Which Two-Sorted Algebras of Booleans and Naturals have a Finite Basis?

Wan Fokkink, Jaco van de Pol, and Sujith Vijay

Abstract. We show that the two-sorted algebra of Booleans and naturals with conjunction, addition and inequality is not finitely based. If addition is removed, or negation is included, then the resulting algebra is finitely based.

1. Introduction

A basis for an algebra A is a set of equations E such that an equation is true in A if and only if it is a logical consequence of E. The existence of finite bases for algebras is a classic topic of study in universal algebra (see, e.g., [16]), dating back to Lyndon [13]. Murskiĭ [18] proved that "almost all" finite algebras (namely all quasi-primal ones) are finitely based, while in [17] he presented an example of a three-element algebra that has no finite basis. McKenzie [15] settled Tarski's Finite Basis Problem in the negative, by showing that the question whether a finite algebra is finitely based is algorithmically undecidable.

As an example of equational logic, Henkin [12] showed that the algebra of natural numbers with addition and multiplication is finitely based. (Subsequently we will refer to the algebra of natural numbers as the algebra of naturals.) Gurevič [11] showed that the algebra of naturals with addition, multiplication and exponentiation is not finitely based. The proof is based on an identity by Wilkie [21], which provided a negative answer to Tarski's High School Algebra Problem. Aceto, Ésik and Ingólfsdóttir [1] proved that a set of equations in finitely many variables (so in particular a finite set of equations) cannot be a basis for the algebra of naturals with addition and maximum.

As further related work, iterative algebras without a finite basis can be found in [2, 8, 9], and a process algebra without a finite basis in [3].

In this paper, we consider two-sorted algebras of Booleans and naturals. We start with proving that the algebra with successor, conjunction and inequality is finitely based. We extend the algebra with addition and present an infinite set of equations, which we prove to be a basis for this second algebra. The proof relies heavily on results for so-called cutting planes [10] by Chvátal [7] and Schrijver

1991 *Mathematics Subject Classification*: 03B25, 08B99.
Key words and phrases: two-sorted algebra, Booleans, naturals, finite basis.
This research was carried out while Sujith Vijay was a student at IIT Delhi, and visiting CWI on a Summer Internship.

[19]. Furthermore, we show that the second algebra is not finitely based. Next, we extend the second algebra with negation and prove that the resulting third algebra is finitely based. Finally, we extend the third algebra with a conditional operator, so that it encompasses the maximum operator, and prove that, in contrast with the negative result obtained in [1], this fourth algebra is finitely based.

It is well-known that the fact whether an algebra is finitely based depends in a subtle way on the precise set of operators. The following relationship with recursion theory is shown in [4]. If the set of true equations in some algebra is recursively enumerable, then there exists a finite basis, provided hidden sorts and function symbols are allowed. Two remarks are in order. The specification is complete with respect to equations in the smaller language; the hidden function symbols are auxiliary operators only. Second, from the general construction it is not clear how to obtain a concrete finite basis.

The algebras that we deal with are clearly recursively enumerable (even recursive). So, by the recursion theoretical argument it is immediately clear that by extending the signature, we can get a finitely based algebra. Our contribution is that for certain examples, we give concrete axiomatizations in a systematic way, by adding a Boolean algebra. Moreover, we prove completeness of the algebra over the full new language.

2. Inequality and conjunction

We start our study of two-sorted algebras of Booleans $\mathbb{B}$ and naturals $\mathbb{N}$ with the algebra $\mathcal{A} = \langle \mathbb{B}, \mathbb{N}; 0, S, \wedge, \preccurlyeq \rangle$. Here, $S : \mathbb{N} \to \mathbb{N}$ denotes the successor, $\wedge : \mathbb{B}\times\mathbb{B} \to \mathbb{B}$ is conjunction and $\preccurlyeq : \mathbb{N} \times \mathbb{N} \to \mathbb{B}$ represents the smaller-or-equal relation. We use T and F to abbreviate $0 \preccurlyeq 0$ and $S(0) \preccurlyeq 0$, respectively. We assume two countably infinite sets of variables of sorts Boolean and natural. A valuation is a mapping from variables (of sort Boolean and natural) to $\mathbb{B}$ and $\mathbb{N}$, respectively. As notational binding convention, $\preccurlyeq$ binds stronger than $\wedge$. Let $S^0(t)$ denote t and let $S^{n+1}(t)$ denote $S(S^n(t))$.

Let u, v, w denote variables of sort Boolean and x, y, z variables of sort natural. The axioms (A1-11) below are all true in $\mathcal{A}$. Let Σ denote the equational base consisting of these axioms. In this section, we show that Σ is a finite basis for $\mathcal{A}$. In other words, given two terms s and t over this algebra such that $\sigma(s)$ coincides with $\sigma(t)$ for all valuations σ, it can be proved using Σ that $s \approx t$ with the usual rules of equational logic (see, e.g., [12]).

$$
\begin{array}{lrcl}
\text{(A1)} & u \wedge T & \approx & u \\
\text{(A2)} & u \wedge F & \approx & F \\
\text{(A3)} & u \wedge v & \approx & v \wedge u \\
\text{(A4)} & u \wedge (v \wedge w) & \approx & (u \wedge v) \wedge w \\
\text{(A5)} & u \wedge u & \approx & u \\
\text{(A6)} & 0 \preccurlyeq x & \approx & T \\
\text{(A7)} & x \preccurlyeq x & \approx & T
\end{array}
$$

(A8)	$x \preccurlyeq S(x)$	$\approx$	T
(A9)	$S(x) \preccurlyeq x$	$\approx$	F
(A10)	$S(x) \preccurlyeq S(y)$	$\approx$	$x \preccurlyeq y$
(A11)	$(x \preccurlyeq y \wedge y \preccurlyeq z) \wedge x \preccurlyeq z$	$\approx$	$x \preccurlyeq y \wedge y \preccurlyeq z$

In view of (A3,4), Boolean terms can be taken modulo associativity and commutativity of conjunction. Let $s \approx_\Sigma t$ denote that the equation can be derived from Σ. By (A10) we have $S^n(x) \preccurlyeq S^n(y) \approx_\Sigma x \preccurlyeq y$ for all $n \geq 0$. We say that a Boolean term b is *satisfiable* if $\sigma(b) = T$ for some valuation σ; in this case, σ is said to *satisfy* b.

Let b and c be Boolean terms, not containing any Boolean variables, that coincide under all valuations. We develop the machinery to prove $b \approx_\Sigma c$.

