Basic Research in Computer Science

On the Two-Variable Fragment of the Equational Theory of the Max-Sum Algebra of the Natural Numbers

Luca Aceto
Zoltán Ésik
Anna Ingólfsdóttir

BRICS Report Series **RS-99-22**

ISSN 0909-0878 **August 1999**

**See back inner page for a list of recent BRICS Report Series publications.
Copies may be obtained by contacting:**

**BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk**

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/99/22/`

On the Two-Variable Fragment of the Equational Theory of the Max-Sum Algebra of the Natural Numbers

Luca Aceto* Zoltán Ésik† Anna Ingólfsdóttir*‡

Abstract

This paper shows that the collection of identities in two variables which hold in the algebra **N** of the natural numbers with constant zero, and binary operations of sum and maximum does not have a finite equational axiomatization. This gives an alternative proof of the non-existence of a finite basis for **N**—a result previously obtained by the authors. As an application of the main theorem, it is shown that the language of Basic Process Algebra (over a singleton set of actions), with or without the empty process, has no finite ω-complete equational axiomatization modulo trace equivalence.

AMS Subject Classification (1991): 08A70, 08B05, 03C05, 68Q70.
ACM Computing Classification System (1998): F.4.1.
Keywords and Phrases: Equational logic, varieties, complete axiomatizations, process algebra, trace equivalence.

1 Introduction

Since Birkhoff's original developments, equational logic has been one of the classic topics of study within universal algebra. (See, e.g., [7, 8, 9] for surveys of results in this area of research.) In particular, the research literature is, among other things, rich in results, both of a positive and negative nature, on the existence of finite bases for theories (i.e. finite sets of axioms for them).

*BRICS (Basic Research in Computer Science), Centre of the Danish National Research Foundation, Department of Computer Science, Aalborg University, Fr. Bajersvej 7E, 9220 Aalborg Ø, Denmark. Email: {luca,annai}@cs.auc.dk. Fax: +45 9815 9889.

†Department of Computer Science, A. József University, Árpád tér 2, 6720 Szeged, Hungary. Partially supported by grant no. T30511 from the National Foundation of Hungary for Scientific Research. Email: esik@inf.u-szeged.hu. Fax: +36-62-420292.

‡Supported by a research grant from the Danish Research Council.

In this paper, we contribute to the study of equational theories that are not finitely based by continuing our analysis of the equational theory of the algebra $\mathbf{N}$ of the natural numbers with constant zero, and binary operations of summation and maximum (written $\vee$ in infix form). Our investigations of this equational theory started in the companion paper [1]. In *op. cit.* we showed that the equational theory of $\mathbf{N}$ is not finitely based. Moreover, we proved that, for all $n \geq 0$, the collection of all the equations in at most n variables that hold in $\mathbf{N}$ does not form an equational basis.

The equational theory of $\mathbf{N}$ is surprisingly rich in non-trivial families of identities. For example, the following infinite schemas of equations also hold in $\mathbf{N}$:

$$\begin{aligned} e_n: &\quad nx_1 \vee \ldots \vee nx_n \vee (x_1 + \ldots + x_n) = nx_1 \vee \ldots \vee nx_n \\ e'_n: &\quad nx \vee ny = n(x \vee y) \ , \end{aligned}$$

where $n \in \mathbb{N}$, and nx denotes the n-fold sum of x with itself.

Let $\mathrm{Eq}_2(\mathbf{N})$ denote the collection of equations that hold in $\mathbf{N}$ containing occurrences of two distinct variables. A natural question suggested by the family of equations e'_n above is the following:

> Is there a finite set E of equations that hold in $\mathbf{N}$ such that $E \vdash \mathrm{Eq}_2(\mathbf{N})$?

This paper is devoted to proving that no finite axiomatization exists for $\mathrm{Eq}_2(\mathbf{N})$. Apart from its intrinsic mathematical interest, this result offers yet another view of the non-existence of a finite axiomatization for the variety generated by $\mathbf{N}$ proven in [1].

The proof of our main technical result is model-theoretic in nature, and follows standard lines. The details are, however, rather challenging. More precisely, for every prime number p, we construct an algebra $\mathbf{A}_p$ in which all the equations that hold in $\mathbf{N}$ and whose "measure of complexity" is strictly smaller than p hold, but neither e_p nor e'_p hold in $\mathbf{A}_p$. As a consequence of this result, we obtain that not only the equational theory of $\mathbf{N}$ is not finitely based, but not even the collection of equations in two variables included in it is.

We also provide an application of our main result to process algebra [2]. More precisely, we show that trace equivalence has no finite ω-complete equational axiomatization for the language of Basic Process Algebra [3] over a singleton alphabet, with or without the empty process [10].

Although the proof of our main theorem uses results from [1], we have striven to make the paper self contained. The interested reader is referred to *op. cit.* and the textbooks [4, 5] for further background information.

2 The Max-Sum Algebra

Let $\mathbf{N} = (\mathbb{N}, \vee, +, 0)$ denote the algebra of the natural numbers equipped with the usual sum operation $+$, constant 0 and the operation $\vee$ for the maximum of two numbers, i.e.,

$$x \vee y \;\; = \;\; \max\{x, y\} \;\; .$$

We study the equational theory of the algebra $\mathbf{N}$—that is, the collection $\mathrm{Eq}(\mathbf{N})$ of equations that hold in $\mathbf{N}$. The reader will have no trouble in checking that the following axioms, that express expected properties of the operations of maximum and sum, hold in $\mathbf{N}$:

$\vee 1$	$x \vee y = y \vee x$	$+1$	$x + y = y + x$
$\vee 2$	$(x \vee y) \vee z = x \vee (y \vee z)$	$+2$	$(x + y) + z = x + (y + z)$
$\vee 3$	$x \vee 0 = x$	$+3$	$x + 0 = x$
		$+\vee$	$(x \vee y) + z = (x + z) \vee (y + z)$

This set of equations will be denoted by Ax_1. Note that the equation $(x + y) \vee x = x + y$ is derivable from $+3$ and $+\vee$, and, using such an equation, it is a simple matter to derive the idempotency law for $\vee$, i.e.,

$$\vee 4 \quad x \vee x = x \;\; .$$

We denote by Ax_0 the set consisting of the equations $\vee 1$, $\vee 2$, $\vee 4$, $+1$–$+3$ and $+\vee$. Moreover, we let $\mathbf{V}_0$ stand for the class of all models of Ax_0, and $\mathbf{V}_1$ for the class of all models of the equations Ax_1. Thus, both $\mathbf{V}_0$ and $\mathbf{V}_1$ are varieties and, by the above discussion, $\mathbf{V}_1$ is a subvariety of $\mathbf{V}_0$, i.e., $\mathbf{V}_1 \subseteq \mathbf{V}_0$.

Since the reduct $(A, \vee)$ of any algebra $A = (A, +, \vee, 0)$ in $\mathbf{V}_0$ is a semilattice, we can define a partial order $\leq$ on the set A by $a \leq b$ if and only if $a \vee b = b$, for all $a, b \in A$. This partial order is called the induced partial order. When A is in the variety $\mathbf{V}_1$, the constant 0 is the least element of A with respect to $\leq$. Moreover, for any $A \in \mathbf{V}_0$, the $\vee$ and $+$ operations are monotonic with respect to the induced partial order.

The axiom system Ax_1 completely axiomatizes the collection of equations in at most one variable which hold in the algebra $\mathbf{N}$. However, the interplay between the operations of maximum and sum generates some nontrivial collections of equations in two or more variables. For example, the following infinite schemas of equations, which will play an important role in the technical developments of this paper, also hold in $\mathbf{N}$:

$$\begin{array}{ll} e_n: & nx_1 \vee \ldots \vee nx_n \vee (x_1 + \ldots + x_n) = nx_1 \vee \ldots \vee nx_n \\ e'_n: & nx \vee ny = n(x \vee y) \;\; , \end{array}$$

where $n \in \mathbb{N}$, nx denotes the n-fold sum of x with itself, and we take advantage of the associativity and commutativity of the operations. By convention, nx stands for 0 when $n = 0$. It is not too difficult to see that, for any n, the equation e_n is derivable from Ax_1 and e'_n.

