

ON THE (UN)DECIDABILITY OF A NU-TERM

MIKLÓS MARÓTI

ABSTRACT. We investigate two problems: the natural duality problem (given a finite algebra \mathbf{P} , decide if the quasi-variety generated by \mathbf{P} is dualizable) and the near-unanimity problem (given a finite algebra, decide if it has a near-unanimity term of finite arity). These problems are intimately related to each other as described in [2]. We prove that a partial version of the second problem is undecidable. On the other hand, we present results towards proving the decidability of the general problem.

1. INTRODUCTION

General duality theory is capable of describing various well-known dualities—for example Stone’s and Priestley’s, among others—between categories of algebras and topological structures. The classes of algebras under consideration are quasi-varieties generated by some finite algebra \mathbf{P} (the class of algebras embeddable into powers of \mathbf{P}). By this theory, not every quasi-variety admits a natural duality. Therefore, to leverage the power of duality, we need to characterize those finitely generated quasi-varieties that 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 problem was partially reduced to a pure algebraic problem in the following way.

Definition 1.1. Let \mathbf{P} be an algebra and $t(x_1, \dots, x_n)$ be a term of \mathbf{P} . We say that t is a *near-unanimity term* if $t(y, \dots, y, x_i, y, \dots, y) = y$ for all $1 \leq i \leq n$ and $x_i, y \in P$.

For brevity, we sometimes write NU-term instead of near-unanimity term. It was already known (B. Davey [2]) that in the presence of a near-unanimity term of \mathbf{P} , the quasi-variety \mathcal{A} generated by \mathbf{P} admits

Date: September 3, 2000.

a natural duality. The converse was proved in [3] under the assumption that \mathcal{A} is congruence distributive: if \mathcal{A} admits a natural duality and is congruence distributive then \mathbf{P} has a (finitary) near-unanimity term. This implies that if it is undecidable whether a finite algebra has a near-unanimity term, then the natural duality problem is also undecidable. We call the premise of this implication the *near-unanimity problem*. It became apparent that we do not know much about the near-unanimity problem.

In [7] R. McKenzie proved that it is undecidable if a finite algebra \mathbf{P} has a term t that behaves as a near-unanimity term on a fixed two-element subset of P . The key development presented in this article is the improvement of this result to a fixed $n - 2$ element subset where $n = |P|$, and the simplification of his elaborate construction. 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. This probably prevents the further improvement of this approach to prove the undecidability of the near-unanimity problem. However, an improvement to $n - 1$ elements might be possible, which could be formulated as the undecidability of the near-unanimity problem for partial algebras (as in [5]).

It is natural to attack the near-unanimity problem from the other perspective, as well: try to prove that it is decidable. We have tried the divide-and-conquer approach using Rosenberg's characterization of maximal clones. It turns out that in three of the six classes of maximal clones the problem is decidable. If we restrict ourselves to idempotent algebras then we can further eliminate one of the three remaining classes. The idempotent case is still not solved, however. The best result, in this case, is obtained using Á. Szendrei's characterization of idempotent strictly simple term minimal algebras [14].

The near-unanimity problem is non-trivial, and intrinsically interesting for algebraists. Maybe its decidability will be proved by topological methods via the theory of natural dualities.

In the next section we review the framework of natural duality theory. We assume basic knowledge of topology and category theory. The reader may skip this section if only the near-unanimity problem is in her interest, or consult [2] and [3] for a detailed discussion of the subject and for references. In Section 3 we will introduce Minsky machines and prove their equivalence with Turing machines. The section is self

contained, assumes only knowledge of the concept of Turing machine. We prove the undecidability of the near-unanimity problem on an $n - 2$ element subset in Section 4. Only the definition of the Minsky machine is required. The last section begins with the review of Rosenberg's theorem, and then its application to the near-unanimity problem. Finally, the case when \mathbf{P} is idempotent is considered. This is the only section in which knowledge of universal algebra is assumed. We refer the reader to either [1] or [8] for the basic definitions.

I am indebted to R. McKenzie for the invaluable conversations, and Á. Szendrei and J. Ježek for their useful comments and directions.

2. NATURAL DUALITY

Duality theory grew out of a few classical special cases; Pontryagin's duality for abelian groups, Stone's duality for Boolean algebras and Priestley's duality for distributive lattices. Each of these dualities establishes a connection between a category \mathcal{A} of algebras with homomorphisms and a category \mathcal{X} of topological structures with continuous structure preserving maps. Surprisingly, 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 a single object $\tilde{\mathbf{P}} \in \mathcal{X}$. Moreover, the structures \mathbf{P} and $\tilde{\mathbf{P}}$ have the same underlying set.

In this section, first we review the general framework of natural duality and present a few examples. Then we jump to the NU-Obstacle Theorem, which provides the bridge between natural duality and near-unanimity. One of the consequences of this connection is that undecidability of the near-unanimity problem yields the undecidability of the natural duality problem.

Let $\mathbf{P} = \langle P; F \rangle$ be a finite, non-trivial algebra, and $\mathcal{A} = \mathbb{ISP}(\mathbf{P})$ be the quasi-variety generated by \mathbf{P} . The morphisms of \mathcal{A} are the (algebraic) homomorphisms.

Definition 2.1. We say that the structure $\tilde{\mathbf{P}} = \langle P; G, H, R, T \rangle$ is *algebraic over \mathbf{P}* if the following conditions hold.

- (1) The underlying set of $\tilde{\mathbf{P}}$ is the same as of \mathbf{P} .
- (2) G is a set of (total) operations on P such that if $g \in G$ is n -ary then $g : \mathbf{P}^n \rightarrow \mathbf{P}$ is a homomorphism. (If $n = 0$ then this means that $\{g\}$ is a subalgebra of \mathbf{P} .)
- (3) H is a set of partial operations on P (of arity at least 1) such that if $h \in H$ is n -ary then the domain, $\text{dom}(h)$, of h is a

(non-empty) subalgebra of \mathbf{P}^n and $h : \text{dom}(h) \rightarrow \mathbf{P}$ is a homomorphism.

- (4) R is a set of finitary relations on P (of arity at least 1) such that if $r \in R$ is n -ary then r is a subalgebra of \mathbf{P}^n .
- (5) \mathcal{T} is the discrete topology on P .

If one wishes to include examples where \mathbf{P} is infinite, then we must assume that \mathcal{T} is a compact Hausdorff topology and that each operation in F is continuous with respect to \mathcal{T} . We will not take this route, however, and must refer the reader to [2] for further information.

To specify the other category \mathcal{X} of topological structures we need the following definitions.

Definition 2.2. Let S be a set. The *power* \mathbf{P}^S of \mathbf{P} is a structure on the power-set P^S and of the same type as \mathbf{P} . The operations, partial operations, relations and topology are all defined in the obvious point-wise manner. In particular, the domain of an n -ary partial operation $h \in H$ on P^S is

$$\{ \langle x_1, \dots, x_n \rangle \in (P^S)^n : \langle x_1(s), \dots, x_n(s) \rangle \in \text{dom}(h) \text{ for all } s \in S \},$$

and the topology on P^S is the product topology.

Definition 2.3. Let \mathbf{X} and \mathbf{Y} be topological structures of the same type as \mathbf{P} . We say that \mathbf{X} is a *substructure* of \mathbf{Y} if

- (1) $\emptyset \neq X \subseteq Y$;
- (2) if $g \in G$ is n -ary then $g^{\mathbf{X}}(x_1, \dots, x_n) = g^{\mathbf{Y}}(x_1, \dots, x_n)$ for all $x_1, \dots, x_n \in X$;
- (3) if $h \in H$ is n -ary then $\text{dom}(h^{\mathbf{X}}) = \text{dom}(h^{\mathbf{Y}}) \cap X^n$ and for all $x_1, \dots, x_n \in X$, $h^{\mathbf{X}}(x_1, \dots, x_n) = h^{\mathbf{Y}}(x_1, \dots, x_n)$;
- (4) if $r \in R$ is n -ary then $r^{\mathbf{X}} = r^{\mathbf{Y}} \cap X^n$;
- (5) $\mathcal{T}^{\mathbf{X}}$ is the subspace topology induced on X by $\mathcal{T}^{\mathbf{Y}}$.

The substructure \mathbf{X} is *closed* if X is a closed set of \mathbf{Y} .

Definition 2.4. Let \mathbf{X} and \mathbf{Y} be topological structures of the same type as \mathbf{P} . A continuous map $\varphi : X \rightarrow Y$ which preserves all operations, partial operations and relations is called a *morphism*. A morphism is called *isomorphism* if it is bijective and its inverse is also a morphism.