Let V_{bc} be a non-empty finite set of variables of sort natural that includes all variables occurring in b or c. Consider a Boolean term d that only contains variables from V_{bc}. It is of the form

$$s_1 \preccurlyeq t_1 \wedge \cdots \wedge s_n \preccurlyeq t_n$$

where the s_i and t_j are of the form $S^m(0)$ or $S^m(x)$ with $x \in V_{bc}$. In view of (A1,6), we can add conjuncts $0 \preccurlyeq x$ for all $x \in V_{bc}$; let $\hat{d}$ denote the resulting Boolean term.

We construct a weighted directed graph G_d. Its vertex set P is $V_{bc} \cup \{0\}$. Furthermore, each conjunct in $\hat{d}$, say $S^m(p) \preccurlyeq S^n(q)$ with $p, q \in P$, gives rise to an edge from p to q with cost $n - m$. The cost of a path in G_d is the sum of the costs of its edges.

Lemma 1. *$S^n(x) \preccurlyeq x \approx_\Sigma F$ for $n \geq 1$.*

Proof. By induction on n. The base case $n = 1$ is (A9). The inductive case goes as follows:

$$\begin{array}{lll}
 & S^{n+1}(x) \preccurlyeq x & \\
\approx_\Sigma & S^{n+1}(x) \preccurlyeq x \wedge x \preccurlyeq S(x) & (\mathrm{A1}, 8) \\
\approx_\Sigma & S^{n+1}(x) \preccurlyeq x \wedge x \preccurlyeq S(x) \wedge S^{n+1}(x) \preccurlyeq S(x) & (\mathrm{A11}) \\
\approx_\Sigma & S^{n+1}(x) \preccurlyeq x \wedge x \preccurlyeq S(x) \wedge S^{n}(x) \preccurlyeq x & (\mathrm{A10}) \\
\approx_\Sigma & S^{n+1}(x) \preccurlyeq x \wedge x \preccurlyeq S(x) \wedge F & (\text{ind. hyp.}) \\
\approx_\Sigma & F & (\mathrm{A2})
\end{array}$$

□

Proposition 1. *If G_d contains a cycle of negative cost, then $d \approx_\Sigma F$.*

Proof. If G_d contains a cycle of cost $k < 0$, then $\hat{d}$ contains conjuncts $S^{m_i}(p_i) \preccurlyeq S^{n_i}(p_{i+1})$ for $i = 0, \ldots, \ell$ with $p_{\ell+1} = p_0$ and $(n_0 - m_0) + \cdots + (n_\ell - m_\ell) = k$. Using (A10,11), we get $\hat{d} \approx_\Sigma \hat{d} \wedge S^{-k}(p_0) \preccurlyeq p_0$. So by Lemma 1 and (A2), $\hat{d} \approx_\Sigma F$. Hence, $d \approx_\Sigma \hat{d} \approx_\Sigma F$. □

Assume G_d does not contain cycles of negative cost. Let ∞ denote infinity: $k < \infty$ for all $k \in \mathbb{Z}$. We define a mapping $\mu_d : P \times P \to \mathbb{Z} \cup \{\infty\}$, where $\mu_d(p, q)$ is the minimum cost of any path from p to q in G_d, or the value ∞ if no path from p to q exists in G_d. Such a minimum exists, owing to the absence of cycles of negative cost. Proposition 2 below expresses that if $p, q \in P$ with $\mu_d(p,q) < \infty$, then d implies $p \preccurlyeq S^{\mu_d(p,q)}(q)$ if $\mu_d(p,q) \geq 0$ or $S^{-\mu_d(p,q)}(p) \preccurlyeq q$ if $\mu_d(p,q) < 0$. For notational convenience, inequalities $S^m(p) \preccurlyeq q$ are written as $p \preccurlyeq S^{-m}(q)$. First, we need to prove two lemmas.

Lemma 2. *$x \preccurlyeq S^n(x) \approx_\Sigma T$ for $n \geq 0$.*

Proof. By induction on n. The base case $n = 0$ is (A7). For the inductive case, assume $x \preccurlyeq S^n(x) \approx_\Sigma T$ can be derived. Using (A10), $S(x) \preccurlyeq S^{n+1}(x) \approx_\Sigma T$. Also, by (A8), $x \preccurlyeq S(x) \approx_\Sigma T$. So using (A1,11), $x \preccurlyeq S^{n+1}(x) \approx_\Sigma T$. □

Lemma 3. *$x \preccurlyeq S^k(y) \wedge x \preccurlyeq S^\ell(y) \approx_\Sigma x \preccurlyeq S^k(y)$ if $k \leq \ell$.*

Proof. We focus on the case where $k \geq 0$ and $\ell \geq 0$. The cases where $k < 0$ or $\ell < 0$ can be treated in a similar fashion.

By Lemma 2 and (A10), $S^k(y) \preccurlyeq S^\ell(y) \approx_\Sigma T$. Thus,

$$\begin{array}{lll} & x \preccurlyeq S^k(y) \wedge x \preccurlyeq S^\ell(y) & \\ \approx_\Sigma & x \preccurlyeq S^k(y) \wedge S^k(y) \preccurlyeq S^\ell(y) \wedge x \preccurlyeq S^\ell(y) & \text{(A1)} \\ \approx_\Sigma & x \preccurlyeq S^k(y) \wedge S^k(y) \preccurlyeq S^\ell(y) & \text{(A11)} \\ \approx_\Sigma & x \preccurlyeq S^k(y) & \text{(A1)} \end{array}$$

□

Proposition 2. *If G_d does not contain cycles of negative cost, then*

$$d \approx_\Sigma \bigwedge_{\{\langle p,q\rangle \in P\times P \mid \mu_d(p,q)<\infty\}} p \preccurlyeq S^{\mu_d(p,q)}(q).$$

Proof. Using induction on the number of edges in a path of minimal cost from p to q, we can derive $\hat{d} \approx_\Sigma \hat{d} \wedge p \preccurlyeq S^{\mu_d(p,q)}(q)$ for all $p, q \in P$ with $\mu_d(p,q) < \infty$. The base case with zero edges follows by (A7), the base case with one edge by (A10), and the inductive case with more than one edge by (A10,11). So

$$d \approx_\Sigma \hat{d} \approx_\Sigma \hat{d} \wedge \bigwedge_{\{\langle p,q\rangle \in P\times P \mid \mu_d(p,q)<\infty\}} p \preccurlyeq S^{\mu_d(p,q)}(q).$$

Since $\mu_d(p,q)$ is the minimum cost of any path from p to q, Lemma 3 together with (A10) can be used to eliminate all conjuncts of $\hat{d}$ from the latter term. □

We are now ready to prove the converse of Proposition 1.