Let $\mathrm{Eq}_2(\mathbf{N})$ denote the collection of equations that hold in $\mathbf{N}$ containing occurrences of two distinct variables. A natural question suggested by the family of equations e'_n above is the following:

Is there a finite subset E of $\mathrm{Eq}(\mathbf{N})$ such that $E \vdash \mathrm{Eq}_2(\mathbf{N})$?

The remainder of this paper is devoted to proving that no finite axiomatization exists for $\mathrm{Eq}_2(\mathbf{N})$. Apart from its intrinsic mathematical interest, this result offers yet another view of the non-existence of a finite axiomatization for the variety generated by $\mathbf{N}$ proven in [1].

3 Explicit Description of the Free Algebras

In this section we give a brief review of some results on the equational theory of the algebra $\mathbf{N}$ that we obtained in [1]. (The proofs of the results stated in this section may be found *ibidem*.) We start by offering an explicit description of the free algebras in the variety $\mathbf{V}$ generated by $\mathbf{N}$. Since $\mathbf{N}$ satisfies the equations in Ax_1, we have that $\mathbf{V}$ is a subvariety of $\mathbf{V}_1$, i.e., $\mathbf{V} \subseteq \mathbf{V}_1$.

For the sake of clarity, and for future reference, we shall describe the finitely generated free algebras in $\mathbf{V}$. We recall that any infinitely generated free algebra is a directed union of the finitely generated free ones. (The interested reader is referred to [4] for this and other basic results in universal algebra that we shall use in what follows.)

Let $n \geq 0$ denote a fixed integer. The set $\mathbb{N}^n$ is the collection of all n-dimensional vectors over $\mathbb{N}$. Let $P_f(\mathbb{N}^n)$ denote the collection of all finite nonempty subsets of $\mathbb{N}^n$, and define the operations in the following way: for all $U, V \in P_f(\mathbb{N}^n)$,

$$\begin{aligned} U \vee V &:= U \cup V \\ U + V &:= \{\overline{u} + \overline{v} : \overline{u} \in U,\ \overline{v} \in V\} \\ 0 &:= \{\overline{0}\}\ , \end{aligned}$$

where $\overline{0}$ stands for the vector whose components are all 0. For each $i \in [n] = \{1, \ldots, n\}$, let $\overline{u}_i$ denote the ith unit vector in $\mathbb{N}^n$, i.e., the vector whose only non-zero component is a 1 in the ith position.

Proposition 3.1 *The algebra $P_f(\mathbb{N}^n)$ is freely generated in $\mathbf{V}_0$ by the n singleton sets $\{\overline{u}_i\}$, $i \in [n]$, containing the unit vectors.*

Note that the induced partial order on $P_f(\mathbb{N}^n)$ is given by set inclusion.

It is easy to see that any term t in the variables $x_1, \ldots, x_n$ ($n \geq 0$) can be rewritten, using the equations in Ax_0, to the maximum of linear combinations of the variables $x_1, \ldots, x_n$, i.e., there are $m \geq 1$, and $c_i^j \in \mathbb{N}$ for $j \in [n]$ and $i \in [m]$ such that the equation

$$t = \bigvee_{i \in [m]} \Big(\sum_{j \in [n]} c_i^j x_j \Big)$$

holds in $\mathbf{V}_0$. (The empty sum is defined to be 0.) We refer to such terms as *normal forms*. Thus we may assume that any equation which holds in a given subvariety of $\mathbf{V}_0$ is in normal form, i.e., of the form $t_1 = t_2$ where t_1 and t_2 are normal forms. Furthermore, an equation

$$t_1 \vee \ldots \vee t_m \quad = \quad t'_1 \vee \ldots \vee t'_{m'}$$

holds in a subvariety of $\mathbf{V}_0$ if and only if, for all $i \in [m]$ and $j \in [m']$,

$$t_i \leq t'_1 \vee \ldots \vee t'_{m'} \quad \text{and} \quad t'_j \leq t_1 \vee \ldots \vee t_m$$

hold in the subvariety. We refer to an inequation of the form

$$t \quad \leq \quad t_1 \vee \ldots \vee t_m$$

where $t, t_1, \ldots, t_m$ are linear combinations of variables, as *simple inequations*.

A simple inequation $t \leq t_1 \vee \ldots \vee t_m$ that holds in $\mathbf{N}$ is *irredundant* if, for every $j \in [m]$,

$$\mathbf{N} \not\models t \leq t_1 \vee \ldots \vee t_{j-1} \vee t_{j+1} \vee \ldots \vee t_m \ .$$

By the discussion above, we may assume, without loss of generality, that every set of inequations that hold in $\mathbf{N}$ consists of simple, irredundant inequations only.

In order to give an explicit description of the finitely generated free algebras in $\mathbf{V}_1$, we need to take into account the effect of equation $\vee 3$. Let $\leq$ denote the pointwise partial order on $\mathbb{N}^n$. As usual, we say that a set $U \subseteq \mathbb{N}^n$ is an order ideal, if $\overline{u} \leq \overline{v}$ and $\overline{v} \in U$ jointly imply that $\overline{u} \in U$, for all vectors $\overline{u}, \overline{v} \in \mathbb{N}^n$. Each set $U \subseteq \mathbb{N}^n$ is contained in a least ideal $(U]_n$, the ideal generated by U. The relation that identifies two sets $U, V \in P_f(\mathbb{N}^n)$

if $(U]_n = (V]_n$ is a congruence relation on $P_f(\mathbb{N}^n)$, and the quotient with respect to this congruence is easily seen to be isomorphic to the subalgebra $I_f(\mathbb{N}^n)$ of $P_f(\mathbb{N}^n)$ generated by the finite non-empty ideals.

For each $i \in [n]$, let $(\overline{u}_i]_n$ denote the principal ideal generated by the unit vector $\overline{u}_i$, i.e., the ideal $(\{\overline{u}_i\}]_n$.

Proposition 3.2 *$I_f(\mathbb{N}^n)$ is freely generated in $\mathbf{V}_1$ by the n principal ideals $(\overline{u}_i]_n$.*

Again, the induced partial order on $I_f(\mathbb{N}^n)$ is the partial order determined by set inclusion.

We note that, if $n \geq 2$, then the equation e_n fails in $I_f(\mathbb{N}^n)$, and *a fortiori* in $\mathbf{V}_1$. Since for $n \geq 2$ the equation e_n holds in $\mathbf{N}$ but fails in $\mathbf{V}_1$, in order to obtain a concrete description of the free algebras in $\mathbf{V}$ we need to make further identifications of the ideals in $I_f(\mathbb{N}^n)$. Technically, we shall start with $P_f(\mathbb{N}^n)$.

Let $\overline{v}_1, \ldots, \overline{v}_k$ $(k \geq 1)$ be vectors in $\mathbb{N}^n$, and suppose that λ_i $(i \in [k])$ are non-negative real numbers with $\sum_{i\in[k]} \lambda_i = 1$. We call the vector of real numbers $\sum_{i\in[k]} \lambda_i \overline{v}_i$ a convex linear combination of the $\overline{v}_i$.

Definition 3.3 *We call a set $U \subseteq P_f(\mathbb{N}^n)$ a* convex ideal *if for any convex linear combination $\sum_{i\in[k]} \lambda_i \overline{v}_i$, with $\overline{v}_i \in U$ for all $i \in [k]$, and for any $\overline{v} \in \mathbb{N}^n$, if*

$$\overline{v} \;\leq\; \sum_{i=1}^{k} \lambda_i \overline{v}_i$$

in the pointwise order, then $\overline{v} \in U$.

Note that any convex ideal is an ideal. Moreover, the intersection of any number of convex ideals is a convex ideal. Thus, any subset U of $\mathbb{N}^n$ is contained in a least convex ideal, $[U]_n$. When U is finite, so is $[U]_n$. We let $\overline{c} \leq U$ mean that the simple inequation

$$\overline{c} \cdot \overline{x} \;\leq\; \bigvee_{\overline{d}\in U} \overline{d} \cdot \overline{x}$$

holds in $\mathbf{N}$. Then we have the following useful characterization of the simple inequations that hold in $\mathbf{N}$.

