiai struktúra hatványainak zárt részstruktúráival izomorf struktúrák osztálya. Továbbá a $\mathbf{P}$ algebra és a $\underset{\sim}{\mathbf{P}}$ topológiai struktúra alaphalmaza mindig megegyezik. A részleteket kerülve megjegyezzük, hogy az $\mathbf{A} \in \mathcal{A}$ algebra $\underset{\sim}{\mathbf{A}} \in \mathcal{X}$ duálisának pontjai a $\varphi\colon \mathbf{A} \to \mathbf{P}$ homomorfizmusok; illetve az $\underset{\sim}{\mathbf{X}} \in \mathcal{X}$ topológiai struktúra $\mathbf{X} \in \mathcal{A}$ duálisának elemei az $f\colon \underset{\sim}{\mathbf{X}} \to \underset{\sim}{\mathbf{P}}$ folytonos, struktúramegőrző függvényei.

Példa. *A Pontrjagin-féle dualitás esetében* $\mathcal{A}$ *az Abel-féle csoportok varietása,* $\mathbf{P}$ *a komplex számok multiplikatív csoportjának* $P = \{z \in \mathbb{C} : |z| = 1\}$ *részhalmazán értelmezett* $\langle P; \cdot, ^{-1}, 1 \rangle$ *egységkörcsoport,* $\mathcal{X}$ *a kompakt topologikus Abel-féle csoportok kategóriája, és végezetül* $\underset{\sim}{\mathbf{P}} = \langle P; \cdot, ^{-1}, 1, \tau \rangle$*, ahol* τ *a komplex számsík topológiájának az egységkörre való megszorítása.*

Példa. *A Stone-féle dualitás esetében* $\mathcal{A}$ *a Boole-algebrák varietása,* $\mathbf{P} = \langle \{0,1\}; \wedge, \vee, ', 0, 1 \rangle$ *a kételemű Boole-algebra,* $\mathcal{X}$ *a teljesen széteső Hausdorff-terek kategóriája, és* $\underset{\sim}{\mathbf{P}} = \langle \{0,1\}; \tau \rangle$*, ahol* τ *a diszkrét topológia. Könnyen látható, hogy az* $\mathbf{A} \in \mathcal{A}$ *Boole-algebra ultrafilterei éppen az* $\mathbf{A}$ *algebra* $\mathbf{P}$*-be menő homomorfizmusainak felelnek meg.*

Példa. *A Priestly-féle dualitás esetében* $\mathcal{A}$ *a korlátos disztributív hálók varietása,* $\mathbf{P} = \langle \{0,1\}; \wedge, \vee, 0, 1 \rangle$ *a kételemű korlátos disztributív háló,* $\mathcal{X}$ *a teljesen rendezésszéteső terek kategóriája, és* $\underset{\sim}{\mathbf{P}} = \langle \{0, 1, \}; \leq, \tau \rangle$*, ahol* τ *a* *diszkrét topológia. Könnyen látható, hogy az $\mathbf{A} \in \mathcal{A}$ korlátos disztributív háló prímfilterei éppen az $\mathbf{A}$ algebra $\mathbf{P}$-be menő homomorfizmusainak felelnek meg.*

Azt mondjuk, hogy a $\mathbf{P}$ algebra *rendelkezik természetes dualitással*, ha létezik olyan $\underset{\sim}{\mathbf{P}}$ topológiai struktúra, amelyre a dualitáselmélet által meghatározott módon, a $\mathbf{P}$ által generált $\mathcal{A}$ kvázivarietásnak a $\underset{\sim}{\mathbf{P}}$ által generált $\mathcal{X}$ kategória duális reprezentációja. Nem minden algebra rendelkezik természetes dualitással, és nem világos, hogy ez a tulajdonság egyáltalán eldönthető-e véges algebrákra. Ezt a problémát nevezzük *természetes dualitási problémának.*