Proposition 3. *If G_d does not contain cycles of negative cost, then d is satisfiable.*

Proof. Let σ be a valuation with $\sigma(x) = -\mu_d(0,x)$ for all $x \in V_{bc}$. Note that $\mu_d(0,x) \leq 0$, and so $0 \leq \sigma(x) < \infty$ for all $x \in V_{bc}$. For we took care to include conjuncts $0 \preccurlyeq x$ in $\hat{d}$, which give rise to edges of zero cost from 0 to x in G_d. Note furthermore that $\sigma(0) = 0 = -\mu_d(0,0)$, owing to the absence of cycles of negative cost in G_d.

For any pair $p, q \in P$ with $\mu_d(p,q) < \infty$, we have $\mu_d(0,q) \leq \mu_d(0,p) + \mu_d(p,q)$; i.e., $\sigma(p) \leq \sigma(q) + \mu_d(p,q)$. So in view of Proposition 2, σ satisfies d. □

Now let us return to the Boolean terms b and c, not containing any Boolean variables, that coincide under all valuations. Clearly, b and c only contain variables from V_{bc}. Let us assume that b and c are satisfiable. In that case, by Proposition 1, G_b and G_c do not contain cycles of negative cost, so μ_b and μ_c are well-defined.

Proposition 4. *If b and c coincide under all valuations and are satisfiable, then $\mu_b(p,q) = \mu_c(p,q)$ for all $p, q \in P$.*

Proof. Assume, toward a contradiction, that $\mu_b(p,q) > \mu_c(p,q)$ for some pair $p, q \in P$. Choose an M sufficiently large (this is specified below). We define for $r \in P$:

$$\nu(r) = \begin{cases} \mu_b(p,r) & \text{if } \mu_b(p,r) < \infty \\ M + \min\{\mu_b(s,r) \mid s \in P\} & \text{otherwise} \end{cases}$$

$\mu_b(0,r) \leq 0$, so $\nu(r) < \infty$ for all $r \in P$. Since $\mu_b(p,q) > \mu_c(p,q)$, by choosing M sufficiently large, we can enforce

$$\nu(q) > \mu_c(p,q).$$

Furthermore, by taking $M \geq \mu_b(p,r) - \mu_b(s,r)$ for all $r, s \in P$ with $\mu_b(p,r) < \infty$ and $\mu_b(s,r) < \infty$, we get

$$\nu(r) \leq M + \mu_b(s,r) \text{ for all } r, s \in P \text{ with } \mu_b(s,r) < \infty.$$

Finally, we have

$$\nu(r) \leq \nu(s) + \mu_b(s,r) \text{ for all } r, s \in P \text{ with } \mu_b(s,r) < \infty.$$

Because if $\mu_b(p,s) < \infty$, then $\mu_b(p,r) < \infty$, so $\nu(r) = \mu_b(p,r) \leq \mu_b(p,s) + \mu_b(s,r) = \nu(s) + \mu_b(s,r)$. And if $\mu_b(p,s) = \infty$, then $\nu(s) = M + \mu_b(t,s)$ for some $t \in P$ with $\mu_b(t,s) < \infty$. Then $\mu_b(t,r) < \infty$, so $\nu(r) \leq M + \mu_b(t,r) \leq M + \mu_b(t,s) + \mu_b(s,r) = \nu(s) + \mu_b(s,r)$.

Let σ be a valuation with $\sigma(x) = \nu(0) - \nu(x)$ for all $x \in V_{bc}$. Since $\mu_b(0,x) \leq 0$, we have $\nu(x) \leq \nu(0) + \mu_b(0,x) \leq \nu(0)$, and so $\sigma(x) \geq 0$ for all $x \in V_{bc}$. Furthermore, $\sigma(0) = 0 = \nu(0) - \nu(0)$. We show that σ satisfies b, but not c.

Consider any pair $r, s \in P$ with $\mu_b(s,r) < \infty$. Since $\nu(r) \leq \nu(s) + \mu_b(s,r)$, we have $\sigma(s) = \nu(0) - \nu(s) \leq \nu(0) - (\nu(r) - \mu_b(s,r)) = \sigma(r) + \mu_b(s,r)$. So σ satisfies $s \preccurlyeq S^{\mu_b(s,r)}(r)$. Hence, in view of Proposition 2, σ satisfies b.

By Proposition 1, G_b does not contain cycles of negative cost, so $\nu(p) = \mu_b(p,p) = 0$. Moreover, $\nu(q) > \mu_c(p,q)$. So $\sigma(p) = \nu(0) - \nu(p) = \nu(0) = \sigma(q) + \nu(q) > \sigma(q) + \mu_c(p,q)$. Then σ does not satisfy $p \preccurlyeq S^{\mu_c(p,q)}(q)$, so in view of Proposition 2, σ does not satisfy c. This contradicts that b and c coincide under all valuations. $\square$

Theorem 1. *(A1-11) constitute a basis for $\mathcal{A}$.*

Proof. Terms of sort natural are of the form $S^n(0)$ or $S^n(x)$. So if two terms of sort natural coincide under all valuations, then clearly they are syntactically equal.

Let b_0 and c_0 be Boolean terms that coincide under all valuations. They are of the form $b \wedge u_1 \wedge \cdots \wedge u_m$ and $c \wedge v_1 \wedge \cdots \wedge v_n$, respectively, where b and c do not contain Boolean variables. By setting all u_i and v_j to T, one obtains that b and c coincide under all valuations. We distinguish two cases.

- CASE 1: b and c are not satisfiable.
  Then according to Proposition 3, G_b and G_c contain cycles of negative cost. So by Proposition 1, $b \approx_\Sigma F \approx_\Sigma c$. Hence, by (A2), $b_0 \approx_\Sigma F \approx_\Sigma c_0$.
- CASE 2: b and c are satisfiable.
  Then clearly $u_1 \wedge \cdots \wedge u_m$ and $v_1 \wedge \cdots \wedge v_n$ must consist of the same Boolean variables. By (A5), $u_1 \wedge \cdots \wedge u_m \approx_\Sigma v_1 \wedge \cdots \wedge v_n$.
  By Proposition 1, G_b and G_c do not contain cycles of negative cost. So by Proposition 2 together with Proposition 4,

$$\begin{array}{lll} b & \approx_\Sigma & \bigwedge_{\{\langle p,q\rangle \in P\times P \mid \mu_b(p,q)<\infty\}} p \preccurlyeq S^{\mu_b(p,q)}(q) \\ & \approx_\Sigma & \bigwedge_{\{\langle p,q\rangle \in P\times P \mid \mu_c(p,q)<\infty\}} p \preccurlyeq S^{\mu_c(p,q)}(q) \quad \approx_\Sigma \quad c. \end{array}$$

  Hence, $b_0 = b \wedge u_1 \wedge \cdots \wedge u_m \approx_\Sigma c \wedge v_1 \wedge \cdots \wedge v_n \approx_\Sigma c_0$.