Lemma 3.4 *Suppose that $U \in P_f(\mathbb{N}^n)$ and $\overline{c} \in \mathbb{N}^n$. Then $\overline{c} \in [U]_n$ iff $\overline{c} \leq U$.*

Let $\sim$ denote the congruence relation on $P_f(\mathbb{N}^n)$ that identifies two sets of vectors iff they generate the same least convex ideal. It is immediate to see that the quotient algebra $P_f(\mathbb{N}^n)/\sim$ is isomorphic to the following algebra $CI_f(\mathbb{N}^n) = (CI_f(\mathbb{N}^n), \vee, +, 0)$ of all non-empty finite convex ideals in $P_f(\mathbb{N}^n)$. For any two $I, J \in CI_f(\mathbb{N}^n)$,

$$\begin{aligned} I \vee J &= [I \cup J]_n \\ I + J &= [\{\overline{u} + \overline{v} : \overline{u} \in I,\ \overline{v} \in J\}]_n \\ 0 &= \{\overline{0}\}\ . \end{aligned}$$

Indeed, an isomorphism $P_f(\mathbb{N}^n)/\sim \to CI_f(\mathbb{N}^n)$ is given by the mapping $U/\sim \mapsto [U]_n$.

Recall that, for each $i \in [n]$, $\overline{u}_i$ denotes the ith unit vector in $\mathbb{N}^n$. For each $i \in [n]$, the set $[\overline{u}_i]_n = (\overline{u}_i]_n = \{\overline{u}_i, \overline{0}\}$ is the least convex ideal containing $\overline{u}_i$.

Theorem 3.5 *$CI_f(\mathbb{N}^n)$ is freely generated by the n convex ideals $[\overline{u}_i]_n$ in the variety $\mathbf{V}$.*

As a corollary of Theorem 3.5, we obtain the following alternative characterization of simple equations which hold in the algebra $\mathbf{N}$.

Corollary 3.6 *Let $\overline{c}, \overline{d}_j$ $(j \in [m])$ be vectors in $\mathbb{N}^n$. Then $\overline{c} \leq \{\overline{d}_1, \ldots, \overline{d}_m\}$ iff there are $\lambda_1, \ldots, \lambda_m \geq 0$ such that $\lambda_1 + \ldots + \lambda_m = 1$ and $\overline{c} \leq \lambda_1\overline{d}_1 + \ldots + \lambda_m\overline{d}_m$ with respect to the pointwise ordering. Moreover, if $\overline{c} \leq \{\overline{d}_1, \ldots, \overline{d}_m\}$ is irredundant, then $\lambda_1, \ldots, \lambda_m > 0$.*

The above result offers a geometric characterization of the simple inequations in $\mathrm{Eq}(\mathbf{N})$, viz. an inequation $\overline{c} \cdot \overline{x} \leq \overline{d}_1 \cdot \overline{x} \vee \ldots \vee \overline{d}_m \cdot \overline{x}$ (where $\overline{x} = (x_1, \ldots, x_n)$ is a vector of variables) holds in $\mathbf{N}$ iff the vector $\overline{c}$ lies in the ideal generated by the convex hull of the vectors $\overline{d}_1, \ldots, \overline{d}_m$.

4 The Two Variable Fragment of the Equational Theory is not Finitely Based

We now proceed to apply the results that we have recalled in the previous section to the study of the two variable fragment of the equational theory of the algebra $\mathbf{N}$. The main aim of this paper is to prove the following result to the effect that the collection of equations $\mathrm{Eq}_2(\mathbf{N})$ cannot be deduced using any finite number of equations in $\mathrm{Eq}(\mathbf{N})$.

Theorem 4.1 *There is no finite set E of equations in* $\mathrm{Eq}(\mathbf{N})$ *such that* $E \vdash \mathrm{Eq}_2(\mathbf{N})$.

To prove Thm. 4.1 we shall define a sequence of algebras $\mathbf{A}_n$ $(n \geq 1)$ in $\mathbf{V}_1$ such that following holds:

> For any finite set E of equations which hold in $\mathbf{N}$, there is an n such that
> $$\mathbf{A}_n \models E \text{ but } \mathbf{A}_n \not\models e'_n \ .$$

Recalling that, for any n, the equation e_n is derivable from e'_n and Ax_1, it is sufficient to prove the statement above with e'_n replaced by e_n. Furthermore, in light of our previous analysis, the result we are aiming at in this section, viz. Thm. 4.1, may now be reformulated as follows.

Proposition 4.2 *Let E be a finite set of simple, irredundant equations such that $\mathbf{N} \models E$. Then there is an $n \in \mathbb{N}$ and an algebra $\mathbf{A}_n \in \mathbf{V}_1$ such that $\mathbf{A}_n \models E$ but $\mathbf{A}_n \not\models e_n$.*

The non-existence of a finite axiomatization of the two variable fragment of the equational theory of $\mathbf{N}$ follows easily from Prop. 4.2 and the preceding discussion. In fact, let E be any finite subset of $\mathrm{Eq}(\mathbf{N})$. Without loss of generality, we may assume that E includes Ax_1, and that $E \setminus Ax_1$ consists of simple, irredundant equations. Then, by Prop. 4.2, there is an algebra $\mathbf{A}_n \in \mathbf{V}_1$ such that $\mathbf{A}_n \models E$ but $\mathbf{A}_n \not\models e_n$. Since e_n is derivable from Ax_1 and e'_n, it follows that $\mathbf{A}_n \not\models e'_n$. We may therefore conclude that $E \nvdash \mathrm{Eq}_2(\mathbf{N})$, which was to be shown.

4.1 The Algebras $\mathbf{A}_n$

We let the weight of a vector $\overline{u} \in \mathbb{N}^n$, notation $|\overline{u}|$, be defined as the sum of its components. (Equivalently $|\overline{u}| = \overline{u} \cdot \overline{\delta}_n$ where $\overline{\delta}_n = (1, \ldots, 1)$.) To define the algebra $\mathbf{A}_n$, where $n \geq 1$ is a fixed integer, let us call a set $I \subseteq \mathbb{N}^n$ an n-convex ideal if it is an ideal and for any convex linear combination $\overline{v} = \lambda_1\overline{v}_1 + \ldots + \lambda_m\overline{v}_m$ and vector $\overline{u} \in \mathbb{N}^n$ of weight $|\overline{u}| < n$, if $\overline{v}_1, \ldots, \overline{v}_m \in I$ and $\overline{u} \leq \overline{v}$, where $\leq$ is the pointwise order, then $\overline{u} \in I$. It is clear that any convex ideal in $\mathbb{N}^n$ is n-convex. Any set $U \subseteq \mathbb{N}^n$ is contained in a least n-convex ideal, denoted $[\![U]\!]_n$. (The subscript n will often be omitted when it is clear from the context.) Call a vector $\overline{v} = (v_1, \ldots, v_n) \in \mathbb{N}^n$ n-ok, written $ok_n(\overline{v})$, if $|\overline{v}| \leq n$ and

$$|\overline{v}| = n \quad \Rightarrow \quad \exists i \in [n].\ v_i = n \ .$$

A set of vectors is n-ok if all of its elements are. Note that if U is a finite non-empty set consisting of n-ok vectors, then $[\![U]\!]$ is also finite and contains only n-ok vectors.

The algebra $\mathbf{A}_n$ consists of all non-empty (finite) n-convex ideals of n-ok vectors, as well as the element $\top$. The operations are defined as follows: for all $I, J \in \mathbf{A}_n$, $I, J \neq \top$, let

$$K \;=\; \{\overline{u} + \overline{v} : \overline{u} \in I,\ \overline{v} \in J\}\ .$$

Then,

$$\begin{array}{rcl} I + J & := & \begin{cases} [\![K]\!] & \text{if } K \text{ contains only } n\text{−ok vectors} \\ \top & \text{otherwise.} \end{cases} \\ I \vee J & := & [\![I \cup J]\!] \\ 0 & := & \{\overline{0}\} = [\![\overline{0}]\!]\ . \end{array}$$

Moreover, we define $\top + I = \top \vee I = \top$, and symmetrically, for all $I \in \mathbf{A}_n$.