Nagy áttörést jelentett a dualitáselmélet vizsgálatában a következő eredmény, amely algebrák egy jelentős osztályára a természetes dualitási problémát tisztán algebrai problémára redukálta. A $\mathbf{P}$ algebra t kifejezésfüggvényét *többségi függvénynek* nevezzük, ha az teljesíti a

$$t(y,x,\dots,x) \approx t(x,y,x,\dots,x) \approx \dots \approx t(x,\dots,x,y) \approx x$$

azonosságokat. *Egyesítés-féligdisztributívnak* nevezünk egy hálót, ha abban teljesül az

$$x \vee y = x \vee z \implies x \vee (y \wedge z) = x \vee y$$

kváziazonosság. Az $\mathbf{A} \in \mathcal{A}$ algebra *kongruencia-egyesítésféligdisztributív*, ha $\mathbf{A}$ kongruenciahálója egyesítés-féligdisztributív.

Tétel (B. A. Davey, L. Heindorf és R. McKenzie [5]). *Tetszőleges véges $\mathbf{P}$ algebrára és az általa generált $\mathcal{A}$ kvázivarietásra a következő állítások ekvivalensek:*

(1) $\mathbf{P}$ *rendelkezik többségi kifejezésfüggvénnyel.*

(2) $\mathbf{P}$ *rendelkezik természetes dualitással, és $\mathcal{A}$ minden algebrája kongruenciadisztributív.*

(3) $\mathbf{P}$ *rendelkezik természetes dualitással, és $\mathcal{A}$ minden véges algebrája kongruencia-egyesítésféligdisztributív.*

A *többségi függvény problémát* az előző tétel motiválta, ahol véges algebráról kell azt eldönteni, hogy rendelkezik-e többségi kifejezésfüggvénnyel. Természetesen, ha tudnánk a többségi függvény változóinak számát, akkor magát a többségi függvényt már könnyen megkereshetnénk, mivel a megfelelő számú elem által generált szabad algebrát egyszerű kiszámolni. A nehézséget az jelenti, hogy nem tudjuk a többségi kifejezésfüggvény változóinak számát, ha egyáltalán létezik; de még felső korlátunk sincs rá.

Többségi kifejezésfüggvénnyel rendelkező algebrák természetes módon fordulnak elő az univerzális algebra különböző területein. Például minden háló rendelkezik az

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$$

háromváltozós többségi függvénnyel. E. L. Post [26] klasszifikációjából kiderül, hogy kételemű alaphalmazon majdnem minden klón tartalmaz többségi műveletet. Ismert, hogy minden többségi függvénnyel rendelkező algebra kongruenciadisztributív varietást generál, és véges azonosságbázissal rendelkezik (feltéve, hogy csak véges sok alapművelete van).

Könnyen eldönthető, hogy egy véges algebra kongruenciadisztributív varietást generál-e, mert elég a véges sok háromváltozós kifejezésfüggvény között Jónsson-függvényeket keresni. Ha a többségi függvény probléma eldönthetetlen lenne, akkor az előző megjegyzések alapján a többségi függvény probléma kongruenciadisztributív varietást generáló algebrákra is eldönthetetlen volna, és a tétel szerint így a természetes dualitási probléma is eldönthetetlen lenne.

A parciális többségi függvény eldönthetetlensége

R. McKenzie a következő megközelítéssel próbálta a többségi függvény problémának az eldönthetetlenségét bizonyítani:

2.1. Definíció. Legyen $t(x_1, \ldots, x_n)$ az $\mathbf{A}$ algebra kifejezésfüggvénye, és legyen $S \subseteq A$. Azt mondjuk, hogy t *parciális többségi függvény az S halmazon*, ha a

$$t(y, x, \ldots, x) = t(x, y, x, \ldots, x) = \cdots = t(x, \ldots, x, y) = x$$

egyenlőség teljesül minden $x, y \in S$ elemre.