□

Remark. In contrast to Theorem 1, the algebra that is obtained if $\preccurlyeq$ is replaced by eq, representing the equality function of type $\mathbb{N} \times \mathbb{N} \to \mathbb{B}$, has no finite basis. We will not elaborate on the proof, but only notice that it can be constructed along the same lines as the proof of Theorem 4, by giving an infinite basis containing, among others, the true equations $eq(S^n(x), x) = F$ for $n \geq 1$.

3. Addition

We introduce addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, and continue to study the algebra $\mathcal{B} = \langle \mathbb{B}, \mathbb{N}; 0, 1, \wedge, +, \preccurlyeq\rangle$. Note that $S(t)$ is definable as $t+1$. As binding convention, $+$ binds stronger than $\preccurlyeq$.

(A1-11) and the axioms below, consisting of (B1-5) together with the infinite family (B6.n) for $n > 1$, are true in $\mathcal{B}$. Let Λ denote the equational base consisting of (A1-11), (B1-5) and (B6.n) for $n > 1$. We show that Λ constitutes a basis for $\mathcal{B}$. In view of (B2,3), natural numbers can be taken modulo associativity and commutativity of addition. We use nt to denote $t + \cdots + t$ (n summands) for $n \geq 1$.

$$\begin{array}{lrcl} \text{(B1)} & x + 0 & \approx & x \\ \text{(B2)} & x + y & \approx & y + x \\ \text{(B3)} & (x+y)+z & \approx & x + (y+z) \\ \text{(B4)} & x \preccurlyeq y & \approx & x + z \preccurlyeq y + z \\ \text{(B5)} & x + x \preccurlyeq (y+y)+1 & \approx & x + x \preccurlyeq y + y \\ \text{(B6.}n\text{)} & nx \preccurlyeq ny & \approx & x \preccurlyeq y \end{array}$$

$s \approx_\Lambda t$ denotes that the equation can be derived from Λ. Note that (B6.n) for $n > 1$ can be derived from (B6.p) for primes p. Because if $mx \preccurlyeq my \approx_\Lambda x \preccurlyeq y$ and $nx \preccurlyeq ny \approx_\Lambda x \preccurlyeq y$ can be derived, then $(mn)x \preccurlyeq (mn)x \approx_\Lambda nx \preccurlyeq ny \approx_\Lambda x \preccurlyeq y$. Furthermore, (A10) follows directly from (B4), and (A7,8) can be derived from the other axioms:

$$
\begin{array}{llllr}
 & x \preccurlyeq x & & x \preccurlyeq x+1 & \\
\approx_\Lambda & 0+x \preccurlyeq 0+x & \approx_\Lambda & x+0 \preccurlyeq x+1 & \text{(B1)} \\
\approx_\Lambda & 0 \preccurlyeq 0 & \approx_\Lambda & 0 \preccurlyeq 1 & \text{(B4)} \\
\approx_\Lambda & T & \approx_\Lambda & T & \text{(A6)}
\end{array}
$$

Let b and c be Boolean terms, not containing any Boolean variables, that coincide under all valuations. We develop the machinery to prove $b \approx_\Lambda c$.

Using (A7,9) and (B1,4), b and c can be written as conjuncts of inequalities

$$n_0 + n_1x_1 + \cdots + n_kx_k \preccurlyeq n_0' + n_1'x_1 + \cdots + n_k'x_k.$$

Furthermore, by (A6), conjuncts $0 \preccurlyeq x_i$ for $i = 1, \ldots, k$ can be added, so that negative solutions are ruled out. This enables us to use the following results from integer programming.

Chvátal [7] and Schrijver [19] (see also [20, Chapter 23]) showed that a number of proof principles, called *cutting planes*, suffice to equate each pair of such conjuncts that have the same solutions over the *integer* domain. Here, we follow the presentation of cutting planes in [6].

Definition 1. The three principles underlying *cutting plane proofs* are:

(1) $nx \preccurlyeq ny + r \Rightarrow x \preccurlyeq y$ for $r = 0, \ldots, n-1$;
(2) $x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 \Rightarrow x_1 + x_2 \preccurlyeq y_1 + y_2$;
(3) $x \preccurlyeq m \Rightarrow x \preccurlyeq n$ if $m \leq n$.

Theorem 2. (Chvátal '73, Schrijver '80) *Let b and c be conjuncts of inequalities $s \preccurlyeq t$, where the s and t are of the form $n_0 + n_1x_1 + \cdots + n_kx_k$.*

(1) *If b is not satisfiable for any valuation* over the integer domain*, then there is a cutting plane proof for $b \approx F$.*
(2) *If b and c are satisfiable, and they coincide under all valuations* over the integer domain*, then there is a cutting plane proof for $b \approx c$.*

We proceed to show that the three principles in Definition 1 can be derived from the axioms. The third principle is a straightforward consequence of Lemma 2 and (A1,10,11). We focus on deriving the first two principles.

Proposition 5. $x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 \approx_\Lambda x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 \wedge x_1 + x_2 \preccurlyeq y_1 + y_2$.

Proof.

$$
\begin{array}{lll}
 & x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 & \\
\approx_\Lambda & x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 \wedge x_1 + x_2 \preccurlyeq y_1 + x_2 \wedge x_2 + y_1 \preccurlyeq y_2 + y_1 & \text{(A5, B4)} \\
\approx_\Lambda & x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 \wedge x_1 + x_2 \preccurlyeq y_1 + x_2 \wedge x_2 + y_1 \preccurlyeq y_2 + y_1 & \\
 & \wedge\ x_1 + x_2 \preccurlyeq y_1 + y_2 & \text{(A11)} \\
\approx_\Lambda & x_1 \preccurlyeq y_1 \wedge x_2 \preccurlyeq y_2 \wedge x_1 + x_2 \preccurlyeq y_1 + y_2 & \text{(B4, A5)}
\end{array}
$$

□

Lemma 4. $2^m x \preccurlyeq 2^m y + r \approx_\Lambda x \preccurlyeq y$ *for* $r = 0, \ldots, 2^m - 1$.