Proposition 4.3 *For each $n \geq 1$, $\mathbf{A}_n \in \mathbf{V}_1$.*

Proof: For every $I \in I_f(\mathbb{N}^n)$, let $h(I) = [\![I]\!]$, if I contains only n-ok vectors, otherwise let $h(I) = \top$. This defines a surjective homomorphism $h : I_f(\mathbb{N}^n) \to \mathbf{A}_n$. Thus $\mathbf{A}_n$ is a quotient algebra of $I_f(\mathbb{N}^n)$, and the result follows from Proposition 3.2. □

We shall now show that, for every $n \geq 2$, the algebra $\mathbf{A}_n$ is not in $\mathbf{V}$. In particular, if $n \geq 2$, then the equations e_n and e'_n do not hold in $\mathbf{A}_n$.

Lemma 4.4 *If $n \geq 2$ then $\mathbf{A}_n \not\models e_n$ and $\mathbf{A}_n \not\models e'_n$.*

Proof: Assume that $n \geq 2$. Let $J_i = [\![\{\overline{u}_i\}]\!]_n$ $(i \in [n])$, where $\overline{u}_i$ denotes the ith unit vector in $\mathbb{N}^n$. Then, since $n \geq 2$,

$$J_1 + \ldots + J_n = \top\ .$$

Furthermore, for $i \in [n]$,

$$nJ_i = [\![\{(\overbrace{0, \ldots, 0, n}^{i \text{ places}}, 0 \ldots, 0)\}]\!]_n$$

and therefore

$$nJ_1 \vee \ldots \vee nJ_n = [\![\{(n,0,\ldots,0,0),\ldots,(0,0,\ldots,0,n)\}]\!]_n \neq \top \ .$$

It follows that e_n fails in $\mathbf{A}_n$. Since e_n is derivable from Ax_1 and e'_n, Prop. 4.3 yields that e'_n also fails in $\mathbf{A}_n$. $\square$

Note that the induced partial order on $\mathbf{A}_n$ has $\top$ as its top element, and coincides with the inclusion order over the elements in $\mathbf{A}_n$ that are different from $\top$. For $K \in P_f(\mathbb{N}^n)$, by slightly abusing notation, we let $[\![K]\!]$ stand for $[\![K]\!]$ in the original sense if K contains only n-ok vectors and $\top$ otherwise. With this extension of the definition of $[\![\_]\!]$ we have that $[\![K]\!]+[\![L]\!] = [\![K+L]\!]$ for all $K, L \in P_f(\mathbb{N}^n)$. Using this notation, denoting the induced preorder on $\mathbf{A}_n$ by $\sqsubseteq_n$, we obtain the following alternative characterization of $\mathbf{A}_n$ as a quotient algebra of $P_f(\mathbb{N}^n)$, which will be used in the technical developments to follow.

Let $L, M \in P_f(\mathbb{N}^n)$. We write

$$L \leq M \ \Leftrightarrow \ \forall \overline{u} \in L.\ \overline{u} \leq M \ .$$

Now,

$$\mathbf{A}_n = \{[\![L]\!] \ : \ L \in P_f(\mathbb{N}^n)\}$$

where

$$[\![L]\!] \sqsubseteq_n [\![M]\!] \text{ iff } L \preceq_n M$$

and

$$L \preceq_n M \ \Leftrightarrow \ [ok_n(M) \ \Rightarrow \ (ok_n(L) \wedge L \leq M)] \ .$$

We use $\approx_n$ to denote the kernel of $\preceq_n$. Similarly Lemma 3.4 provides us with the following characterization of $CI_f(\mathbb{N}^n)$:

$$CI_f(\mathbb{N}^n) = \{[L] \ : \ L \in P_f(\mathbb{N}^n)\}$$

where, by Lemma 3.4,

$$[L] \subseteq [M] \text{ iff } L \leq M \ .$$

We extend the definition of the weight function to elements of $P_f(\mathbb{N}^n)$ thus:

$$|L| \ = \ \max\{|\overline{u}| \ : \ \overline{u} \in L\} \ .$$

Now we have the following easy, but useful result.

Lemma 4.5 *If $L \leq M$ then $|L| \leq |M|$.*

We recall that $\sim$ denotes the kernel of the preorder $\leq$.

Lemma 4.6

1. *For all m and all $L \in P_f(\mathbb{N}^n)$, $mL \sim \{m\overline{u} \ : \ \overline{u} \in L\}$.*
2. *If p is prime and $m < p$ then $m[\![K]\!]_p = [\![\{m\overline{u} | \overline{u} \in K\}]\!]_p$.*

Proof: We prove the two statements in turn.

1. Let $K = \{m\overline{u} \ : \ \overline{u} \in L\}$. We shall prove that $mL \sim K$. Obviously $K \subseteq mL$, which in turn implies that $K \leq mL$. To prove that $mL \leq K$ holds, assume $\overline{v} = \overline{v}_1 + \ldots + \overline{v}_m \in mL$, where $\overline{v}_1, \ldots, \overline{v}_m \in L$, and that $\overline{r} \in \mathbb{N}^n$. Let $i_{\overline{r}}$ be the index of the largest amongst the numbers $\overline{v}_1 \cdot \overline{r}, \ldots, \overline{v}_m \cdot \overline{r}$. Then we have

$$\overline{v} \cdot \overline{r} = \overline{v}_1 \cdot \overline{r} + \ldots + \overline{v}_m \cdot \overline{r} \leq (m\overline{v}_{i_{\overline{r}}}) \cdot \overline{r}$$

   where $m\overline{v}_{i_{\overline{r}}} \in K$. This proves the first statement in the lemma.

2. The case $m = 1$ is trivial so we may assume that $m > 1$. To prove the statement in this case, let $L = \{m\overline{v} | \overline{v} \in K\}$. Suppose that p is a prime number and $2 \leq m < p$. In light of our previous remarks, it is sufficient to show that $mK \approx_p L$. First we recall that

$$mK = \underbrace{K + \ldots + K}_{m\,times} = \{\overline{v}_1 + \ldots + \overline{v}_m \ : \ \overline{v}_i \in K, i \in [m]\} \ .$$

   In particular this implies that $L \subseteq mK$ and therefore that $L \preceq_p mK$. To prove that $mK \preceq_p L$ holds we proceed as follows. We know from Lemma 4.6(1) that $mK \leq L$. It is therefore sufficient to prove that $\neg ok_p(mK)$ implies $\neg ok_p(L)$. To this end, assume that there is a $\overline{v}_1 + \ldots + \overline{v}_m \in mK$ which is not p-ok and let $\overline{v}_i$ be the vector of maximum weight amongst $\overline{v}_1, \ldots \overline{v}_m$. Then

$$|m\overline{v}_i| = m|\overline{v}_i| \geq |\overline{v}_1| + \ldots |\overline{v}_m| \geq p \ .$$

   That $m|\overline{v}_i| = p$ is impossible, as p is prime and $m \geq 2$. Therefore $|m\overline{v}_i| = m|\overline{v}_i| > p$ which means that $m\overline{v}_i$ is not p-ok. As $m\overline{v}_i \in L$, this proves that L is not p-ok, which was to be shown. $\square$