Define $\mathcal{X} = \mathbb{I}\mathbb{S}_c\mathbb{P}(\mathbf{P})$ to be the class of all isomorphic copies of (topologically) closed substructures of powers of \mathbf{P} . So far we have defined

the categories \mathcal{A} and \mathcal{X} . Now we define the hom-functors $D : \mathcal{A} \rightarrow \mathcal{X}$ and $E : \mathcal{X} \rightarrow \mathcal{A}$.

Definition 2.5. The dual of an algebra $\mathbf{A} \in \mathcal{A}$ is the set $D(\mathbf{A}) = \mathcal{A}(\mathbf{A}, \mathbf{P}) \leq \mathbf{P}^A$ of homomorphisms from \mathbf{A} to \mathbf{P} . The dual of a homomorphism $u : \mathbf{A} \rightarrow \mathbf{B}$, where $\mathbf{A}, \mathbf{B} \in \mathcal{A}$, is the map $D(u) : D(\mathbf{B}) \rightarrow D(\mathbf{A})$ defined by $(D(u))(x) = x \circ u$. The dual of a topological structure $\mathbf{X} \in \mathcal{X}$ is the set $E(\mathbf{X}) = \mathcal{X}(\mathbf{X}, \mathbf{P}) \leq \mathbf{P}^X$ of morphisms. The dual of a morphism $\varphi : \mathbf{X} \rightarrow \mathbf{Y}$, where $\mathbf{X}, \mathbf{Y} \in \mathcal{X}$, is the map $E(\varphi) : E(\mathbf{Y}) \rightarrow E(\mathbf{X})$ defined by $(E(\varphi))(\alpha) = \alpha \circ \varphi$.

Lemma 2.6 (B. Davey [2]). *Assume that the structure on \mathbf{P} is algebraic over \mathbf{P} . Then D and E are well-defined functors between the categories \mathcal{A} and \mathcal{X} ,*

Our goal is to show that the second dual of an object is isomorphic to the original. This, however, does not follow automatically from the fact that \mathbf{P} is algebraic over \mathbf{P} . On the other hand, the original object can be embedded into its second dual.

Definition 2.7. Let $\mathbf{X}, \mathbf{Y} \in \mathcal{X}$. A morphism $\varphi : \mathbf{X} \rightarrow \mathbf{Y}$ is an *embedding* if it is an isomorphism of \mathbf{X} onto a closed substructure of \mathbf{Y} .

For all $\mathbf{A} \in \mathcal{A}$ define the evaluation map $e_{\mathbf{A}} : \mathbf{A} \rightarrow ED(\mathbf{A})$ by

$$(e_{\mathbf{A}}(a))(x) = x(a)$$

for all $a \in A$ and $x \in D(A) = \mathcal{A}(\mathbf{A}, \mathbf{P})$. Similarly, for all $\mathbf{X} \in \mathcal{X}$ define the evaluation map $\varepsilon_{\mathbf{X}} : \mathbf{X} \rightarrow DE(\mathbf{X})$ by

$$(\varepsilon_{\mathbf{X}}(x))(\alpha) = \alpha(x)$$

for all $x \in X$ and $\alpha \in E(X) = \mathcal{X}(\mathbf{X}, \mathbf{P})$.

Lemma 2.8 (B. Davey [2]). *Assume that \mathbf{P} is algebraic over \mathbf{P} . Then for all $\mathbf{A} \in \mathcal{A}$ and $\mathbf{X} \in \mathcal{X}$ the evaluation maps $e_{\mathbf{A}}$ and $\varepsilon_{\mathbf{X}}$ are embeddings.*

Definition 2.9. Assume that \mathbf{P} is algebraic over \mathbf{P} . We say that \mathbf{P} yields a *natural duality on \mathcal{A}* if for all $\mathbf{A} \in \mathcal{A}$ the evaluation map $e_{\mathbf{A}}$ is an isomorphism. The algebra \mathbf{P} *admits a natural duality* (or is *dualizable*) provided there is some structure \mathbf{P} which yields a natural duality on the quasi-variety $\mathcal{A} = \mathbb{ISP}(\mathbf{P})$ generated by \mathbf{P} .

Example 2.10 (Pontryagin duality). Denote by \mathcal{A} the class of abelian groups. The *circle group* is the subgroup $\mathbf{P} = \{z \in \mathbb{C} : |z| = 1\}$ of the group of nonzero complex numbers under multiplication. It is not hard to show that $\mathcal{A} = \mathbb{ISP}(\mathbf{P})$. To get the topological structure $\underline{\mathbf{P}}$, let \mathcal{T} be the subspace topology of \mathbb{C} , $G = \{\cdot, ^{-1}, 1\}$, and $H = R = \emptyset$. The generated class $\mathcal{X} = \mathbb{IS}_c\mathbb{P}(\underline{\mathbf{P}})$ is the category of compact topological abelian groups.

Example 2.11 (Stone duality). Let \mathbf{P} be the two-element Boolean algebra on $\{0, 1\}$, and $\underline{\mathbf{P}}$ be $\langle \{0, 1\}; \mathcal{T} \rangle$ where \mathcal{T} is the discrete topology. Then $\mathcal{A} = \mathbb{ISP}(\mathbf{P})$ is the category of Boolean algebras and $\mathcal{X} = \mathbb{IS}_c\mathbb{P}(\underline{\mathbf{P}})$ is the category of totally disconnected Hausdorff spaces. It is easy to see that the ultra filters of a Boolean algebra \mathbf{A} correspond to the homomorphisms of \mathbf{A} onto \mathbf{P} .

Example 2.12 (Priestley duality). Let $\mathbf{P} = \langle \{0, 1\}; \vee, \wedge, 0, 1 \rangle$ be the two-element bounded distributive lattice, and $\underline{\mathbf{P}} = \langle \{0, 1\}; \leq, \mathcal{T} \rangle$ where \leq is the binary order relation and \mathcal{T} is the discrete topology. Then $\mathcal{A} = \mathbb{ISP}(\mathbf{P})$ is the category of bounded distributive lattices and $\mathcal{X} = \mathbb{IS}_c\mathbb{P}(\underline{\mathbf{P}})$ is the category of totally order-disconnected spaces. It is easy to see that the prime filters of a distributed lattice \mathbf{A} correspond to the homomorphisms of \mathbf{A} to \mathbf{P} .

B. Davey and H. Warner [4] showed that if \mathbf{P} has a near-unanimity term then \mathbf{P} is dualizable, thus providing an easy route to natural-duality. But this is a two-edged sword; in the presence of even a small degree of congruence distributivity the only dualizable algebras are those which possess a near-unanimity term.

Recall that a lattice is *join-semi-distributive* if it satisfies the quasi-identity

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

Clearly, distributive lattices are join-semi-distributive. An algebra $\mathbf{A} \in \mathcal{A}$ is congruence join-semi-distributive if its congruence lattice is join-semi-distributive.

Theorem 2.13 (The NU-Obstacle Theorem, see [3]). *Let \mathbf{P} be a finite non-trivial algebra and let $\mathcal{A} = \mathbb{ISP}(\mathbf{P})$. The following are equivalent:*

- (1) \mathbf{P} has a near-unanimity term;
- (2) \mathbf{P} generates a congruence-distributive variety and \mathbf{P} admits a natural duality;
- (3) every finite algebra in \mathcal{A} is congruence join-semi-distributive and \mathbf{P} admits a natural duality.

This theorem is true in a slightly stronger form. Please consult [3] for further details.

Corollary 2.14. *If the near-unanimity problem for finite algebras is undecidable then it is also undecidable if a finite algebra is dualizable.*

Proof. Assume that it is decidable if a finite algebra is dualizable. Now we present a decision procedure for the near-unanimity problem. Take a finite algebra \mathbf{P} . By Jónsson’s theorem we can decide if the variety \mathcal{V} generated by \mathbf{P} is congruence distributive (check if the 3-generated free algebra in \mathcal{V} is congruence distributive). If it is not, then \mathbf{P} cannot have a near-unanimity term. Otherwise, check if \mathbf{P} admits a duality. If it does, then \mathbf{P} has a near-unanimity term, otherwise it does not. \square

3. MINSKY MACHINES

In mathematics we capture the concept of deterministic computation by generic “machines”. The best known example is the Turing machine, but there are several other equivalent machines. In this section we introduce one of the less known machines, the Minsky machine, which can be a very powerful tool in proving the undecidability of algebraic problems. For a beautiful survey of algorithmic problems in varieties, including applications of the Minsky machine see [6].