Proof. By induction on m. The base case $m = 0$ is trivial. For the inductive case, assume the result holds for m, and let $0 \leq r < 2^{m+1}$. Then $0 \leq r/2 < 2^m$, so if r is even,

$$\begin{array}{rcll} 2^{m+1}x \preccurlyeq 2^{m+1}y + r & \approx_\Lambda & 2^m x \preccurlyeq 2^m y + r/2 & \text{(B6.2)} \\ & \approx_\Lambda & x \preccurlyeq y & \text{(ind. hyp.)} \end{array}$$

and if r is odd,

$$\begin{array}{rcll} 2^{m+1}x \preccurlyeq 2^{m+1}y + r & \approx_\Lambda & 2^{m+1}x \preccurlyeq 2^{m+1}y + (r-1) & \text{(B5)} \\ & \approx_\Lambda & 2^m x \preccurlyeq 2^m y + (r-1)/2 & \text{(B6.2)} \\ & \approx_\Lambda & x \preccurlyeq y & \text{(ind. hyp.)} \end{array}$$

□

Proposition 6. *$nx \preccurlyeq ny + r \approx_\Lambda x \preccurlyeq y$ for $r = 0, \ldots, n-1$.*

Proof. Fix an m with $2^m \geq n$. Let $2^m r = qn - r'$ with $0 \leq r' < n$. Note that $qn \leq 2^m(n-1) + n - 1 < 2^m n$, so $0 \leq q < 2^m$. Hence,

$$\begin{array}{rcll} nx \preccurlyeq ny + r & \approx_\Lambda & 2^m nx \preccurlyeq 2^m(ny + r) + r' & \text{(Lem. 4)} \\ & \approx_\Lambda & 2^m nx \preccurlyeq 2^m ny + qn & \\ & \approx_\Lambda & 2^m x \preccurlyeq 2^m y + q & \text{(B6.}n\text{)} \\ & \approx_\Lambda & x \preccurlyeq y & \text{(Lem. 4)} \end{array}$$

□

Theorem 3. *(A1-6,9,11), (B1-5) and (B6.p) for primes p constitute a basis for $\mathcal{B}$.*

Proof. Using (B1), each term of sort natural can be written in the form $n_0 + n_1 x_1 + \cdots + n_k x_k$. Clearly, if two terms of the latter form coincide under all valuations, then they are syntactically equal (modulo associativity and commutativity of addition).

Let b_0 and c_0 be Boolean terms that coincide under all valuations. They are of the form $b \wedge u_1 \wedge \cdots \wedge u_m$ and $c \wedge v_1 \wedge \cdots \wedge v_n$, respectively, where b and c do not contain Boolean variables. Clearly, b and c coincide under all valuations. We distinguish two cases.

- Case 1: b and c are not satisfiable.

  Then b and c do not have solutions in the natural numbers. By (A6), conjuncts $0 \preccurlyeq x$ can be added to guarantee that they do not have integer solutions. Since the three proof principles of cutting planes can be derived from the axioms, Theorem 2(1) implies $b \approx_\Lambda F \approx_\Lambda c$. Hence, by (A2), $b_0 \approx_\Lambda F \approx_\Lambda c_0$.
- Case 2: b and c are satisfiable.

  Then $u_1 \wedge \cdots \wedge u_m$ and $v_1 \wedge \cdots \wedge v_n$ consist of the same Boolean variables. By (A5), $u_1 \wedge \cdots \wedge u_m \approx_\Lambda v_1 \wedge \cdots \wedge v_n$. Furthermore, by (A6), conjuncts $0 \preccurlyeq x$ can be added to guarantee that b and c coincide over the integer domain. So, according to Theorem 2(2), $b \approx_\Lambda c$. So $b_0 = b \wedge u_1 \wedge \cdots \wedge u_m \approx_\Lambda c \wedge v_1 \wedge \cdots \wedge v_n \approx_\Lambda c_0$.

□

We proceed with proving that $\mathcal{B}$ does not have a finite basis, by exhibiting algebras M_p for primes p such that:

(1) for each finite set of equations that are true in $\mathcal{B}$, there is a prime p such that the equations hold in M_p; and
(2) (B6.p) does not hold in M_p for primes p.

The algebras M_p consist of the Booleans $\mathbb{B}$ together with $\mathbb{N}^3$. The two-sorted algebra of Booleans and naturals is embedded in M_p: conjunction is interpreted as usual, 0 and 1 are mapped to $(0,0,0)$ and $(1,0,0)$, respectively, and $+, \preccurlyeq \colon \mathbb{N}^3 \times \mathbb{N}^3 \to \mathbb{B}$ are defined on $\mathbb{N}^3$ as follows. By abuse of notation, in the right-hand sides of these definitions the symbol $+$ represents standard addition on natural numbers, while $\wedge$ and $\vee$ denote standard conjunction and disjunction, respectively, on the Booleans.

$$(m_0,m_1,m_2)+(n_0,n_1,n_2) \quad =_{\text{def}} \quad (m_0+n_0, m_1+n_1, m_2+n_2)$$

$$\begin{aligned}(m_0,m_1,m_2) \preccurlyeq (n_0,n_1,n_2) \quad =_{\text{def}} \quad & m_0 \le n_0 \wedge (m_1+n_1 < m_2+n_2 \vee \\ & (m_1+n_1 = m_2+n_2 \wedge m_1 \equiv n_1 \pmod p))\end{aligned}$$

Note that if p divides n, then (B6.n) does not hold in M_p. Namely, $(0,n,0) \preccurlyeq (0,0,n)$, because $n \equiv 0 \pmod p$, but not $(0,1,0) \preccurlyeq (0,0,1)$.

Proposition 7. *Let p be a prime. (A1-6,9,11), (B1-5) and (B6.n) for $n \not\equiv 0 \pmod p$ hold in M_p.*

Proof. (A1-5) and (B1-3) clearly hold in M_p. We focus on the remaining axioms.

(A6): $(0,0,0) \preccurlyeq (n_0,n_1,n_2) = 0 \le n_0 \wedge (0 < n_1+n_2 \vee (0 = n_1+n_2 \wedge 0 \equiv n_1 \pmod p))) = T$. Because if $0 = n_1+n_2$, then $n_1 = 0$.

(A9): $(n_0+1,n_1,n_2) \preccurlyeq (n_0,n_1,n_2) = F$, since $n_0+1 > n_0$.

(A11): If $(\ell_0,\ell_1,\ell_2) \preccurlyeq (m_0,m_1,m_2) \wedge (m_0,m_1,m_2) \preccurlyeq (n_0,n_1,n_2) = T$, then $\ell_0 \le m_0 \le n_0$, and either $\ell_1+\ell_2 < m_1+m_2 \le n_1+n_2$, $\ell_1+\ell_2 \le m_1+m_2 < n_1+n_2$, or $\ell_1+\ell_2 = m_1+m_2 = n_1+n_2$ with $\ell_1 \equiv m_1 \equiv n_1 \pmod p$. This implies $\ell_0 \le n_0$, and either $\ell_1+\ell_2 < n_1+n_2$, or $\ell_1+\ell_2 = n_1+n_2$ with $\ell_1 \equiv n_1 \pmod p$. So $(\ell_0,\ell_1,\ell_2) \preccurlyeq (n_0,n_1,n_2) = T$.