Könnyen látható, hogy a t kifejezésfüggvény akkor és csak akkor többségi függvénye az $\mathbf{A}$ algebrának, ha az $\mathbf{A}$ által generált varietás két elem által generált szabad algebrájában t parciális többségi függvény a generáló elemek $\{x, y\}$ halmazán. Talán ez motiválta a parciális többségi függvény eldönthetőségét vizsgáló [22] cikket, amelyben R. McKenzie bebizonyítja, hogy a parciális többségi függvény létezése eldönthetetlen kételemű részhalmazokra. A disszertáció második fejezetében ezt az eredményt terjesztem ki olyan részhalmazokra, amely az algebra két elemén kívül minden más elemet tartalmaz.

2.2. Tétel. *Nem létezik olyan algoritmus, amely tetszőleges véges $\mathbf{A}$ algebráról és $r, w \in A$ elemekről eldöntené, hogy $\mathbf{A}$ rendelkezik-e parciális többségi kifejezésfüggvénnyel az $A \setminus \{r, w\}$ halmazon.*

Ez a tétel nem tűnik jelentősnek utólag, a többségi függvény létezésének eldönthetőségét ismerve. Mindenesetre a bizonyításban használt technikák önmagukban is érdekesek, és esetleg hasznosak lehetnek más kifejezésfüggvények létezésével foglalkozó problémák eldönthetőségének vizsgálatakor.

A bizonyításban Minsky-gépeket használunk, amelyek lényegében ekvivalensek a Turing-gépekkel (lásd [24, 25]). A Minsky-gép végtelen szalag helyett csak két *regiszterrel* rendelkezik, amelyek tetszőleges nemnegatív egész értéket vehetnek fel. A gép programja *állapotok*, köztük egy *kezdő-* és egy *leállóállapot*, illetve *parancsok* véges halmazaiból áll. Kétféle parancs van: az első az adott állapotban az egyik regiszter aktuális értékét eggyel megnöveli, majd a gépet egy új állapotba lépteti. A másik fajta parancs végrehajtásakor a gép először megnézi, hogy milyen érték van az adott regiszterben; ha az nem nulla, akkor a gép azt eggyel csökkenti, és új állapotba lép; ha nulla, akkor egy másik állapotba lép. A gép *számításán* a gép állapotainak és regiszterei értékeinek a lépések során felvett (akár végtelen) sorozatát értjük.

Mivel a Minsky-gépek megállási problémája eldönthetetlen, ezért minden $\mathcal{M}$ Minsky-géphez elég (egy algoritmus segítségével leírható) olyan speciális r, w elemekkel rendelkező $\mathbf{A}(\mathcal{M})$ algebrát definiálni, amelynek akkor és csak akkor van parciális többségi kifejezésfüggvénye az alaphalmaz $A(\mathcal{M}) \setminus \{r, w\}$ részhalmazán, ha $\mathcal{M}$ megáll.

Az $\mathbf{A}(\mathcal{M})$ algebra konstruckiójában az alaphalmaz, illetve a műveletek halmaza rendre $\mathcal{M}$ állapotainak, illetve parancsainak halmazától függ. A konstrukcióban az a célunk, hogy $\mathcal{M}$ megálló számítását bekódoljuk $\mathbf{A}(\mathcal{M})$ valamely parciális többségi kifejezésfüggvényébe. A bizonyítás legkritikusabb része az, amikor megmutatjuk, hogy $\mathcal{M}$ megálló számítása felfedezhető minden olyan t kifejezésfüggvény alapműveletekből felépített fájában, amely az $A(\mathcal{M}) \setminus \{r, w\}$ halmazon parciális többségi függvény. Az alapműveletek megfelelő definíciójával elérhető, hogy ilyen esetben t lényegében lineáris szerkezetű legyen, amely $\mathcal{M}$ állapotainak egy sorozatát kódolja. Megfelelően definiálva az alapműveleteket, például úgy, hogy a különböző műveletek értékkészlete különböző legyen, könnyen elérhető az is, hogy az állapotok sorozata lényegében helyes legyen azt az esetet kivéve, amikor a következő állapot attól függ, hogy a regiszter tartalma nulla-e vagy nem. Ezt a problémát úgy oldjuk meg, hogy az állapotok mellé meg azt is bekódoljuk, hogy az adott lépésben az egyes regiszterek értéke nulla-e. Természetesen a regiszter pillanatnyi értékét, ami tetszőlegesen nagy természetes szám lehet, nem tudjuk bekódólni, mivel az $\mathbf{A}(\mathcal{M})$ algebrának csak véges sok eleme és művelete lehet. Már csak azt kell ellenőriznünk, hogy a fában kódolt állapotok és a regiszterek nulla értékét jelző kódok a Minsky-gép számításának megfelelően vannak-e elhelyezve. Ezt a fában előforduló változók megfelelő párosításával oldjuk meg, felhasználva azt, hogy ismerjük t értékét a parciális többségi függvény által előírt helyeken.