Note that Lemma 4.6(2) does not hold in general if p is not prime. For instance, if $p = 4$, $m = 2$ and $K = \{(2,0),(0,2)\}$, then

$$\top = m[\![K]\!]_p \neq [\![\{(4,0),(0,4)\}]\!]_p \ .$$

In what follows we let the simple inequation

$$a^1x_1 + \ldots + a^mx_m \leq \begin{array}{c} c_1^1x_1 + \ldots + c_1^mx_m \\ \vee \\ \vdots \\ \vee \\ c_k^1x_1 + \ldots + c_k^mx_m \end{array}$$

be represented by $(a^i)^{i\leq m} \leq (c^i_j)^{i\leq m}_{j\leq k}$ (or sometimes simply by $\overline{a} \leq \overline{\overline{C}}$ if the meaning is clear from the context), where $(a^i)^{i\leq m}$ denotes the the row vector $(a^1, \cdots, a^m)$ and $(c^i_j)^{i\leq m}_{j\leq k}$ the $k \times m$ matrix $\left[\begin{array}{ccc} c_1^1 \ldots c_1^m \\ \vdots \quad\quad \vdots \\ c_k^1 \ldots c_k^m \end{array}\right]$. We also let an instantiation of the variables $x_1, \ldots, x_m$ by the singleton sets $\{\overline{\eta}_1\}, \ldots, \{\overline{\eta}_m\}$ (or equivalence classes generated by these sets) be represented as

$$\overline{\overline{\eta}} = \left[\begin{array}{c} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{array}\right] = \left[\begin{array}{ccc} \eta_1^1 \ldots \eta_1^n \\ \vdots \quad\quad \vdots \\ \eta_m^1 \ldots \eta_m^n \end{array}\right] \ ,$$

i.e. the matrix with row vectors $\overline{\eta}_1, \ldots, \overline{\eta}_m$. We note that, by commutativity of $\vee$, the simple inequation $\overline{a} \leq \overline{\overline{B}}$, where $\overline{\overline{B}}$ is any matrix obtained by permuting the rows of $\overline{\overline{C}}$, represents exactly the same simple inequation as $\overline{a} \leq \overline{\overline{C}}$, viz. the inequation $\overline{a} \leq U$, where $U = \{\overline{c}_1, \ldots, \overline{c}_k\}$ and the $\overline{c}_i$ ($i \in [k]$) are the row vectors of $\overline{\overline{C}}$. Similarly any permutation of the column vectors of $\overline{\overline{C}}$ combined with a corresponding permutation of the entries of $\overline{a}$ yields a simple inequation that holds in $\mathbf{N}$ iff $\overline{a} \leq \overline{\overline{C}}$ does. (Any instantiation matrix should be similarly permuted as well.) The weight of $\overline{\overline{C}}$, notation $|\overline{\overline{C}}|$, is defined as the sum of its entries.

Notation: In the remainder of this paper, $\overline{a}$ and $\overline{\overline{C}}$ will denote a row vector in $\mathbb{N}^{1\times m}$ and a matrix in $\mathbb{N}^{k\times m}$, respectively.

Now we have the following corollaries of Lemma 4.6.

Corollary 4.7 *Let p be a prime number. If $p > \max\{|\overline{a}|, |\overline{\overline{C}}|\}$ then the following holds. For all $L_1, \ldots, L_m \in P_f(\mathbb{N}^p)$,*

$$\begin{array}{ll} \forall(\overline{v}_1, \ldots, \overline{v}_m) \in L_1 \times \ldots \times L_m. & \\ & \{c_1^1\overline{v}_1 + \ldots + c_1^m\overline{v}_m, \\ \{a^1\overline{v}_1 + \ldots + a^m\overline{v}_m\} \preceq_p & \quad \vdots \\ & c_k^1\overline{v}_1 + \ldots + c_k^m\overline{v}_m\} \end{array}$$

implies

$$\begin{array}{ll} & c_1^1 L_1 + \ldots + c_1^m L_m \\ & \quad \cup \\ a^1 L_1 + \ldots + a^m L_m \preceq_p & \quad \vdots \\ & \quad \cup \\ & c_k^1 L_1 + \ldots + c_k^m L_m \ . \end{array}$$

Proof: Follows directly from Lemma 4.6(2). □

The next result will play a key role in the proof of Thm. 4.9 to follow.

Corollary 4.8 *Assume that $\overline{a} \leq \overline{\overline{C}}$ holds and is irredundant. Then $\mathbf{A}_p \not\models \overline{a} \leq \overline{\overline{C}}$, where p is a prime number with $|\overline{a}| < p$ and $|\overline{\overline{C}}| < p$, iff there is an instantiation matrix $\overline{\overline{\eta}} \in \mathbb{N}^{m \times p}$, such that*

1. *$\overline{a} \cdot \overline{\overline{\eta}}$ has weight p and at least two non-zero coefficients, and*
2. *$\overline{c}_j \cdot \overline{\overline{\eta}}$ has weight p and exactly one non-zero coefficient for $j \in [k]$.*

Proof: We prove the two implications separately.

- 'Only If Implication': We establish that each condition is met in turn.
  1. Assume that $\overline{a} \leq \overline{\overline{C}}$ holds in $\mathbf{N}$, and therefore in $CI_f(\mathbb{N}^p)$ (Theorem 3.5), but not in $\mathbf{A}_p$. Then, as $|\overline{a}| < p$ and $|\overline{\overline{C}}| < p$, for some $L_1, \ldots, L_m \in P_f(\mathbb{N}^p)$,

$$\overline{a} \cdot \begin{bmatrix} L_1 \\ \vdots \\ L_m \end{bmatrix} \leq \overline{\overline{C}} \cdot \begin{bmatrix} L_1 \\ \vdots \\ L_m \end{bmatrix}$$

but

$$\overline{a} \cdot \begin{bmatrix} L_1 \\ \vdots \\ L_m \end{bmatrix} \not\preceq_p \overline{\overline{C}} \cdot \begin{bmatrix} L_1 \\ \vdots \\ L_m \end{bmatrix}$$

where $\overline{\overline{C}} \cdot \begin{bmatrix} L_1 \\ \vdots \\ L_m \end{bmatrix}$ has the obvious meaning in $P_f(\mathbb{N}^p)$. By Cor. 4.7 there is a $(\overline{\eta}_1, \ldots, \overline{\eta}_m) \in L_1 \times \ldots \times L_m$ such that

$$\left\{ \overline{a} \cdot \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix} \right\} \leq \left\{ \begin{array}{l} \overline{c}_1 \cdot \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix}, \\ \vdots \\ \overline{c}_k \cdot \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix} \end{array} \right\}$$

but

$$\left\{ \overline{a} \cdot \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix} \right\} \not\preceq_p \left\{ \begin{array}{l} \overline{c}_1 \cdot \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix}, \\ \vdots \\ \overline{c}_k \cdot \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix} \end{array} \right\} .$$

Let $\overline{\overline{\eta}} = \begin{bmatrix} \overline{\eta}_1 \\ \vdots \\ \overline{\eta}_m \end{bmatrix}$. First we note that if $\overline{a} \cdot \overline{\overline{\eta}}$ is p-ok then, by definition of $\preceq_p$,

$$\{\overline{a} \cdot \overline{\overline{\eta}}\} \preceq_p \{\overline{c}_j \cdot \overline{\overline{\eta}} \ : \ j \in [k]\}$$

which contradicts our assumption. Thus we may conclude that $\overline{a} \cdot \overline{\overline{\eta}}$ is not p-ok. Next we note that if $|\overline{a} \cdot \overline{\overline{\eta}}| > p$ then, by Lemma 4.5, $|\{\overline{c}_j \cdot \overline{\overline{\eta}} \ : \ j \in [k]\}| > p$ and therefore

$$\{\overline{a} \cdot \overline{\overline{\eta}}\} \preceq_p \{\overline{c}_j \cdot \overline{\overline{\eta}} \ : \ j \in [k]\} \ ,$$

again a contradiction to our assumption. Thus we are left with the case where $|\overline{a} \cdot \overline{\overline{\eta}}| = p$ and $\overline{a} \cdot \overline{\overline{\eta}}$ has at least two non-zero coefficients.