(B4):

$$\begin{aligned} & (\ell_0+n_0, \ell_1+n_1, \ell_2+n_2) \preccurlyeq (m_0+n_0, m_1+n_1, m_2+n_2) \\ = \; & \ell_0+n_0 \le m_0+n_0 \wedge (\ell_1+n_1+\ell_2+n_2 < m_1+n_1+m_2+n_2 \vee \\ & (\ell_1+n_1+\ell_2+n_2 = m_1+n_1+m_2+n_2 \wedge \ell_1+n_1 \equiv m_1+n_1 \pmod p)) \\ = \; & \ell_0 \le m_0 \wedge (\ell_1+\ell_2 < m_1+m_2 \vee \\ & (\ell_1+\ell_2 = m_1+m_2 \wedge \ell_1 \equiv m_1 \pmod p)) \\ = \; & (\ell_0,\ell_1,\ell_2) \preccurlyeq (m_0,m_1,m_2) \end{aligned}$$

(B5):

$$\begin{aligned} & (2m_0, 2m_1, 2m_2) \preccurlyeq (2n_0+1, 2n_1, 2n_2) \\ = \; & 2m_0 \le 2n_0+1 \wedge (2m_1+2m_2 < 2n_1+2n_2 \vee \\ & (2m_1+2m_2 = 2n_1+2n_2 \wedge 2m_1 \equiv 2n_1 \pmod p)) \\ = \; & 2m_0 \le 2n_0 \wedge (2m_1+2m_2 < 2n_1+2n_2 \vee \\ & (2m_1+2m_2 = 2n_1+2n_2 \wedge 2m_1 \equiv 2n_1 \pmod p)) \\ = \; & (2m_0, 2m_1, 2m_2) \preccurlyeq (2n_0, 2n_1, 2n_2) \end{aligned}$$

(B6.n) with $n \not\equiv 0 \pmod p$:

$$\begin{array}{ll} & (n\ell_0, n\ell_1, n\ell_2) \preccurlyeq (nm_0, nm_1, nm_2) \\ = & n\ell_0 \leq nm_0 \wedge (n\ell_1 + n\ell_2 < nm_1 + nm_2 \vee \\ & (n\ell_1 + n\ell_2 = nm_1 + nm_2 \wedge n\ell_1 \equiv nm_1 \pmod p)) \\ = & \ell_0 \leq m_0 \wedge (\ell_1 + \ell_2 < m_1 + m_2 \vee \\ & (\ell_1 + \ell_2 = m_1 + m_2 \wedge \ell_1 \equiv m_1 \pmod p)) \\ = & (\ell_0, \ell_1, \ell_2) \preccurlyeq (m_0, m_1, m_2) \end{array}$$

□

Theorem 4. *$\mathcal{B}$ does not have a finite basis.*

Proof. Let E be a finite set of equations that are true in $\mathcal{B}$. By Theorem 3, the equations in E can be derived from (A1-6,9,11), (B1-5) and (B6.p) for primes p. Since each proof of an equation in E requires only a finite number of applications of axioms, the equations in E can be derived from (A1-6,9,11), (B1-5) and (B6.p) where p ranges over a finite set P of primes. Fix a prime p outside P. By Proposition 7, all equations in E hold in M_p. Since (B6.p) does not hold in M_p, it cannot be derived from E. □

4. Negation

We introduce negation $\neg : \mathbb{B} \to \mathbb{B}$, and continue to study the algebra $\mathcal{C} = \langle \mathbb{B}, \mathbb{N}; 0, 1, \neg, \wedge, +, \preccurlyeq \rangle$. We use $\vee$ for notational convenience, where $b \vee c$ represents $\neg(\neg b \wedge \neg c)$. As binding convention, $\neg$ binds stronger than $\wedge$. The axioms (C1-4) below are true in $\mathcal{C}$.

Let Γ denote the equational base consisting of (A1-6,9,11), (B1-4) and (C1-4). We show that Γ constitutes a basis for $\mathcal{C}$.

$$\begin{array}{lrcl} \text{(C1)} & u \wedge \neg u & \approx & F \\ \text{(C2)} & \neg\neg u & \approx & u \\ \text{(C3)} & u \wedge (v \vee w) & \approx & (u \wedge v) \vee (u \wedge w) \\ \text{(C4)} & \neg(x \preccurlyeq y) & \approx & y + 1 \preccurlyeq x \end{array}$$

$s \approx_\Gamma t$ denotes that the equation can be derived from Γ. Due to our abbreviations, $\neg T \approx_\Gamma F$ is an instance of (C4). Furthermore, $u \vee T \approx_\Gamma T$ and $u \vee F \approx_\Gamma u$:

$$\begin{array}{rcll} \neg(\neg u \wedge \neg(0 \preccurlyeq 0)) & \approx_\Gamma & \neg(\neg u \wedge 1 \preccurlyeq 0) & \text{(C4, B1)} \\ & \approx_\Gamma & \neg(1 \preccurlyeq 0) & \text{(A2)} \\ & \approx_\Gamma & \neg\neg(0 \preccurlyeq 0) & \text{(B1, C4)} \\ & \approx_\Gamma & 0 \preccurlyeq 0 & \text{(C2)} \end{array}$$

$$\begin{array}{rcll} \neg(\neg u \wedge \neg(1 \preccurlyeq 0)) & \approx_\Gamma & \neg(\neg u \wedge \neg\neg(0 \preccurlyeq 0)) & \text{(C4, B1)} \\ & \approx_\Gamma & \neg(\neg u \wedge 0 \preccurlyeq 0) & \text{(C2)} \\ & \approx_\Gamma & \neg\neg u & \text{(A1)} \\ & \approx_\Gamma & u & \text{(C2)} \end{array}$$

(A9) can be derived from the other axioms (note that the derivations of (A7,8,10) in the previous section did not use (A9), (B5) or (B6.n)):

$$\begin{array}{lll} x+1 \preccurlyeq x & \approx_\Gamma \neg(x \preccurlyeq x) & \text{(C4)} \\ & \approx_\Gamma \neg T & \text{(A7)} \\ & \approx_\Gamma F & \text{(C4)} \end{array}$$

As in Section 3, we want to show that the three proof principles of cutting planes can be derived from the axioms. In Section 3 it was shown that these three principles can be derived from (A1-11), (B1-5) and (B6.n) for $n \geq 1$. So it suffices to derive (B5) and (B6.n) for $n \geq 1$ from our current set of axioms.