The Minsky machine was invented by Marvin Minsky in 1961 (see [9, 10]), but he writes that the concept was inspired by some ideas of Rabin and Scott [12]. The “canonical” definition is a two-tape non-writing machine, whose tapes are infinite to the right and bound on the left. The first cells on both tapes always contain the digit 1, and all other cells contain the digit 0. The digit 1 on each tape only serves as an indicator of the beginning of the tape. We give an equivalent definition here.

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 single command which describes the state-transition from state i together with the change of the registers’ contents. There are two types of commands:

- in state i increase register X by one and go to state j , and

- in state i if register X contains zero then go to state j otherwise decrease X by one and go to state k .

Now we give the formal definition.

Definition 3.1. 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

$$M : S \setminus \{q_0\} \rightarrow \{ \langle X, j \rangle, \langle X, j, k \rangle \mid X \in \{A, B\} \text{ and } j, k \in S \}.$$

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 $\langle X, j \rangle$ or $\langle X, j, k \rangle$, which correspond to the two types of commands described earlier.

Definition 3.2. 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 is the initial state q_1 (or the halting state 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 empty registers, we obtain a sequence of configurations, which will be called the computation of \mathcal{M} .

Definition 3.3. 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 $\bar{\mathcal{M}}^{n+1}(\langle i, a, b \rangle) = \bar{\mathcal{M}}(\bar{\mathcal{M}}^n(\langle i, a, b \rangle))$. Note that $\bar{\mathcal{M}}^n(\langle i, a, b \rangle)$ is not defined if and only if $\bar{\mathcal{M}}^m(\langle i, a, b \rangle)$ is a halting configuration for some $m < n$.

Definition 3.4. 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 $n > 0$.

We are going to show 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 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. To tackle this problem, first we show the equivalence of regular Minsky machines and Minsky machines with more than two registers. We leave the formal definition of the n -register Minsky machine to the reader.

Lemma 3.5. *Minsky machines and Minsky machines with more than two registers are equivalent.*

Proof. It is clear that an n -register Minsky machine can simulate a 2-register Minsky machine; we just use the same program and do not use the remaining registers. To prove the other direction we need a few subroutines for Minsky machines.

Each subroutine definition has three parts: the head, the body and the tail. The head is a single line starting with the keyword DEF followed by the name of the subroutine and a list of formal parameters. The body consists of commands, one in each line. Each command starts with the state in which it must be applied, followed by the command to be executed. In the tail we list each state in which the machine can continue after the completion of the defined subroutine. The “built-in” subroutines are the commands of Minsky machines denoted by $i : \text{inc } X, j$ for $M(i) = \langle X, j \rangle$ and $i : \text{dec } X, j, k$ for $M(i) = \langle X, j, k \rangle$. Clearly, subroutines and composition of subroutines can be compiled into lists of commands in a trivial way.

CLAIM 1. *We can clear a register X (decrement it to zero).*

DEF clr X, r :
 $s_1 : \text{dec } X, r, s_1$
 $r : (\text{next statement, assures that } X = 0)$

CLAIM 2. *If register $A = 0$ then we can swap the values of A and B .*

DEF mov B, A, r : (assumes that $A = 0$)
 $s_1 : \text{dec } B, r, s_2$
 $s_2 : \text{inc } A, s_1$
 $r : (\text{next statement, assures that } B = 0)$

From now on we assume that the value of register B is zero before and after the following computations. We will use B to hold temporary values. Let p be a fixed positive integer.

CLAIM 3. *We can multiply the value of A by p .*

First in a loop we decrement A by one and increment B by p , then we swap the values of A and B .

```

DEF mul  $A, p, r$ : (assumes that  $B = 0$ )
   $s_1$  : dec  $A, s_{p+2}, s_2$ 
   $s_2$  : inc  $B, s_3$ 
  :
   $s_p$  : inc  $B, s_{p+1}$ 
 $s_{p+1}$  : inc  $B, s_1$ 
 $s_{p+2}$  : mov  $B, A, r$ 
   $r$  : (next statement, assures that  $B = 0$ )

```

CLAIM 4. *We can divide the value of A by p and store the integer part of the quotient in A .*

This is clear. First in a loop we decrement A by p and increment B by one, then we swap the values of A and B .

```

DEF div  $A, p, r$ : (assumes that  $B = 0$ )
   $s_1$  : dec  $A, s_{p+2}, s_2$ 
  :
 $s_{p-1}$  : dec  $A, s_{p+2}, s_p$ 
   $s_p$  : dec  $A, s_{p+2}, s_{p+1}$ 
 $s_{p+1}$  : inc  $B, s_1$ 
 $s_{p+2}$  : mov  $B, A, r$ 
   $r$  : (next statement, assures that  $B = 0$ )

```

One can notice that with a slight modification of the previous subroutine we can test the divisibility of A by p . The trick is to record the remainder “in the states”, and then to rebuild the original value. We can do this since p is a fixed integer.

CLAIM 5. *We can test whether the value of A is divisible by p , while keeping the value of A the same.*

```

DEF test-div  $A, p, r_1, r_2$ : (assumes that  $B = 0$ )
   $s_1$  : dec  $A, s_{2p+3}, s_2$ 
   $s_2$  : dec  $A, s_{2p+1}, s_3$ 

```

$$\begin{aligned}
s_2 &: \text{dec } A, s_{2p}, s_4 \\
&\vdots \\
s_{p-1} &: \text{dec } A, s_{p+4}, s_p \\
s_p &: \text{dec } A, s_{p+3}, s_{p+1} \\
s_{p+1} &: \text{inc } B, s_1 \\
s_{p+2} &: \text{inc } A, s_{p+3} \\
s_{p+3} &: \text{inc } A, s_{p+4} \\
&\vdots \\
s_{2p} &: \text{inc } A, s_{2p+1} \\
s_{2p+1} &: \text{inc } A, s_{2p+2} \\
s_{2p+2} &: \text{dec } B, r_2, s_{p+2} \\
s_{2p+3} &: \text{mov } B, A, s_{2p+4} \\
s_{2p+4} &: \text{mul } A, p, r_1 \\
r_1 &: (\text{next statement when } A \equiv 0 \pmod{p}, \text{ assures that } B = 0) \\
r_2 &: (\text{next statement when } A \not\equiv 0 \pmod{p}, \text{ assures that } B = 0)
\end{aligned}$$

Now we are ready to describe the emulation of an n -register Minsky machine \mathcal{N} in a 2-register Minsky machine \mathcal{M} . The machine \mathcal{N} has configurations like $\langle i, a_1, \dots, a_n \rangle$. We encode it as the configuration $\langle i, p_1^{a_1} \dots p_n^{a_n}, 0 \rangle$ of \mathcal{M} where p_1, \dots, p_n are the first n prime numbers. The states of \mathcal{M} will consist of the states of \mathcal{N} together with additional states necessary for subroutines. The program of \mathcal{M} is a list of subroutines, one for each command of \mathcal{N} . For the command $i : \text{inc } X, j$ of \mathcal{N} where X is the x th register let the corresponding subroutine of \mathcal{M} be $i : \text{mul } A, p_x, j$. For the command $i : \text{dec } X, j, k$ of \mathcal{N} let it be

$$\begin{aligned}
i &: \text{test-div } A, p_x, s_1, j \\
s_1 &: \text{div } A, p_x, k.
\end{aligned}$$

Note that we keep the value of register B zero all the time except for temporary calculations in subroutines. One remaining small detail is that our simulation must start from the configuration $\langle q_1, 1, 0 \rangle$ instead of $\langle q_1, 0, 0 \rangle$, hence we must increment the register A by one at the very beginning. Clearly, the states and commands of \mathcal{M} can be algorithmically constructed from those of \mathcal{N} . \square

Now we prove the equivalence of Turing machines and 3-register Minsky machines. There are many equivalent definitions of the Turing machine. Here we will use a one-tape machine, whose tape is infinite in both directions and can store the digits 0 and 1.

Lemma 3.6. *Turing machines and Minsky machines with three registers are equivalent.*

Proof. It is an easy programming exercise to simulate Minsky machines by Turing machines. For example one can have a tape for each register, then the encoding is trivial, and refer to the equivalence of regular Turing machines and Turing machines with more than one tape. The other direction is more interesting, although not more difficult.