2. By Cor. 3.6, since $\overline{a} \leq \overline{\overline{C}}$ holds in $CI_f(\mathbb{N}^p)$, we may infer that

$$\overline{a} \leq \lambda_1 \overline{c}_1 + \ldots + \lambda_k \overline{c}_k \ ,$$

where, as $\overline{a} \leq \overline{\overline{C}}$ is irredundant, $\lambda_1, \ldots, \lambda_k > 0$ and $\lambda_1 + \ldots + \lambda_m = 1$. By associativity of matrix multiplication we have that

$$\overline{a} \cdot \overline{\overline{\eta}} \leq \lambda_1(\overline{c}_1 \cdot \overline{\overline{\eta}}) + \ldots + \lambda_k(\overline{c}_k \cdot \overline{\overline{\eta}})$$

which in turn implies

$$\begin{array}{l} p = |\overline{a} \cdot \overline{\overline{\eta}}| \leq \\ |\lambda_1(\overline{c}_1 \cdot \overline{\overline{\eta}})| + \ldots + |\lambda_k(\overline{c}_k \cdot \overline{\overline{\eta}})| = \\ \lambda_1|\overline{c}_1 \cdot \overline{\overline{\eta}}| + \ldots + \lambda_k|\overline{c}_k \cdot \overline{\overline{\eta}}| \ . \end{array}$$

As by the analysis at point 1 of the proof $|\overline{c}_j \cdot \overline{\overline{\eta}}| \leq p$, for $j \in [k]$, this implies that $|\overline{c}_j \cdot \overline{\overline{\eta}}| = p$ for $j \in [k]$. Thus, as every $\overline{c}_j \cdot \overline{\overline{\eta}}$ is p-ok, it must have exactly one non-zero coefficient for every $j \in [k]$.

- 'If Implication": Take an instantiation matrix $\overline{\overline{\eta}} \in \mathbb{N}^{m \times p}$ that satisfies the proviso of this statement. Let $x_1 = J_1 = [\![\{\overline{\eta_1}\}]\!]_n, \ldots, x_m = J_m = [\![\{\overline{\eta_m}\}]\!]_n$. Then it is easy to check that

$$a^1 J_1 + \ldots + a^m J_m = \top$$

but that

$$c_j^1 J_1 + \ldots + c_j^m J_m \neq \top \text{ for } j \in [k]$$

and therefore

$$\bigvee_{j \in [k]} c_j^1 J_1 + \ldots + c_j^m J_m \neq \top \ .$$

Thus the inequation $\overline{a} \leq \overline{\overline{C}}$ does not hold in $\mathbf{A}_p$. □

Note that if $\overline{\overline{\eta}}$ is an instantiation matrix satisfying points 1–2 in the above statement, then so does any matrix obtained by permuting the columns of $\overline{\overline{\eta}}$.

Using the previous result, we are now in a position to show the following theorem, which is the key to the proof of Propn. 4.2 and of Thm. 4.1.

Theorem 4.9 *If $\overline{a} \leq \overline{\overline{C}}$ is irredundant and holds in* $\mathbf{N}$*, then* $\mathbf{A}_p \not\models \overline{a} \leq \overline{\overline{C}}$ *for at most one prime number* $p > \max\{|\overline{a}|, |\overline{\overline{C}}|\}$.

Proof: Assume that $\overline{a} = (a^1, \ldots, a^m) \in \mathbb{N}^{1\times m}$ and $\overline{\overline{C}} = (c^i_j)^{i\leq m}_{j\leq k} \in \mathbb{N}^{k\times m}$ (i.e. the inequation $\overline{a} \leq \overline{\overline{C}}$ contains at most m variables) and that $\mathbf{N} \models \overline{a} \leq \overline{\overline{C}}$. Assume furthermore that the statement of the theorem does not hold and that m is the smallest number of variables for which it fails; we shall show that this leads to a contradiction. So suppose that $\mathbf{N} \models \overline{a} \leq \overline{\overline{C}}$ but that $\mathbf{A}_p \not\models \overline{a} \leq \overline{\overline{C}}$ and $\mathbf{A}_q \not\models \overline{a} \leq \overline{\overline{C}}$, where p and q are prime and $\max\{|\overline{a}|, |\overline{\overline{C}}|\} < p < q$. First we note that we may assume that $a^i > 0$ for $i \in [m]$, or else we could immediately reduce the number of variables in the equation under consideration. Since $\overline{a} \leq \overline{\overline{C}}$ holds in $\mathbf{N}$, this implies that each column of $\overline{\overline{C}}$ is non-zero. We now continue with the proof as follows: First we use the assumption $\mathbf{A}_p \not\models \overline{a} \leq \overline{\overline{C}}$ and Corollary 4.8 to analyze the structure of $\overline{a}$ and $\overline{\overline{C}}$. Then we argue that the result of this analysis contradicts our second assumption, viz. the failure of the inequation $\overline{a} \leq \overline{\overline{C}}$ in $\mathbf{A}_q$.

As $\mathbf{A}_p \not\models \overline{a} \leq \overline{\overline{C}}$, by Corollary 4.8 there is an instantiation matrix $\overline{\overline{\eta}} = (\eta^r_i)^{r\leq p}_{i\leq m} \in \mathbb{N}^{m,p}$, such that

- $\overline{a} \cdot \overline{\overline{\eta}}$ has weight p and at least two non-zero coefficients and
- $\overline{c}_j \cdot \overline{\overline{\eta}}$ has weight p and exactly one non-zero coefficient, for every $j \in [k]$.

By minimality of m, we may furthermore assume that each row of $\overline{\overline{\eta}}$ contains a non-zero entry.

By rearranging the order of the rows of $\overline{\overline{C}}$ (i.e. the order of the terms that occur on the right-hand side of the simple equation) and of the columns of $\overline{\overline{\eta}}$, we may assume that there is a $0 < k_0 \leq k$ such that

1. $\overline{c}_j \cdot \overline{\overline{\eta}} = (p, 0, \ldots, 0)$ for $j \in [k_0]$ and
2. $\overline{c}_j \cdot \overline{\overline{\eta}} = (0, l^2_j, \ldots, l^m_j)$ for $k_0 < j \leq k$, where exactly one of the l^i_j is non-zero for $2 \leq i \leq m$.

By rearranging the columns of $\overline{\overline{C}}$ and correspondingly the order of the entries of $\overline{a}$ and $\overline{\overline{\eta}}$ (i.e. the order of the variables that occur in the equation), we may assume that there is an $m_0 \in [m]$ such that if $j \leq k_0$ then $c^i_j = 0$ for

all $i > m_0$. Therefore we may suppose that $\overline{\overline{C}}$ looks as follows:

$$\overline{\overline{C}} \;=\; \left[\begin{array}{c|c} \begin{matrix} c_1^1 \dots c_1^{m_0} \\ \vdots \quad\quad \vdots \\ c_{k_0}^1 \dots c_{k_0}^{m_0} \end{matrix} & \overline{\overline{O}}_1 \\ \hline \overline{\overline{O}}_2 & ? \end{array}\right] \tag{1}$$

where $\overline{\overline{O}}_1$ and $\overline{\overline{O}}_2$ are (possibly empty) 0-matrices (i.e., matrices whose entries are all 0) and ? just means that this part of the matrix is unknown. Recall that, as previously observed, some of the c_j^i ($i \in [m_0], j \in [k_0]$) may be 0, but no column in the upper left corner of $\overline{\overline{C}}$ is identically 0.

We claim that $k_0 < k$ and $m_0 < m$, and therefore that $\overline{\overline{O}}_1$ and $\overline{\overline{O}}_2$ are both non-trivial. To see that this claim holds, note that, by 1.-2. above, $\overline{\overline{\eta}}$ has the form

$$\overline{\overline{\eta}} = \left[\begin{array}{c|c} \begin{matrix} \eta_1^1 \\ \vdots \\ \eta_{m_0}^1 \end{matrix} & \overline{\overline{O}} \\ \hline ? & ? \end{array}\right]$$

where $\overline{\overline{O}}$ is a 0-matrix. This follows because if some of the columns of the matrix to the right of the first column (the one that starts with $\begin{bmatrix} \eta_1^1 \\ \vdots \\ \eta_{m_0}^1 \end{bmatrix}$) has a non-zero entry above the horizontal solid line, at least one of the $\overline{c}_j \cdot \overline{\overline{\eta}}$, $j \in [k_0]$, is going to have more than one non-zero entry. Since the rows of $\overline{\overline{\eta}}$ are non-zero, we have that $\eta_j^1 \neq 0$ for every $j \in [m_0]$. Using this fact it is not difficult to see that, as claimed, the cases where either $k_0 = k$ or $m_0 = m$ cannot occur. Indeed, if $m_0 = m$ then $\overline{\overline{\eta}}$ has only one non-zero column and consequently $\overline{a} \cdot \overline{\overline{\eta}}$ cannot have two non-zero coefficients. Moreover, if $k_0 = k$ and $m_0 < m$ then the right hand side of the inequation does not contain the variables x_i, with $m_0 < i \leq m$, whereas, by assumption, the left hand side does—a contradiction to the fact that the inequation $\overline{a} \leq \overline{\overline{C}}$ holds in $\mathbf{N}$. We may therefore assume that $k_0 < k$ and $m_0 < m$.