Lemma 5. *$x \preccurlyeq y \approx_\Gamma x \preccurlyeq y \wedge nx \preccurlyeq ny$ for $n \geq 1$.*

Proof. By induction on n. The base case $n = 1$ follows by (A5). For the inductive case, note that the derivation of Proposition 5 used neither (B5) nor (B6.n), so that it also follows from our current set of axioms.

$$\begin{array}{llll} x \preccurlyeq y & \approx_\Gamma & x \preccurlyeq y \wedge nx \preccurlyeq ny & \text{(ind. hyp.)} \\ & \approx_\Gamma & x \preccurlyeq y \wedge nx \preccurlyeq ny \wedge x + nx \preccurlyeq y + ny & \text{(Prop. 5)} \\ & \approx_\Gamma & x \preccurlyeq y \wedge (n+1)x \preccurlyeq (n+1)y & \text{(ind. hyp.)} \end{array}$$

□

We note that in order to prove $b \approx_\Gamma c$, it suffices to derive $b \wedge \neg c \approx_\Gamma F$ and $\neg b \wedge c \approx_\Gamma F$. Namely, from $b \wedge \neg c \approx_\Gamma F$ we obtain $b \approx_\Gamma b \wedge c$ as follows:

$$\begin{array}{llll} b & \approx_\Gamma & b \wedge \neg F & \text{(A1, C4)} \\ & \approx_\Gamma & b \wedge \neg(b \wedge \neg c) & \text{(assumption above)} \\ & \approx_\Gamma & b \wedge (\neg b \vee c) & \text{(definition } \vee, \text{C2)} \\ & \approx_\Gamma & (b \wedge \neg b) \vee (b \wedge c) & \text{(C3)} \\ & \approx_\Gamma & b \wedge c & \text{(C1, derivation above)} \end{array}$$

Similarly, from $\neg b \wedge c \approx_\Gamma F$ we obtain $c \approx_\Gamma b \wedge c$. Hence, $b \approx_\Gamma c$.

Proposition 8. *$nx \preccurlyeq ny \approx_\Gamma x \preccurlyeq y$ for $n \geq 1$.*

Proof.

$$\begin{array}{lll} & nx \preccurlyeq ny \wedge \neg(x \preccurlyeq y) & \\ \approx_\Gamma & nx \preccurlyeq ny \wedge y + 1 \preccurlyeq x & \text{(C4)} \\ \approx_\Gamma & nx \preccurlyeq ny \wedge y + 1 \preccurlyeq x \wedge ny + n \preccurlyeq nx & \text{(Lem. 5)} \\ \approx_\Gamma & nx \preccurlyeq ny \wedge y + 1 \preccurlyeq x \wedge ny + n \preccurlyeq nx \wedge ny + n \preccurlyeq ny & \text{(A11)} \\ \approx_\Gamma & F & \text{(Lem. 1, A2)} \end{array}$$

$$\begin{array}{lll} & \neg(nx \preccurlyeq ny) \wedge x \preccurlyeq y & \\ \approx_\Gamma & \neg(nx \preccurlyeq ny) \wedge x \preccurlyeq y \wedge nx \preccurlyeq ny & \text{(Lem. 5)} \\ \approx_\Gamma & F & \text{(C1, A2)} \end{array}$$

□

Proposition 9. *$2x \preccurlyeq 2y + 1 \approx_\Gamma 2x \preccurlyeq 2y$.*

Proof. By Proposition 8 it suffices to derive $2x \preccurlyeq 2y+1 \approx_\Gamma x \preccurlyeq y$.

$$\begin{array}{lll}
 & 2x \preccurlyeq 2y+1 \wedge \neg(x \preccurlyeq y) & \\
\approx_\Gamma & 2x \preccurlyeq 2y+1 \wedge y+1 \preccurlyeq x & \text{(C4)} \\
\approx_\Gamma & 2x+1 \preccurlyeq 2y+2 \wedge 2y+2 \preccurlyeq 2x & \text{(A10, Prop. 8)} \\
\approx_\Gamma & 2x+1 \preccurlyeq 2y+2 \wedge 2y+2 \preccurlyeq 2x \wedge 2x+1 \preccurlyeq 2x & \text{(A11)} \\
\approx_\Gamma & F & \text{(A9, 2)}
\end{array}$$

$$\begin{array}{lll}
 & \neg(2x \preccurlyeq 2y+1) \wedge x \preccurlyeq y & \\
\approx_\Gamma & 2y+2 \preccurlyeq 2x \wedge x \preccurlyeq y & \text{(C4)} \\
\approx_\Gamma & y+1 \preccurlyeq x \wedge x \preccurlyeq y & \text{(Prop. 8)} \\
\approx_\Gamma & y+1 \preccurlyeq x \wedge x \preccurlyeq y \wedge y+1 \preccurlyeq y & \text{(A11)} \\
\approx_\Gamma & F & \text{(A9, 2)}
\end{array}$$

□

Theorem 5. *(A1-6,11), (B1-4) and (C1-4) constitute a basis for $\mathcal{C}$.*

Proof. Using (B1), each term of sort natural can be reduced to the form $n_0+n_1x_1+\cdots+n_kx_k$. If two terms of the latter form coincide under all valuations, then they are syntactically equal.

Let b and c be Boolean terms that coincide under all valuations; we prove $b \approx_\Gamma c$. As stated earlier, it suffices to derive $b \wedge \neg c \approx_\Gamma F$ and $\neg b \wedge c \approx_\Gamma F$.

$b \wedge \neg c$ and $\neg b \wedge c$ can be written in disjunctive normal form using (A7,9), (B1) and (C2-4), where each disjunct is of the form

$$s_1 \preccurlyeq t_1 \wedge \cdots \wedge s_n \preccurlyeq t_n \wedge u_1 \wedge \cdots \wedge u_m \wedge \neg v_1 \wedge \cdots \wedge \neg v_\ell$$

with the s_i and t_j of the form $n_0 + n_1x_1 + \cdots + n_kx_k$. It suffices to equate each of the disjuncts above to F.

(1) If $u_i = v_j$ for some i and j, then the disjunct above can be equated to F using (C1) and (A2).
(2) If the u_i and v_j are all distinct, then clearly $s_1 \preccurlyeq t_1 \wedge \cdots \wedge s_n \preccurlyeq t_n$ must be unsatisfiable, so it does not have solutions in the natural numbers. By (A6), conjuncts $0 \preccurlyeq x_i$ can be added for $i = 1, \ldots, k$, so we can even assume that there are no integer solutions. Since the three principles of cutting planes can be derived from the axioms, it follows by Theorem 2(1) that $s_1 \preccurlyeq t_1 \wedge \cdots \wedge s_n \preccurlyeq t_n \approx_\Gamma F$. So the disjunct above can be equated to F with the help of (A2).