Let \mathcal{T} be a Turing machine. A configuration of \mathcal{T} can be specified by a tuple $\langle i, t, p \rangle$ where i is a state, $t : \mathbb{Z} \rightarrow \{0, 1\}$ is a mapping describing the tape and $p \in \mathbb{Z}$ is the current position of the head. Since \mathcal{T} starts on the empty tape, only finitely many 1's can be written on t . This allows us to encode t and p , up to equivalence under the operation of shifting the tape, into two natural numbers:

$$A_{t,p} = \sum_{n=0}^{\infty} t(p+n) * 2^n, \text{ and}$$

$$C_{t,p} = \sum_{n=0}^{\infty} t(p-1-n) * 2^n.$$

We will store these values in registers A and C of a 3-register Minsky machine. Remember that we need register B to hold temporary values; otherwise it must be zero. Now we can test the digit under the head by checking if A is divisible by 2. We can modify the digit under the head by either incrementing or decrementing A by one. We can move the head to the right by reading the digit under the head, dividing A by 2, multiplying C by 2 and incrementing C by one if the digit 1 was under the head at the previous position. Moving the head to the left is analogous. All these computations can be calculated with a 3-register Minsky machine \mathcal{N} (see the proof of the previous lemma), and the states and commands of \mathcal{N} can be algorithmically constructed from those of \mathcal{T} . \square

Corollary 3.7 (Minsky [9]). *Turing machines and Minsky machines are equivalent.*

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 proving the undecidability of various kinds of word problems [6]. Perhaps the

simplicity of the Minsky machine could be employed in other algebraic problems.

We already know that Turing and Minsky machines are equivalent, but a stronger connection exists between them, connecting the class of Turing-computable and Minsky-computable functions.

Definition 3.8. We say that a partial function $f : \mathbb{N} \rightarrow \mathbb{N}$ is *computable by a Minsky machine* if there exists a Minsky machine \mathcal{M} such that for all $a \in \mathbb{N}$

- (1) if $f(a)$ is defined then \mathcal{M} halts on the input $\langle q_1, a, 0 \rangle$, that is $\bar{\mathcal{M}}^n(\langle q_1, a, 0 \rangle) = \langle q_0, a', b' \rangle$ for some $n > 0$, and the final value a' of register A is $f(a)$,
- (2) if $f(a)$ is undefined then \mathcal{M} does not halt on the input $\langle q_1, a, 0 \rangle$.

We assume that the reader knows the corresponding definition for Turing machines and can figure it out for Minsky machines with more than two registers.

Theorem 3.9. *Let $f : \mathbb{N} \rightarrow \mathbb{N}$ be a partial function. Then the following are equivalent:*

- (1) f is computable by a Turing machine.
- (2) f is computable by a Minsky machine with three registers.
- (3) There exists a partial mapping $g : \mathbb{N} \rightarrow \mathbb{N}$ that is computable by a 2-register Minsky machine such that $g(2^a)$ is defined iff $f(a)$ is defined and $g(2^a) = 2^{f(a)}$ for all natural numbers a .

Proof. (1) \Rightarrow (2) Assume that f is computable by a Turing machine \mathcal{T} . We will use the encoding described in the proof of Lemma 3.6. We already know that the commands of \mathcal{T} can be carried out by a 3-register Minsky machine \mathcal{N} provided that the the initial configuration of \mathcal{N} matches that of \mathcal{T} .

Let a be a fixed natural number and assume that we are calculating $f(a)$. The corresponding initial configuration of \mathcal{T} is $\langle q_1, t, 0 \rangle$ where the tape contains the standard encoding of the number a :

$$t(n) = \begin{cases} 1 & \text{if } 0 \leq n < a, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

The corresponding configuration of \mathcal{N} is $\langle q_1, A_{t,0}, 0, C_{t,0} \rangle$ where $A_{t,0} = 2^a - 1$ and $C_{t,0} = 0$. So our first task is to transform the initial configuration $\langle q_1, a, 0, 0 \rangle$ of \mathcal{N} to $\langle q_1, 2^a - 1, 0, 0 \rangle$, then we start the simulation of \mathcal{T} . Clearly, this transformation can be done using the following subroutine.

DEF $\text{exp } A, p, r$: (assumes that $B = C = 0$)
 s_1 : mov A, C, s_2
 s_2 : inc A, s_3
 s_3 : dec C, r, s_4
 s_4 : mul A, p, s_3
 r : (next statement, assures that $B = C = 0$)

Now we are at the point where the simulation is finished and the result is on the “tape”, that is, encoded in the registers. The result must be somehow decoded and stored in register A . To do this we need to know the format of the answer on the tape. One possible format (of the many equivalent ones) is the following. We say that \mathcal{T} has computed b if it stops in a halting configuration $\langle q_0, t, p \rangle$ where

$$t(n) = \begin{cases} 1 & \text{if } p \leq n < p + b, \text{ and} \\ 0 & \text{if } n = p + b. \end{cases}$$

This means in our encoding that $A_{t,p} = 2^{f(a)} - 1 + c * 2^{f(a)+1}$ for some natural number c . But this number is easy to convert to $f(a)$ by the following subroutine (assuming that $B = 0$):

s_1 : clr C, s_2
 s_2 : test-div $A, 2, s_5, s_3$
 s_3 : inc C, s_4
 s_4 : div $A, 2, s_2$
 s_5 : clr A, s_6
 s_6 : mov C, A, q_0 .

(2) \Rightarrow (3) Assume that f is computable by a 3-register Minsky machine \mathcal{N} . Now let \mathcal{M} be the 2-register Minsky machine described in the proof of Lemma 3.5, and g be the partial function computed by \mathcal{M} . Let a be a fixed natural number, and assume further that we want to calculate $f(a)$. The corresponding initial configuration of \mathcal{N} is $\langle q_1, a, 0, 0 \rangle$. This is encoded as $\langle q_1, 2^a 3^0 5^0, 0 \rangle$ in our simulation which is exactly the initial configuration of \mathcal{M} for $g(a)$. So nothing is to be done at the start.

Once the simulation is over, the machine \mathcal{M} will stop in a halting configuration of the form $\langle q_0, 2^{f(a)} 3^b 5^c, 0 \rangle$ for some natural numbers b and c . Our job is now to convert $2^{f(a)} 3^b 5^c$ to $2^{f(a)}$, which can be done with the following subroutine:

s_1 : test-div $A, 3, s_2, s_3$

$s_2 : \text{div } A, 3, s_1$
 $s_3 : \text{test-div } A, 5, s_4, q_0$
 $s_4 : \text{div } A, 5, s_3.$

(3) \Rightarrow (1) Minsky machines can be simulated by Turing machines, and any recursive function can be calculated by Turing machines. Therefore if a Minsky machine \mathcal{M} can calculate g then a Turing machine calculating f can be constructed algorithmically from \mathcal{M} . \square

4. UNDECIDABILITY OF A PARTIAL NU-TERM

The *near-unanimity problem* (or *NU-problem*) is to input a finite algebra and then determine if it has a near-unanimity term. At present, it is unknown if the NU-problem is decidable. However, partial results have been proven and we hope that they might be extended to solve the problem. The following direction was taken in [7].

Definition 4.1. Let \mathbf{A} be a fixed finite algebra, $t(x_1, \dots, x_n)$ 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 $t(y, \dots, y, x_i, y, \dots, y) = y$ for all $1 \leq i \leq n$ and $x_i, y \in S$.

Note that a term t of \mathbf{A} is a NU-term iff it is a partial NU-term on A . Now one can ask the decidability of a partial NU-term on some subset. It was proved in [7] that the existence of a partial NU-term on a fixed two-element subset is undecidable. In the proof R. McKenzie used Minsky machines. I was able to extend his proof to larger subsets, namely to the subset excluding two fixed elements; still proving undecidability. To get the complete version one just has to “paste together the 2 and $n - 2$ element proofs”. The feasibility of such a result, however, seems remote.

In the rest of this section we are going to prove the $n - 2$ element version 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 $A(\mathcal{M}) \setminus \{r, w\}$ iff \mathcal{M} halts. This is clearly enough since the halting problem for Minsky machines is undecidable.

Let S be the set of states of \mathcal{M} with two special states: the initial state $q_1 \in S$ and the halting state $q_0 \in S$. Let the symbols A and B denote the registers of \mathcal{M} . For each $i \in S \setminus \{q_0\}$ there is a unique command which is either of the form

- $i : \text{inc } R, j$ (increase register $R \in \{A, B\}$ by one and go to state $j \in S$), or

- $i : \text{dec } R, j, k$ (if register $R \in \{A, B\}$ contains zero then go to state $j \in S$ otherwise decrease register R by one and go to state $k \in S$).