A $w \in A(\mathcal{M})$ elemnek (lényegében) megvan az úgynevezett *elnyelő tulajdonsága*, azaz minden $f(x_1, \ldots, x_n)$ alapműveletre a

$$w \in \{x_1, \ldots, x_n\} \implies f(x_1, \ldots, x_n) = w$$

tulajdonság teljesül. Az alkalmazott módszer a w elem segíségével jelzi, ha a t kifejezésfüggvény alakja vagy az általa bekódolt állapotsorozat nem felel meg a megálló számításnak. Ha valahol eltérés van, akkor a fában levő valamely alapművelet a megfelelő többségi $(x, \ldots, x, y, x, \ldots, x)$ kiértékelésnél a w elemet adja vissza, ami automatikusan terjed a fában a gyökér felé. Ebből az következne, hogy $t(x, \ldots, x, y, x, \ldots, x) = w$, ami pedig ellentmondás.

Valószínű, hogy a 2.2. tételt ki lehet terjeszteni az alaphalmaz csak egyetlenegy elemét, w-t kizáró részhalmazára, amit a [13] kézirat eredményéhez hasonlóan, legegyszerűbben parciális algebrákra lehet megfogalmazni:

1. Probléma. *Véges parciális algebráról eldönthető-e az, hogy rendelkezik olyan kifejezésfüggvénnyel, amely minden többségi kiértékelésnél értelmezve van, és teljesíti a többségi függvény azonosságait?*

A többségi függvény eldönthetősége

A disszertáció utolsó fejezetében bebizonyítom, hogy a többségi függvény probléma eldönthető. Mivel a bizonyítás során a klónok nyelvezetét használom, magát a tételt is így mondom ki:

3.17. Tétel. *Véges halmazon definiált véges sok műveletről eldönthető, hogy az általuk generált klón tartalmaz-e többségi függvényt.*

A bizonyítás a következő ötletre épül. A műveletek és a rajtuk értelmezett kompozícióoperátor használata helyett a műveletek olyan osztályozását keressük, amelyben

(1) a többségi függvények az osztályozás egyik blokkját alkotják,

(2) a blokkok halmazán be lehet vezetni a kompozíció fogalmát, és

(3) elég kevés blokk van ahhoz, hogy véges lépésben meg lehessen határozni a blokkok kompozícióra zárt halmazait.

Ezek alapján talán nem annyira meglepő a következő definíció, melynek kimondásához szükséges néhány jelölés bevezetése. Legyen ω, illetve ω^+ rendre a véges, illetve megszámlálható számosságok halmaza. Az A halmazon értelmezett műveletek halmazát $\mathcal{O}_A$-val jelöljük, továbbá minden $n \in \omega$ egészre legyen $\mathcal{O}_A^{(n)} = A^{A^n}$, ami az A halmazon értelmezett n-változós műveletek halmaza.