Now we recall from Cor. 3.6 that, since $\overline{a} \leq \overline{\overline{C}}$ is an irredundant inequation that holds in $\mathbf{N}$, there is a sequence of real numbers λ_i, $i \in [k]$, such that

$$\overline{a} \leq (\lambda_1 \overline{c}_1 + \ldots + \lambda_{k_0} \overline{c}_{k_0}) + (\lambda_{k_0+1} \overline{c}_{k_0+1} + \ldots + \lambda_k \overline{c}_k) \ ,$$

where $\lambda_i > 0$ for $i \in [k]$ and $\lambda_1 + \ldots + \lambda_k \leq 1$. Next let

$$\begin{array}{rcll} \overline{a}_1 & = & (a^1, \ldots, a^{m_0}, 0, \ldots, 0) & \text{and} \\ \overline{a}_2 & = & (0, \ldots, 0, a^{m_0+1}, \ldots, a^m) \ . & \end{array}$$

Then $\overline{a} = \overline{a}_1 + \overline{a}_2$ and

$$\begin{array}{l} \overline{a} \cdot \overline{\overline{\eta}} = \overline{a}_1 \cdot \overline{\overline{\eta}} + \overline{a}_2 \cdot \overline{\overline{\eta}} \leq \\ (\lambda_1 \overline{c}_1 \cdot \overline{\overline{\eta}} + \ldots + \lambda_{k_0} \overline{c}_{k_0} \cdot \overline{\overline{\eta}}) + (\lambda_{k_0+1} \overline{c}_{k_0+1} \cdot \overline{\overline{\eta}} + \ldots + \lambda_k \overline{c}_k \cdot \overline{\overline{\eta}}) \ . \end{array}$$

By multiplying with $\overline{\delta}_p = (1, ..., 1) \in \mathbb{N}^p$, and therefore getting the weight, we have:

$$\begin{array}{l} p = (\overline{a} \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p = (\overline{a}_1 \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p + (\overline{a}_2 \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p \leq \\ \lambda_1 (\overline{c}_1 \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p + \ldots + \lambda_k (\overline{c}_k \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p = \\ \lambda_1 |\overline{c}_1 \cdot \overline{\overline{\eta}}| + \ldots + \lambda_k |\overline{c}_k \cdot \overline{\overline{\eta}}| = \\ \lambda_1 p + \ldots + \lambda_k p \leq p \ . \end{array}$$

Thus these last two inequalities must be equalities, and

$$p = (\overline{a} \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p = (\lambda_1 + \ldots + \lambda_k) p \ .$$

Furthermore, because of the special structure of the coordinates of the vectors $\overline{a}_1, \overline{a}_2, \overline{c}_1, ..., \overline{c}_k$, we must have that

$$\overline{a}_1 \leq \lambda_1 \overline{c}_1 + ... + \lambda_{k_0} \overline{c}_{k_0}$$

and

$$\overline{a}_2 \leq \lambda_{k_0+1} \overline{c}_{k_0+1} + ... + \lambda_k \overline{c}_k$$

and therefore, using similar reasoning as above,

$$(\overline{a}_1 \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p \leq (\lambda_1 + \ldots + \lambda_{k_0}) p$$

and

$$(\overline{a}_2 \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p \leq (\lambda_{k_0+1} + \ldots + \lambda_k) p \ .$$

From above we know that both the left hand sides and the right hand sides of these inequalities sum up to p; therefore these two inequalities must be equalities. Thus we have proven that

$$n_p = (\overline{a}_1 \cdot \overline{\overline{\eta}}) \cdot \overline{\delta}_p = \lambda p \ ,$$

where $\lambda = \lambda_1 + \ldots + \lambda_{k_0}$ and $n_p \in \mathbb{N}$. Note that, as $k_0 < k$ and $\lambda_i > 0$ ($i \in [k]$), it holds that $\lambda < 1$. Hence we have that $n_p < p$.

In a similar way, using the form of $\overline{\overline{C}}$ in (1) and the fact that $q > p$, $\mathbf{N} \models \overline{a} \leq \overline{\overline{C}}$ and $\mathbf{A}_q \not\models \overline{a} \leq \overline{\overline{C}}$, we may conclude that there is a $\overline{\overline{\gamma}} \in \mathbb{N}^{m \times q}$ such that

$$n_q = (\overline{a}_1 \cdot \overline{\overline{\gamma}}) \cdot \overline{\delta}_q = \lambda q \ .$$

This in turn implies that $\frac{n_p}{p} = \frac{n_q}{q}$ or equivalently $n_p \cdot q = n_q \cdot p$, contradicting our assumption that $n_p < p$, $n_q < q$ and p and q are different primes. We may therefore conclude that no such minimal number of variables m exists and consequently that the statement of the theorem holds. This completes the proof of the theorem. □

Prop. 4.2 follows immediately from the above result, completing the proof of the non-existence of a finite equational axiomatization for the two-variable fragment of the equational theory of the algebra **N**.

Remark 4.1 Using our results, it is easy to show that the reduct $(\mathbb{N}, \vee, +)$ of **N** is also not finitely based, and that the two variable fragment of its equational theory has no finite equational axiomatization.

Remark 4.2 As a further corollary of Thm 4.1, we obtain that the equational theory of the algebra $(\mathbb{N}, \vee, +, 0, 1)$ is also not finitely based. To see this, note that whenever an equation holds in $(\mathbb{N}, \vee, +, 0, 1)$ and one side contains an occurrence of the symbol 1, then so does the other side. Let E be an axiom system for $(\mathbb{N}, \vee, +, 0, 1)$, and let E_0 denote the subset of E consisting of all the equations not containing occurrences of the constant 1. In light of the above observation, E_0 is an axiom system for the reduct **N** of $(\mathbb{N}, \vee, +, 0, 1)$. Thus the existence of a finite basis for the algebra $(\mathbb{N}, \vee, +, 0, 1)$ would contradict Thm. 4.1.

In similar fashion, it is easy to prove that the two variable fragment of the equational theory of the algebra $(\mathbb{N}, \vee, +, 0, 1)$ has no finite equational axiomatization.

5 An Application to Process Algebra

We now offer an application of the results we have developed in this paper to the field of process algebra. (The interested reader is referred to [2] for a textbook presentation of this field of research.)

We begin by presenting the language of Basic Process Algebra (BPA) [3] (over a singleton set of actions) with the empty process [10] and its operational semantics.

The Syntax We assume a countably infinite set Var of process variables, with typical element x. We use a to denote the only action symbol that may be used in process terms.

The language $\mathbb{T}(\mathrm{BPA}_\varepsilon)$ of Basic Process Algebra with the empty process and action a is given by the following BNF grammar:

$$P ::= \varepsilon \mid a \mid x \mid P + P \mid P \cdot P \ .$$

The set of closed terms, i.e., terms that do not contain occurrences of process variables, is denoted by $\mathrm{T}(\mathrm{BPA}_\varepsilon)$. We shall use P, Q to range over $\mathbb{T}(\mathrm{BPA}_\varepsilon)$. A closed substitution is a mapping from process variables to closed terms in the language $\mathbb{T}(\mathrm{BPA}_\varepsilon)$. For every term P and closed substitution σ, the closed term obtained by replacing every occurrence of a variable x in P with the closed term $\sigma(x)$ will be written $P\sigma$.