Now we define the algebra $\mathbf{A}(\mathcal{M})$ in full detail. We advise the reader to skim through this definition and return to it when reading the subsequent proofs.

Definition 4.2. 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

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

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

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 4.3. Let A be a set, and $f : A^n \rightarrow A$. An element $w \in A$ is *absorbing for f* if $f(\bar{a}) = w$ whenever $\bar{a} \in A^n$ and $w \in \{a_1, \dots, a_n\}$.

Fact 4.4. *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. \square

Note that w is not an absorbing element for the operation M , but almost, except in the first variable. Combining this with the previous fact one can see that $\mathbf{A}(\mathcal{M})$ cannot have a partial NU-term on a subset of more than one element 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 4.5. Let $\bar{x} = (x_1, x_2, \dots)$ 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 4.6. 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 $y \in \bar{x}$.

Fact 4.7. *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.

Suppose that $t(\bar{x}) = I(t_1(\bar{x}))$. Because of Fact 4.4 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 4.8. *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 3.3. 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 $i : \text{inc } R, j$, 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 $i : \text{dec } R, j, k$ 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 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 $a_m \leq a_{m'+1}, \dots, a_m$ (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 $i : \text{inc } R, j$ and $R = A$. On the other hand, the command for state i_m is of the form $i : \text{dec } A, j, k$ and $a_m \neq 0$, therefore $a_{m+1} = a_m - 1$. To summarize, for each pair $\langle m', m \rangle$

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

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 thus $t_{m+1}(\bar{p}|_{y_h=e}) = F_{i_m}(\langle i_m, A \rangle, p) = \langle i_{m+1}, A \rangle$. The same 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 $a_h < a_{h+1}, \dots, a_n$. 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 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 $t(\bar{a}) = M(t_n(\bar{a}), z_1, z_2, z_3) = \text{maj}(z_1, z_2, z_3)$. 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 near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$. \square

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 4.9. *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 for i_m is of the form $i : \text{inc } R, j$ then $t_{m+1} = F_{i_m}(t_m, -)$.*
- (2) *If the command for i_m is of the form $i : \text{dec } R, j, k$, 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 $i : \text{dec } R, j, k$, 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 $i : \text{inc } R, j$ 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 $i : \text{inc } R, j$, 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 $i : \text{dec } R, j, k$ 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,

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

Now using the induction hypothesis we get that

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

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 $m \notin S^-$. 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 $i : \text{dec } R, j, k$ 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 near-unanimity term on $A(\mathcal{M}) \setminus \{r, w\}$, or at least as a subterm of a “minimal” near-unanimity term.

Definition 4.10. 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 4.11. *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 Fact 4.4. 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 sub-term. So assume that M does not occur in t_2, t_3 and t_4 . By Fact 4.7, 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 Fact 4.7 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 4.9 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 4.12. *Let \mathcal{M} be a Minsky machine. The algebra $\mathbf{A}(\mathcal{M})$ has a near-unanimity term on the set $A(\mathcal{M}) \setminus \{r, w\}$ iff \mathcal{M} halts.*

Proof. Suppose that t is a 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 4.11, \mathcal{M} halts. The other direction is proved in Lemma 4.8. \square

5. BITS AND PIECES TOWARDS DECIDABILITY

In this section we try to solve the NU-problem for special classes of algebras. We start with Rosenberg's primal algebra characterization theorem (see [13, 11]), which presents a natural framework for this.

Definition 5.1. A finite non-trivial algebra \mathbf{A} is *primal* if every function on A is a term of \mathbf{A} . We call \mathbf{A} *preprimal* if it is not primal, but including any new operation (which is not already a term of \mathbf{A}) yields a primal algebra. The clones of preprimal algebras are called *maximal clones*. They are exactly the coatoms in the lattice of clones on the set A .

Clearly, a primal algebra has a ternary NU-term; and it is decidable if an algebra is primal. If the algebra is not primal, then its clone lies in one of the maximal clones described in Rosenberg's theorem. We solve the NU-problem in three classes of maximal clones (out of six), and present other partial result.

Rosenberg's characterization is in terms of six classes of finitary relations; a non-trivial finite algebra \mathbf{A} is preprimal if and only if there is a relation ϱ in one of the six classes such that the term functions of

\mathbf{A} are exactly the functions preserving the relation ϱ . Now we define these classes, following Quackenbush [11].

Definition 5.2. Let A be a finite set.

A subset $\varrho \subseteq A^2$ is a *partial order* if it is *reflexive* ($\langle a, a \rangle \in \varrho$ for all $a \in A$), *antisymmetric* ($\langle a, b \rangle, \langle b, a \rangle \in \varrho$ imply that $a = b$), and *transitive* ($\langle a, b \rangle, \langle b, c \rangle \in \varrho$ imply that $\langle a, c \rangle \in \varrho$). We say that $b \in A$ is a *zero (unit)* of $\varrho \subseteq A^2$ if $\langle b, a \rangle \in \varrho$ ($\langle a, b \rangle \in \varrho$) for all $a \in A$. Note that a partial order has at most one zero and at most one unit.

Class (1) is the set of all partial orders with a zero and unit.

A subset $\varrho \subseteq A^2$ is a *permutation* if $\varrho = \{ \langle a, \alpha(a) \rangle : a \in A \}$ where $\alpha : A \rightarrow A$ is a permutation on A . We say that the permutation ϱ is *prime* if all cycles of α have the same prime length.

Class (2) is the set of all prime permutations.

A subset $\varrho \subseteq A^2$ is an *equivalence relation* if ϱ is reflexive, *symmetric* ($\langle a, b \rangle \in \varrho$ implies $\langle b, a \rangle \in \varrho$), and transitive. An equivalence relation ϱ is *non-trivial* if $\varrho \neq A^2$ and $\varrho \neq \{ \langle a, a \rangle : a \in A \}$.

Class (3) is the set of all non-trivial equivalence relations.

A subset $\varrho \subseteq A^4$ is *affine* if we can define an abelian group operation, $+$, on A so that $\langle a, b, c, d \rangle \in \varrho$ if and only if $a + b = c + d$. An affine ϱ is *prime* if $\langle A; + \rangle$ is an elementary abelian p -group.

Class (4) is the set of all prime affine relations.

A subset $\varrho \subseteq A^h$ (for $h \geq 1$) is *totally symmetric* if for every permutation α on $\{1, \dots, h\}$, $\langle a_1, \dots, a_h \rangle \in \varrho$ if and only if $\langle a_{\alpha(1)}, \dots, a_{\alpha(h)} \rangle \in \varrho$. Let $A_h \subseteq A^h$ be defined by

$$(*) \quad A_h = \{ \langle a_1, \dots, a_h \rangle : a_i = a_j \text{ for some } i \neq j \}.$$

We say that ϱ is *totally reflexive* if $A_h \subseteq \varrho$. The *center* of ϱ is the set of all $a \in A$ such that for all $a_2, \dots, a_h \in A$, $\langle a, a_2, \dots, a_h \rangle \in \varrho$. We say that ϱ is *central* if it is totally symmetric, totally reflexive and has a center which is a non-empty, proper subset of A .

Class (5) is the set of all central relations.

Let $h = \{0, 1, \dots, h-1\}$. For $1 \leq r \leq m$, let π_r^m be the r th projection of h^m onto h . Define ω_m to be the h -ary relation on h^m such that $\langle a_1, \dots, a_h \rangle \in \omega_m$ if and only if for all $1 \leq r \leq m$, $\langle \pi_r^m(a_1), \dots, \pi_r^m(a_h) \rangle \in h_h$ (where h_h is defined by $(*)$). A subset $\varrho \subseteq A^h$ for $h \geq 3$ is *h -regularly generated* if for some $m \geq 1$ there is a surjection $\varphi : A \rightarrow h^m$ such that $\varrho = \varphi^{-1}(\omega_m)$; i.e., $\langle a_1, \dots, a_h \rangle \in \varrho$ if and only if $\langle \varphi(a_1), \dots, \varphi(a_h) \rangle \in$

ω_m . Clearly, if ϱ is h -regularly generated, then ϱ is totally reflexive and totally symmetric.

Class (6) is the set of all h -regularly generated relations.

Theorem 5.3 (Rosenberg [13]). *A finite non-trivial algebra \mathbf{A} is pre-primal if and only if for some h -ary relation, ϱ , in classes (1) – (6), the set of term functions of \mathbf{A} is just the set of all functions on \mathbf{A} preserving ϱ .*

First we show that the NU-term problem is decidable inside a maximal clone of class (1). We need the following lemma, which grew out of discussions with R. McKenzie.