3.1. Definíció. Minden $f \in \mathcal{O}_A^{(n)}$ műveletre és $i \in \omega$ egészre definiáljuk az f művelet i-edik *polimerjének* nevezett $f|_i \in \mathcal{O}_A^{(2)}$ kétváltozós műveletet:

$$f|_i(x,y) = \begin{cases} f(x,\dots,x,\overset{i.}{\overbrace{y}},x,\dots,x) & \text{ha } 0 \le i < n, \\ f(x,\dots,x) & \text{ha } i \ge n, \end{cases}$$

ahol y az i-edik pozícióban szerepel az első esetben. Az f művelet polimerjeinek multihalmazát f *karakterisztikus függvényének* nevezzük, ami formálisan a

$$\chi_f(b) = |\{\, i \in \omega : f|_i = b \,\}|$$

formula által definiált $\chi_f \colon \mathcal{O}_A^{(2)} \to \omega^+$ leképezés.

Könnyen belátható, hogy a többségi függvények jellemezhetőek polimerjeik segítségével úgy, hogy minden polimernek x-szel kell egyenlőnek lennie. Következésképp az összes többségi függvénynek ugyanaz a χ_{nu} leképezés a karakterisztikus függvénye, amelyet a

$$\chi_{\mathrm{nu}}(b) = \begin{cases} \omega & \text{ha } b(x,y) \approx x, \\ 0 & \text{egyébként} \end{cases}$$

formula definiál. Legyen $\mathcal{X}_A$ az A halmazon értelmezett műveletek karakterisztikus függvényeinek halmaza. Tehát a karakterisztikusfüggvény-képzés

$$\mathsf{X}\colon \mathcal{O}_A \to \mathcal{X}_A, \qquad \mathsf{X}\colon f \mapsto \chi_f$$

operátorának magja teljesíti az (1)-es célkitűzésünket.

A $\mathsf{C}_{\mathcal{F}}$ kompozícióoperátor technikai definícióját itt nem adjuk meg. Elég most annyit tudnunk róla, hogy megkülönböztetjük a „külső" $\mathcal{F} \subseteq \mathcal{O}_A$ műveleteket azoktól a „belső" elemektől, amelyekre az $\mathcal{F}$-beli műveleteket alkalmazzuk. Műveletek minden $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$ halmazaira $\mathsf{C}_{\mathcal{F}}(\mathcal{G})$ tartalmazza az összes olyan

$$t(y_1, \ldots, y_k) = f\big(g(x_{11}, \ldots, x_{1n}), \ldots, g(x_{m1}, \ldots, x_{mn})\big)$$

műveletet, ahol $f \in \mathcal{F}$ és $g \in \mathcal{G}$ rendre m- és n-változós műveletek, továbbá $\{x_{11}, \ldots, x_{mn}\} \subseteq \{y_1, \ldots, y_k\}$. A karakterisztikus függvények kompozícióoperátorának jelölésére is ugyanazt a $\mathsf{C}_{\mathcal{F}}$ szimbólumot használjuk: így minden $\mathcal{U} \subseteq \mathcal{X}_A$ halmazra $\mathsf{C}_{\mathcal{F}}(\mathcal{U}) \subseteq \mathcal{X}_A$. A két kompozícióoperátor közötti kapcsolatot, a (2)-es célkitűzés valódi tartalmát, a következő segédtétel fejezi ki.

3.6. Segédtétel. $\mathsf{X}\mathsf{C}_{\mathcal{F}}(\mathcal{G}) = \mathsf{C}_{\mathcal{F}}\mathsf{X}(\mathcal{G})$ *tetszőleges* $\mathcal{F}, \mathcal{G} \subseteq \mathcal{O}_A$ *halmazokra.*

Az eddigiek alapján az $\mathcal{F}$ műveletek által generált $\langle \mathcal{F} \rangle$ klón akkor és csak akkor tartalmaz többségi függvényt, ha az egyváltozós projekció χ_{id} karakterisztikus függvényéből kiindulva a $\mathsf{C}_{\mathcal{F}}$ kompozícióoperátor véges sokszori alkalmazásával χ_{nu} megkapható. Sajnos a (3)-as célkitűzés megvalósításától még nagyon messze vagyunk; valójában annak csak egy gyengített változatát bizonyítjuk.