Operational Semantics and Trace Equivalence The operational semantics for the language of closed terms $\mathrm{T}(\mathrm{BPA}_\varepsilon)$ is defined by the transition rules in Table 1 from [2]. These rules define transitions $P \stackrel{a}{\to} P'$ to express that term P can evolve into term P' by the execution of action a, and transitions $P\surd$ to express that term P can terminate successfully.

$$\frac{}{a \stackrel{a}{\to} \epsilon} \qquad \frac{}{\epsilon\surd}$$

$$\frac{P\surd}{P + Q\surd} \qquad \frac{P \stackrel{a}{\to} P'}{P + Q \stackrel{a}{\to} P'} \qquad \frac{Q\surd}{P + Q\surd} \qquad \frac{Q \stackrel{a}{\to} Q'}{P + Q \stackrel{a}{\to} Q'}$$

$$\frac{P\surd \quad Q\surd}{P \cdot Q\surd} \qquad \frac{P\surd \quad Q \stackrel{a}{\to} Q'}{P \cdot Q \stackrel{a}{\to} Q'} \qquad \frac{P \stackrel{a}{\to} P'}{P \cdot Q \stackrel{a}{\to} P' \cdot Q}$$

Table 1: Transition Rules for $\mathrm{T}(\mathrm{BPA}_\varepsilon)$.

For $n \geq 0$, we write $P \stackrel{a^n}{\to} P'$ iff there exist terms $P_0, \ldots, P_n$ such that $P = P_0 \stackrel{a}{\to} P_1 \stackrel{a}{\to} \cdots P_{n-1} \stackrel{a}{\to} P_n = P'$. In that case, we say that a^n is

a *trace* of term P [6]. For terms $P, Q \in \mathrm{T}(\mathrm{BPA}_\varepsilon)$, we write $P \simeq Q$ iff P and Q afford the same traces. Note that the collection of traces of a term is non-empty and prefix-closed. Moreover, since a is the only action, it is completely determined by the longest sequence it contains. This is the key to the proof of the following result.

Proposition 5.1 *The relation $\simeq$ is preserved by the operators in the signature of $\mathbb{T}(\mathrm{BPA}_\varepsilon)$.*

In light of Propn. 5.1, we can construct the quotient algebra

$$\mathbf{T} = (\mathrm{T}(\mathrm{BPA}_\varepsilon)/\simeq, \cdot, +, \varepsilon, a)$$

of closed $\mathbb{T}(\mathrm{BPA}_\varepsilon)$-terms modulo $\simeq$. That is, for $P, Q \in \mathbb{T}(\mathrm{BPA}_\varepsilon)$,

$$\mathbf{T} \models P = Q \quad \text{iff} \quad (\text{for all closed substitutions } \sigma : P\sigma \simeq Q\sigma) \ .$$

The equational theory of $\mathbf{T}$ will be written $\mathrm{Eq}(\mathbf{T})$. Our order of business in the remainder of this paper will be to show the following result to the effect that there is no finite equational axiomatization of the algebra $\mathbf{T}$, i.e., of trace equivalence over the language $\mathrm{T}(\mathrm{BPA}_\varepsilon)$.

Theorem 5.1 *The algebra $\mathbf{T}$ is not finitely based. In particular, no finite subset of $\mathrm{Eq}(\mathbf{T})$ proves all the equations in two variables that hold in $\mathbf{T}$.*

To prove the above theorem, note that $\mathbf{T}$ is isomorphic to the algebra $(\mathbb{N}, \vee, +, 0, 1)$, if we interpret summation over $\mathbb{N}$ as $\cdot$, $\vee$ as $+$, and the constants 0 and 1 as ε and a, respectively. (An isomorphism would simply map the congruence class of term P to the length of the longest trace P affords.) Therefore the claim follows immediately from Remark 4.2.

Remark 5.1 As a corollary of the observations in Remark 4.1, similar results can be proven *mutatis mutandis* for trace equivalence over the language of Basic Process Algebra (over a singleton set of actions) without the empty process.

References

[1] L. Aceto, Z. Ésik, and A. Ingólfsdóttir, *The Max-Sum Algebra of the Natural Numbers has no Finite Equational Basis*, Technical Report 99-1-001, Department of Computer Science, The University of Aizu, 1999.

[2] J. Baeten and W. Weijland, *Process Algebra*, Cambridge Tracts in Theoretical Computer Science 18, Cambridge University Press, 1990.

[3] J. Bergstra and J. Klop, *Fixed point semantics in process algebras*, Report IW 206, Mathematisch Centrum, Amsterdam, 1982.

[4] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, New York, 1981.

[5] G. Grätzer, *Universal Algebra*, Springer-Verlag, second ed., 1979.

[6] C. Hoare, *Communicating Sequential Processes*, Prentice-Hall International, Englewood Cliffs, 1985.

[7] G. McNulty, *A field guide to equational logic*, J. Symbolic Computation, 14 (1992), pp. 371–397.

[8] W. Taylor, *Equational logic*, in Contributions to universal algebra, North-Holland Publishing Co., Amsterdam, 1977, pp. 465–501. Proceedings of the Colloquium held in Szeged, 1975. Colloquia Mathematica Societatis János Bolyai, vol. 17.

[9] ——, *Equational logic*, in [5], Appendix 4, pp. 378–400.

[10] J. Vrancken, *The algebra of communicating processes with empty process*, Theoretical Comput. Sci., 177(1997), pp. 287–328.

Recent BRICS Report Series Publications

RS-99-22 **Luca Aceto, Zoltán Ésik, and Anna Ingólfsdóttir.** ***On the Two-Variable Fragment of the Equational Theory of the Max-Sum Algebra of the Natural Numbers*****. August 1999. 22 pp.**

RS-99-21 **Olivier Danvy.** ***An Extensional Characterization of Lambda-Lifting and Lambda-Dropping*****. August 1999. 13 pp. Extended version of an article to appear in** ***Fourth Fuji International Symposium on Functional and Logic Programming*****, FLOPS '99 Proceedings (Tsukuba, Japan, November 11–13, 1999). This report supersedes the earlier report BRICS RS-98-2.**

RS-99-20 **Ulrich Kohlenbach.** ***A Note on Spector's Quantifier-Free Rule of Extensionality*****. August 1999. 5 pp. To appear in** ***Archive for Mathematical Logic*****.**

RS-99-19 **Marcin Jurdziński and Mogens Nielsen.** ***Hereditary History Preserving Bisimilarity is Undecidable*****. June 1999. 18 pp.**

RS-99-18 **M. Oliver Möller and Harald Rueß.** ***Solving Bit-Vector Equations of Fixed and Non-Fixed Size*****. June 1999. 18 pp. Revised version of an article appearing under the title** ***Solving Bit-Vector Equations*** **in Gopalakrishnan and Windley, editors,** ***Formal Methods in Computer-Aided Design: Second International Conference*****, FMCAD '98 Proceedings, LNCS 1522, 1998, pages 36–48.**

RS-99-17 **Andrzej Filinski.** ***A Semantic Account of Type-Directed Partial Evaluation*****. June 1999. To appear in Nadathur, editor,** ***International Conference on Principles and Practice of Declarative Programming*****, PPDP99 '99 Proceedings, LNCS, 1999.**

RS-99-16 **Rune B. Lyngsø and Christian N. S. Pedersen.** ***Protein Folding in the 2D HP Model*****. June 1999. 15 pp.**

RS-99-15 **Rune B. Lyngsø, Michael Zuker, and Christian N. S. Pedersen.** ***An Improved Algorithm for RNA Secondary Structure Prediction*****. May 1999. 24 pp. An alloy of two articles appearing in Istrail, Pevzner and Waterman, editors,** ***Third Annual International Conference on Computational Molecular Biology*****, RECOMB 99 Proceedings, 1999, pages 260–267, and** ***Bioinformatics*****, 15, 1999.**