Lemma 5.4. *For a finite algebra \mathbf{A} and a natural number k , it is decidable whether \mathbf{A} has a near-unanimity term in which at most k variables have repeated occurrences.*

Proof. It is enough to effectively find a number K so that if \mathbf{A} has a NU-term, then it has a NU-term of depth at most K .

Suppose we do have a near-unanimity term t , and its tree has a long branch $t = t_0, t_1, \dots, t_n$. Here $t_i = g_i(t_{i+1}, -, \dots, -)$, where g_i is a basic operation with variables permuted. Let X be the tuple x_1, x_2, \dots, x_k of variables permitted to have repeated occurrences, and Y be the tuple of remaining variables.

We find a long subsequence $\{s_j\}$ of $\{t_i\}$, such that when all variables of Y are replaced by one new variable z , then $s_j(X; z) = s_l(X; z)$ for all j and l . We can also assume that $B(s_j) = B(s_l)$ for all j and l , where $B(s(X; Y))$ is the set of all term operations $b(x, z)$ of \mathbf{A} arising from the term $s(X; Y)$ by choosing some variable among Y , replacing it by z , and then replacing all other variables of Y and X by x . Also, we can assume that $s_j(x, \dots, x) = s_l(x, \dots, x)$.

Now we claim that if we create a new term t' by replacing the explicit occurrence of s_1 in t (i.e., at $t_i = g_i(s_1, -, \dots, -)$, where $s_1 = t_{i+1}$) by s_2 , then this shorter term t' is also a near-unanimity term.

Indeed, in each near-unanimous evaluation in which the minority variable is from X , the terms s_1 and s_2 behave the same. If the minority variable is from Y then it has exactly one occurrence. If this occurrence is inside of s_1 , then we use that fact that $B(s_1) = B(s_2)$. If it is outside then we use that fact that $s_1(x, \dots, x) = s_2(x, \dots, x)$. \square

Corollary 5.5. *Given a finite algebra \mathbf{A} whose clone lies in a maximal clone of class (1). Then it is decidable if \mathbf{A} has a near-unanimity term.*

Proof. We will prove that if \mathbf{A} has a NU-term, then it has an NU-term in which no variable has multiple occurrences. By the previous lemma this is enough.

Assume that $t(x_1, \dots, x_n)$ is a NU-term of \mathbf{A} . Put

$$t'(y_{11}, \dots, y_{1m_1}, y_{21}, \dots, y_{nm_n}),$$

the term obtained from t by replacing all occurrences of each variable x_i by distinct variables y_{ij} . We claim that t' is also a NU-term. Let \leq be a compatible partial order on \mathbf{A} with a zero element $0 \in A$ and a unit element $1 \in A$. Take elements $a, b \in A$, and consider the near-unanimous evaluation $t'(a, \dots, a, b, a, \dots, a)$ where $y_{ij} = b$ for some i and j . Since \leq is compatible with t' ,

$$\begin{aligned} t'(a, \dots, a, b, a, \dots, a) &\leq t'(a, \dots, a, 1, \dots, 1, a, \dots, a) \\ &= t(a, \dots, a, 1, a, \dots, a) = a, \end{aligned}$$

where $y_{ik} = 1$ for all k , and $x_i = 1$. On the other hand, $a \leq t'(a, \dots, a, b, a, \dots, a)$ by a similar argument. Therefore

$$t'(a, \dots, a, b, a, \dots, a) = a$$

for all $a, b \in A$ and i, j . \square

Now we show that no NU-term can exist in the maximal clones of class (4) and (6), so the problem is decidable in these cases. We call an algebra \mathbf{A} *affine* if it has a compatible affine relation.

Proposition 5.6. *No finite affine algebra has a near-unanimity term. In particular, a finite algebra \mathbf{A} whose clone lies in a maximal clone of class (4), has no near-unanimity term.*

Proof. Assume the contrary, that there exists a NU-term $t(x_1, \dots, x_n)$ of \mathbf{A} . Let $0 \in A$ be the zero element of the abelian group $\langle A; + \rangle$. Fix another element $a \neq 0$ of A . For $0 \leq k \leq n$, let \bar{a}^k be the vector $\langle a, \dots, a, 0, \dots, 0 \rangle \in A^n$ with k -many a entries. We show by induction that $t(\bar{a}^k) = 0$, which is a contradiction for $k = n$. The base of the induction, $k = 0$, is true, since t is a NU-term. For the induction step

$$\begin{aligned} t(a, \dots, a, 0, 0, \dots, 0) &= 0, && \text{by the induction hypothesis,} \\ t(0, \dots, 0, a, 0, \dots, 0) &= 0, && \text{by the NU-term } t, \\ t(0, \dots, 0, 0, 0, \dots, 0) &= 0, && \text{by the NU-term } t, \text{ and} \\ t(a, \dots, a, a, 0, \dots, 0) &= b, && \text{for some } b \in A. \end{aligned}$$

On the left hand side all columns are in the relation $x + y = z + u$. Since this relation is preserved by t , $0 + 0 = 0 + b$, that is, $b = 0$. \square

Proposition 5.7. *A finite algebra \mathbf{A} whose clone lies in a maximal clone of class (6), has no near-unanimity term.*

Proof. Let h, m be natural numbers, $\varphi : A \rightarrow h^m$ be a surjection, and $\varrho \subseteq A^h$ be a relation as described in the Definition 5.2 under class (6). Assume that there exists a NU-term $t(x_1, \dots, x_n)$ of \mathbf{A} which preserves ϱ . We want to get a contradiction.

Recall that $h = \{0, 1, \dots, h-1\}$ and $h \geq 3$. Since φ is surjective, there exist $a_0, \dots, a_{h-1} \in A$ such that $\pi_1^m(\varphi(a_i)) = i$ for all $0 \leq i < h$. For $0 \leq k \leq n$ put $\bar{b}^k = \langle a_0, \dots, a_0, a_1, \dots, a_1 \rangle \in A^n$ with k many a_0 entries. We will prove by induction that $\pi_1^m(\varphi(t(\bar{b}^k))) \neq 0$ for all $0 \leq k \leq n$. For $k = 0$ this is true by definition.

For the induction step assume that the claim is true for k . Put $j = \pi_1^m(\varphi(t(\bar{b}^k)))$. By the induction hypothesis, $j \neq 0$. Consider the following tuples of A^n

$$\begin{aligned} \bar{b}^{k+1} &= \langle a_0, \dots, a_0, a_0, a_1, \dots, a_1 \rangle, \\ &\quad \langle a_1, \dots, a_1, a_0, a_1, \dots, a_1 \rangle, \\ &\quad \vdots \\ &\quad \langle a_{j-1}, \dots, a_{j-1}, a_0, a_{j-1}, \dots, a_{j-1} \rangle, \\ \bar{b}^k &= \langle a_0, \dots, a_0, a_1, a_1, \dots, a_1 \rangle, \\ &\quad \langle a_{j+1}, \dots, a_{j+1}, a_0, a_{j+1}, \dots, a_{j+1} \rangle, \\ &\quad \vdots \\ &\quad \langle a_{h-1}, \dots, a_{h-1}, a_0, a_{h-1}, \dots, a_{h-1} \rangle, \end{aligned}$$

where the i th row ($i \neq 0, j$) is the near-unanimous a_i tuple with a_0 at the $k+1$ -th coordinate. Notice that each column has a repeated entry. Indeed, for the $k+1$ -th column it is a_0 , and for all other columns it is either a_0 or a_1 from the rows \bar{b}^{k+1} and \bar{b}^k . This means that each column is in the relation ϱ . Therefore, by applying t ,

$$\langle t(\bar{b}^{k+1}), a_1, \dots, a_{j-1}, t(\bar{b}^k), a_{j+1}, \dots, a_{h-1} \rangle \in \varrho.$$

Denote this tuple by \bar{c} . By the definition of ϱ , $\varphi(\bar{c}) \in \omega_m$. Then by the definition of ω_m , $\pi_1^m(\varphi(\bar{c})) \in h_h$. But we can calculate this tuple,

$$\pi_1^m(\varphi(\bar{c})) = \langle \pi_1^m(\varphi(t(\bar{b}^{k+1}))), 1, \dots, j-1, j, j+1, \dots, h-1 \rangle.$$

By the definition of h_h , this tuple must have a repetition, therefore $\pi_1^m(\varphi(t(\bar{b}^{k+1}))) \neq 0$. This completes the proof of the induction step.