Tegyük fel, hogy mind az A alaphalmaz, mind az $\mathcal{F} \subseteq \mathcal{O}_A$ műveletek halmaza véges, továbbá azt, hogy $\langle F \rangle$ tartalmaz többségi függvényt. Lovász Lászlónak a Kneser-gráfok kromatikus számáról szóló tételét (lásd [17]) felhasználva megmutatható, hogy $\langle F \rangle$-nek tartalmaznia kell a többségi függvény azonosságaihoz nagyon hasonló technikai feltételt teljesítő g műveletet is, amelynek változószáma csak A elemszámától függ, így az megkereshető.

A g művelet segítségével egy jólrendezett parciális rendezést definiálunk a karakterisztikus függvények valamely részhalmazán. Megmutatjuk, hogy ha a kompozícióoperátort (karakterisztikus függvényekből álló) filterre alkalmazzuk, akkor ismét filtert kapunk. A kapott filter minimális elemei (melyek száma szükségképpen véges) az eredeti filter minimális elemeiből kiszámíthatók. Ha a kompozícióoperátort ismételten alkalmazzuk, akkor filterek egy, a tartalmazásra nézve bővülő láncát kapjuk. Ismert azonban, hogy jólrendezett parciális rendezés filterei nem alkothatnak végtelen, szigorúan bővülő láncot, tehát ennek az eljárásnak véges lépésben meg kell állnia, és így a karakterisztikus függvények kompozícióoperátor szerinti lezártja kiszámítható.

Ahogy már utaltunk rá, az [5] cikk eredményét felhasználva a bizonyított tétel következményeként azt is megkaptuk, hogy kongruencia-egyesítés-féligdisztributív varietásba tartozó véges algebrákra a természetes dualitás problémája eldönthető.

Mivel legfeljebb r-változós műveletekkel rendelkező algebrából csak véges sok definiálható egy n-elemű halmazon, a többségi függvény eldönthetőségéből az is következik, hogy létezik olyan $N(n, r)$ rekurzív függvény, amely felülről korlátozza a többségi függvénnyel rendelkező ilyen algebrák többségi függvényeinek minimális változószámát. Következésképpen, minden ilyen $\mathbf{A}$ algebrára elég a legfeljebb $N(n, r)$ változójú kifejezésfüggvények között keresni a többségi függvényt. Ha ilyet nem találunk, akkor $\mathbf{A}$-nak nincs többségi kifejezésfüggvénye. Tudjuk, hogy létezik ilyen rekurzív függvény, de egyelőre nincs rá formulánk.

Nagyon érdekes megoldatlan probléma kapcsolódik az úgynevezett kényszerkielégíthetőségi problémához (constraint satisfaction problem). A problémát itt mi nem definiáljuk; az érdeklődő olvasónak T. Feder és M. Y. Vardi [8] cikkét ajánljuk. A [10] cikk eredménye szerint, ha relációk egy Γ halmazának van kompatibilis többségi függvénye, akkor a CSP(Γ) kényszerkielégíthetőségi probléma polinomiális időben megoldható. Ezért (is) érdekes a többségi függvény relációkra vonatkoztatott problémája:

2. Probléma. *Véges halmazon értelmezett relációk véges halmazáról eldönthető-e, hogy létezik a relációkkal kompatibilis többségi függvény?*

Egyelőre nem ismerjük erre a problémára a választ. Tudjuk azt (lásd pl. [30]), hogy ha relációk (akár végtelen) Γ halmazához létezik kompatibilis többségi függvény, akkor mind a Γ által generált relációklón, mind a relációkkal kompatibilis műveletek klónja végesen generált. Utolsó problémánk ehhez a kérdéskörhöz kapcsolódik:

3. Probléma. *Véges, közös alaphalmazon értelmezett műveletek $\mathcal{F}$ és relációk Γ halmazairól eldönthető-e, hogy az $\langle \mathcal{F} \rangle$ klón megegyezik a Γ-val kompatibilis műveletek klónjával?*