We have shown that $\pi_1^m(\varphi(t(\bar{b}^n))) \neq 0$. On the other hand,

$$\pi_1^m(\varphi(t(\bar{b}^n))) = \pi_1^m(\varphi(t(a_0, \dots, a_0))) = \pi_1^m(\varphi(a_0)) = 0,$$

which is a contradiction. \square

In the rest of this section we focus on the case when the finite algebra in question is idempotent. As the first step we reduce the problem to simple algebras.

Definition 5.8. An algebra \mathbf{A} is idempotent if $f(x, \dots, x) = x$ for each basic operation f . Note that \mathbf{A} cannot have constants, by definition, if $|A| > 1$.

Lemma 5.9. *The existence of a near-unanimity term for idempotent algebras is decidable if and only if it is decidable for simple idempotent algebras.*

In order to prove this result we need the following definition and fact which describe a way to compose NU-terms.

Definition 5.10. Let $s(x_1, \dots, x_n)$ and $t(y_1, \dots, y_m)$ be terms in n and m variables, respectively. Their *star product* $s \star t$ is a term in nm variables defined as

$$(s \star t)(z_{11}, \dots, z_{nm}) = s(t(z_{11}, \dots, z_{1m}), \dots, t(z_{n1}, \dots, z_{nm})).$$

Fact 5.11. *Let \mathbf{A} and \mathbf{B} be similar idempotent algebras. If s and t are near-unanimity terms of \mathbf{A} and \mathbf{B} , respectively, then $s \star t$ is a near-unanimity term of both \mathbf{A} and \mathbf{B} .*

Proof. First we prove the claim for \mathbf{A} . Let $a, b \in A$, and put $c = (s \star t)(a, b, \dots, b)$. We want to show that $c = b$. Notice that this is enough, as we did not assume any ordering of the variables of s and t . By definition, $c = s(t(a, b, \dots, b), t(b, \dots, b), \dots, t(b, \dots, b))$. Since \mathbf{A} is idempotent, $t(b, \dots, b) = b$, and $c = s(t(a, b, \dots, b), b, \dots, b)$. As s is a NU-term, we conclude that $c = b$. The proof for \mathbf{B} is similar. \square

Proof of Lemma 5.9. One direction is trivial. For the other direction assume that the problem is decidable for simple idempotent algebras, and let \mathbf{A} be a finite idempotent algebra, which is not simple. The decision procedure we present is recursive; we assume that for all algebras of cardinality less than of \mathbf{A} we can decide the problem.

Let ϑ be a nontrivial congruence of \mathbf{A} , and B be a congruence block of ϑ . We claim that B is a subuniverse of \mathbf{A} . Indeed, for each basic operation f and elements $b_1, \dots, b_k \in B$, $f(b_1, \dots, b_k) \vartheta f(b_1, \dots, b_1) = b_1$. Note that, by Definition 5.8, f cannot be a constant.

Denote by \mathbf{B} the subalgebra of \mathbf{A} on the set B . If \mathbf{A} has a NU-term, then the same term is a NU-term for \mathbf{B} . Similarly, the same term is a NU-term for \mathbf{A}/ϑ . Therefore a necessary condition for \mathbf{A} to have an

NU-term is that each proper subalgebra and proper homomorphic image of \mathbf{A} have a NU-term. We will show that this condition is sufficient, as well.

Let t_1, \dots, t_n be NU-terms on the nontrivial congruence blocks of ϑ , respectively, and s be a NU-term on \mathbf{A}/ϑ . By Fact 5.11, the term $t = t_1 \star (t_2 \star (\dots (t_{n-1} \star t_n) \dots))$ is a NU-term on each congruence block of ϑ . We claim that $t \star s$ is a NU-term on \mathbf{A} . Take $a, b \in A$. Since s is idempotent on A and a NU-term of \mathbf{A}/ϑ ,

$$(t \star s)(a, \dots, a, b, a, \dots, a) = t(a, \dots, a, b', a, \dots, a) = a$$

for some element $b' = s(a, \dots, a, b, a, \dots, a) \vartheta a$. \square

We call an algebra \mathbf{A} *strictly simple* if it is simple and has no non-trivial subalgebras. By a non-trivial subalgebra we mean a proper subalgebra having at least two elements.

Theorem 5.12 (Á. Szendrei [14, 15]). *Let \mathbf{A} be a finite idempotent strictly simple algebra. Then the clone of \mathbf{A} is one of the following clones.*

- (1) $|A| = 2$ and $\text{Clo } \mathbf{A}$ is the trivial clone [id].

For a vector space \mathbf{V} denote by $\text{End } \mathbf{V}$ the ring of endomorphisms of \mathbf{V} , and by ${}_{(\text{End } \mathbf{V})} \mathbf{V}$ the left module over $\text{End } \mathbf{V}$.

- (2) *A finite dimensional vector space $\mathbf{V} = \langle A; +, K \rangle$ over a finite field K can be defined on A , and $\text{Clo } \mathbf{A}$ is the clone $\text{Clo}_{\text{id}}({}_{(\text{End } \mathbf{V})} \mathbf{V})$ of idempotent operations of ${}_{(\text{End } \mathbf{V})} \mathbf{V}$.*

For a permutation group G on A let $\mathcal{R}_{\text{id}}(G)$ denote the clone of all idempotent operations f on A such that f admits each member of G as an automorphism.

- (3) $\text{Clo } \mathbf{A} = \mathcal{R}_{\text{id}}(G)$ for some permutation group G on A such that every non-identity member of G has at most one fixed point.

Let $0 \in A$ be some fixed element. For $k \geq 2$ put

$$\chi_k^0 = \{ \langle a_1, \dots, a_k \rangle \in A^k : a_i = 0 \text{ for at least one } i, 1 \leq i \leq k \}.$$

Denote by \mathcal{F}_k^0 the clone of all operations on A preserving the relation χ_k^0 . Furthermore, put $\mathcal{F}_\omega^0 = \bigcap_{k=2}^\infty \mathcal{F}_k^0$.

- (4) $\text{Clo } \mathbf{A} = \mathcal{R}_{\text{id}}(G) \cap \mathcal{F}_k^0$ for some k ($2 \leq k \leq \omega$), some element $0 \in A$, and some permutation group G on A such that 0 is the unique fixed point of every non-identity member of G .

For a relation ϱ on A let \mathcal{P}_ϱ denote the clone of operations on A preserving ϱ .

- (5) $|A| = 2$ and $\text{Clo } \mathbf{A} = \mathcal{R}_{\text{id}}(G) \cap \mathcal{P}_\leq$ for some permutation group G on A ; or $|A| = 2$ and $\text{Clo } \mathbf{A} = \mathcal{R}_{\text{id}}(\{\text{id}\}) \cap \mathcal{P}_\leq \cap \mathcal{F}_k^0$ for some k ($2 \leq k \leq \omega$) and some element $0 \in A$.
- (6) $|A| = 2$ and $\text{Clo } \mathbf{A}$ is the clone $[\vee]$ generated by the join operation; or $|A| = 2$ and $\text{Clo } \mathbf{A}$ is the clone $[\wedge]$ generated by the meet operation.

Lemma 5.13. *The near-unanimity problem for idempotent, strictly simple algebras is decidable.*

Proof. Let \mathbf{A} be a idempotent, strictly simple algebra. We will use classification of Theorem 5.12 in the following decision procedure.

Assume that \mathbf{A} has a compatible partial order relation with zero and unit. Clearly, this condition is decidable. Then by Corollary 5.5 the NU-problem is decidable. This handles the cases (1), (5) and (6) of Theorem 5.12.

Recall that the algebra \mathbf{A} is called affine if it has a compatible affine relation. This is also a decidable property of \mathbf{A} . In Proposition 5.6 we have seen that if \mathbf{A} is affine then it has no NU-term. This handles case (2) of Theorem 5.12, because in that case $\text{Clo } \mathbf{A}$ has a compatible affine relation.

If neither of the previous two conditions hold, then by Theorem 5.12 we know that $\text{Clo } \mathbf{A}$ is of type (3) or (4). In the rest of the proof we will show that the NU-problem is decidable even in these two cases.

CLAIM 1. *Assume that $\text{Clo } \mathbf{A} = \mathcal{R}_{\text{id}}(G)$ as described in case (3) of Theorem 5.12. Then \mathbf{A} has a ternary NU-term.*

Consider the function $f : A^3 \rightarrow A$, defined as

$$f(a, b, c) = \begin{cases} \text{maj}(a, b, c) & \text{if the majority exists,} \\ a & \text{otherwise.} \end{cases}$$

Clearly, f is a NU-term and admits all permutations on A .

CLAIM 2. *Assume that $\text{Clo } \mathbf{A} = \mathcal{R}_{\text{id}}(G) \cap \mathcal{F}_k^0$ as described in case (4) of Theorem 5.12, and $k < \omega$. Then \mathbf{A} has a NU-term.*

Consider the function $f : A^{k+1} \rightarrow A$, defined as

$$f(a_1, \dots, a_{k+1}) = \begin{cases} 0 & \text{if } a_i = a_j = 0 \text{ for some } i \neq j, \\ \text{maj}(a_1, \dots, a_{k+1}) & \text{else if the majority exists,} \\ a_1 & \text{otherwise.} \end{cases}$$

Clearly, f is a NU-term. By the description of case (4), the element 0 is a fixed point of every member of G . Therefore $f \in R_{\text{id}}(G)$. To show that $f \in \mathcal{F}_k^0$, take $\bar{a}^1, \dots, \bar{a}^{k+1} \in \chi_k^0$. By the Pigeon Hole Principle, there exist i, i' ($1 \leq i, i' \leq k+1$) and j ($1 \leq j \leq k$) such that $a_j^i = a_j^{i'} = 0$. This shows that $f(a_j^1, \dots, a_j^{k+1}) = 0$, therefore

$$\langle f(a_1^1, \dots, a_1^{k+1}), \dots, f(a_k^1, \dots, a_k^{k+1}) \rangle \in \chi_n^0.$$

CLAIM 3. *If $\text{Clo } \mathbf{A} \subseteq \mathcal{F}_\omega^0$ for some $0 \in A$ then \mathbf{A} has no NU-term.*

Assume the contrary, that $f \in \mathcal{F}_\omega^0$ is an n -ary NU-term. Take an element $a \in A \setminus \{0\}$, and consider the tuples $\bar{a}^i = \langle a, \dots, a, 0, a, \dots, a \rangle \in A^n$ for $1 \leq i \leq n$ where $a_i^i = 0$. Clearly, $\bar{a}^i \in \chi_n^0$, and

$$\langle f(a_1^1, \dots, a_1^n), \dots, f(a_n^1, \dots, a_n^n) \rangle = \langle a, \dots, a \rangle \notin \chi_n^0.$$

This shows that $f \notin \mathcal{F}_n^0$, which is a contradiction.

CLAIM 4. *Fix an element $0 \in A$. Then $\mathcal{F}_k^0 \supseteq \mathcal{F}_{k+1}^0$ for all $k \geq 2$.*

Take a function $f : A^n \rightarrow A$ preserving χ_{k+1}^0 . To show that it preserves χ_k^0 , as well, take $\bar{a}^1, \dots, \bar{a}^n \in \chi_k^0$. Put $\bar{b}^i = \langle \bar{a}^i, a_k^i \rangle = \langle a_1^i, \dots, a_k^i, a_k^i \rangle$ for $1 \leq i \leq n$. Clearly, $\bar{b}^i \in \chi_{k+1}^0$. Since f preserves χ_{k+1}^0 , the tuple

$$\begin{aligned} & \langle f(b_1^1, \dots, b_1^n), \dots, f(b_k^1, \dots, b_k^n), f(b_{k+1}^1, \dots, b_{k+1}^n) \rangle \\ &= \langle f(a_1^1, \dots, a_1^n), \dots, f(a_k^1, \dots, a_k^n), f(a_k^1, \dots, a_k^n) \rangle \end{aligned}$$

is in relation χ_{k+1}^0 . This means that $\langle f(a_1^1, \dots, a_1^n), \dots, f(a_k^1, \dots, a_k^n) \rangle \in \chi_k^0$, which is what we wanted to show.

CLAIM 5. *Let f be an n -ary function on A , and $0 \in A$. If $f \in \mathcal{F}_n^0$ then $f \in \mathcal{F}_k^0$ for all $n \leq k \leq \omega$.*

Fix k such that $n \leq k < \omega$, and take $\bar{a}^1, \dots, \bar{a}^n \in \chi_k^0$. By definition, there exists a ‘‘choice function’’ $\zeta : \{1, \dots, n\} \rightarrow \{1, \dots, k\}$ such that $a_{\zeta(i)}^i = 0$ for all $1 \leq i \leq n$. Put $\bar{b}^i = \langle a_{\zeta(1)}^i, \dots, a_{\zeta(n)}^i \rangle$ for $1 \leq i \leq n$. Since $b_i^i = 0$, $\bar{b}^i \in \chi_n^0$. By our hypothesis,

$$\langle f(b_1^1, \dots, b_1^n), \dots, f(b_n^1, \dots, b_n^n) \rangle \in \chi_n^0.$$

This means that $f(b_j^1, \dots, b_j^n) = 0$ for some $1 \leq j \leq n$, and therefore $f(a_{\zeta(j)}^1, \dots, a_{\zeta(j)}^n) = 0$. Hence $f \in \mathcal{F}_k^0$. Finally, since $\mathcal{F}_2^0 \supseteq \dots \supseteq \mathcal{F}_\omega^0$ and $f \in \mathcal{F}_k^0$ for all $n \leq k < \omega$, $f \in \mathcal{F}_\omega^0$.

CLAIM 6. *Assume that Clo \mathbf{A} is of type (3) or (4) as described in Theorem 5.12. Then it is decidable if \mathbf{A} has a NU-term.*

First we check if \mathbf{A} has a ternary NU-term. If it does, then we are done. Assume that \mathbf{A} has no ternary NU-term. Then by Claim 1, Clo \mathbf{A} is of type (4). Moreover, by Claims 2 and 3, \mathbf{A} has no NU-term if and only if Clo $\mathbf{A} \subseteq \mathcal{F}_\omega^0$ for some $0 \in A$.

Now we show that, given $0 \in A$, it is decidable if Clo $\mathbf{A} \subseteq \mathcal{F}_\omega^0$. Take a basic n -ary operation f of \mathbf{A} . Clearly, we can decide if $f \in \mathcal{F}_n^0$. If $f \in \mathcal{F}_n^0$ then $f \in \mathcal{F}_\omega^0$, otherwise $f \notin \mathcal{F}_\omega^0$. So, Clo $\mathbf{A} \subseteq \mathcal{F}_\omega^0$ if and only if $f \in \mathcal{F}_n^0$ for all basic operations $f(x_1, \dots, x_n)$. \square

REFERENCES

- [1] S. Burris and H.P. Sankappanavar, *A course in universal algebra*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1981.
- [2] 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.
- [3] B. A. Davey, L. Heindorf and R. McKenzie, *Near unanimity: an obstacle to general duality theory* Algebra Universalis, **33** (1995), 428–439.
- [4] 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.
- [5] J. Ježek and M. Maróti, *Membership problems for finite entropic groupoids*. (to appear).
- [6] O. G. Kharlampovich and M. V. Sapir, *Algorithmic problems in varieties*. Int. Journal of Algebra and Comp., **5**, Augustus & October 1995.
- [7] R. McKenzie, *Is the presence of a nu-term a decidable property of a finite algebra?* October 15, 1997 (manuscript).
- [8] R. McKenzie, G. McNulty and W. Taylor, *Algebras, Lattices, Varieties, Volume I*. Wadsworth & Brooks/Cole, Monterey, CA, 1987.
- [9] 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.
- [10] M. L. Minsky, *Computations: finite and infinite machines*. Prentice-Hall, Englewood Cliffs, N.J., 1967.
- [11] R. W. Quackenbush, *A new proof of Rosenberg’s primal algebra characterization theorem*. Finite algebra and multiple-valued logic (Szeged, 1979), Colloq. Math. Soc. János Bolyai, **28** (1981), 603–634.
- [12] M. O. Rabin and D. Scott, *Finite automata and their decision problems*, IBM Journal of Res. and Devel., **3**(2) (1969), 114–125.

- [13] I. Rosenberg, *Über die funktionale Vollständigkeit in den mehrwertigen Logiken*. Rozprawy Československe Akad. Věd., Ser. Math. Nat. Sci., **80** (1970), 3–93.
- [14] Á. Szendrei, *Idempotent algebras with restrictions on subalgebras*. Acta Sci. Math. (Szeged) **51** (1987), 251–268.
- [15] Á. Szendrei, *Term minimal algebras*. Algebra Universalis, **32** (1994), 439–477.

DEPARTMENT OF MATHEMATICS, VANDERBILT UNIVERSITY, 1326 STEVENSON
CENTER, NASHVILLE, TN 37240

E-mail address: mmaroti@math.vanderbilt.edu