□

5. If-then-else

The algebra $\mathcal{D}$ consists of $\mathcal{C}$ extended with the conditional operator $\lhd\rhd : \mathbb{N} \times \mathbb{B} \times \mathbb{N} \to \mathbb{N}$, where $s \lhd b \rhd t$ evaluates to s or t if b is true or false, respectively. Bloom and Tindell [5] and Manes [14] provided finite bases for algebras with an if-then-else construct, but without $\preccurlyeq$. Note that $\max\{x, y\}$ is captured by $x \lhd y \preccurlyeq x \rhd y$; so $\mathcal{D}$ encompasses the max-plus algebra of [1], which does not have a finite basis.

The axioms (D1-4) below are true in the algebra $\mathcal{D} = \langle \mathbb{B}, \mathbb{N}; 0, 1, \neg, \wedge, +, \preccurlyeq, \triangleleft\,\triangleright \rangle$. Let Δ be the equational base consisting of (A1-6,11), (B1-4), (C1-4) and (D1-4). We show that Δ constitutes a basis for $\mathcal{D}$.

$$
\begin{array}{lrcl}
\text{(D1)} & x \triangleleft T \triangleright y & \approx & x \\
\text{(D2)} & x \triangleleft (y \preccurlyeq x) \triangleright y & \approx & y \triangleleft (x \preccurlyeq y) \triangleright x \\
\text{(D3)} & (x \triangleleft u \triangleright y) + z & \approx & (x + z) \triangleleft u \triangleright (y + z) \\
\text{(D4)} & (x \triangleleft u \triangleright y) \preccurlyeq z & \approx & (u \wedge x \preccurlyeq z) \vee (\neg u \wedge y \preccurlyeq z)
\end{array}
$$

$s \approx_\Delta t$ denotes that the equation can be derived from Δ.

As a first step, we will show that $\triangleleft\,\triangleright$ can be eliminated from Boolean terms. To this end we will use the following equations from left to right as rewrite rules:

$$(x \triangleleft u \triangleright y) + z \approx (x + z) \triangleleft u \triangleright (y + z) \tag{1}$$
$$z + (x \triangleleft u \triangleright y) \approx (z + x) \triangleleft u \triangleright (z + y) \tag{2}$$
$$(x \triangleleft u \triangleright y) \preccurlyeq z \approx (u \wedge x \preccurlyeq z) \vee (\neg u \wedge y \preccurlyeq z) \tag{3}$$
$$z \preccurlyeq (x \triangleleft u \triangleright y) \approx (u \wedge z \preccurlyeq x) \vee (\neg u \wedge z \preccurlyeq y) \tag{4}$$

Lemma 6. *Equations (1)–(4) can be derived from Δ.*

Proof. (1) and (3) correspond to (D3) and (D4), respectively. (2) can be derived by (D3) and (B2). (4) is derived as follows:

$$
\begin{array}{lll}
 & z \preccurlyeq (x \triangleleft u \triangleright y) & \\
\approx_\Delta & \neg\neg(z \preccurlyeq (x \triangleleft u \triangleright y)) & \text{(C2)} \\
\approx_\Delta & \neg((x \triangleleft u \triangleright y) + 1 \preccurlyeq z) & \text{(C4)} \\
\approx_\Delta & \neg((x + 1 \triangleleft u \triangleright y + 1) \preccurlyeq z) & \text{(D3)} \\
\approx_\Delta & \neg((u \wedge x + 1 \preccurlyeq z) \vee (\neg u \wedge y + 1 \preccurlyeq z)) & \text{(D4)} \\
\approx_\Delta & (u \wedge z \preccurlyeq x) \vee (\neg u \wedge z \preccurlyeq y) & \text{(Thm. 5)}
\end{array}
$$

Note that the last step involves a true equation without if-then-else. □

Next we show that the rewrite system above doesn't admit infinite rewrite sequences.

Lemma 7. *The rewrite rules (1)-(4) are terminating.*

Proof. This is a standard application of the recursive path order with lexicographic status in term rewriting (see [22] for a recent survey of such termination techniques). The required precedence of function symbols is $\{+\} \succ \{\triangleleft\,\triangleright\}$ and $\{\preccurlyeq\} \succ \{\wedge, \neg\}$. □

Lemma 8. *For every Boolean term s of $\mathcal{D}$ there exists a term t without $\triangleleft\,\triangleright$, such that $s \approx_\Delta t$.*

Proof. By the previous lemmas it follows that $s \approx_\Delta r$, where no rewrite rule (1)-(4) can be applied to the term r. Assume towards a contradiction that r contains $\triangleleft\,\triangleright$. Let r' be the largest subterm of r that starts with $\triangleleft\,\triangleright$. This is a natural, so it has a function symbol above it. The only candidates are $\triangleleft\,\triangleright$ itself (which contradicts maximality of r') or $+$ or $\preccurlyeq$ (which contradicts that (1)-(4) are not applicable). □

Theorem 6. *(A1-6,11), (B1-4), (C1-4) and (D1-4) constitute a basis for $\mathcal{D}$.*

Proof. Let b and c be Boolean terms that coincide under all valuations. By the previous lemma we find b' and c' without $\lhd\ \rhd$, with $b \approx_\Delta b'$ and $c \approx_\Delta c'$. Then b' and c' coincide under all valuations, hence by Theorem 5, $b' \approx_\Gamma c'$. This proves $b \approx_\Delta c$.

Next, let s and t be terms of sort natural that coincide under all valuations. Then both $s \preccurlyeq t \approx T$ and $t \preccurlyeq s \approx T$ are true Boolean equations in $\mathcal{D}$, so by the previous paragraph, $s \preccurlyeq t \approx_\Delta T$ and $t \preccurlyeq s \approx_\Delta T$. We derive $s \approx_\Delta t$ using (D1,2) as follows:

$$s \approx_\Delta s \lhd T \rhd t \approx_\Delta s \lhd (t \preccurlyeq s) \rhd t \approx_\Delta t \lhd (s \preccurlyeq t) \rhd s \approx_\Delta t \lhd T \rhd s \approx_\Delta t.$$

□

Acknowledgements: Jan Heering, Bas Luttik and Lex Schrijver are thanked for useful discussions. Luca Aceto provided relevant pointers to the literature.

References

[1] L. Aceto, Z. Ésik, and A. Ingólfsdóttir. The max-plus algebra of the natural numbers has no finite basis. *Theoretical Computer Science*, 293(1):169–188, 2003.

[2] L. Aceto, W.J. Fokkink, and A. Ingólfsdóttir. A menagerie of non-finitely based process semantics over BPA*: from ready simulation to completed traces. *Mathematical Structures in Computer Science*, 8(3):193–230, 1998.

[3] L. Aceto, W.J. Fokkink, and A. Ingólfsdóttir. 2-nested simulation is not finitely equationally axiomatizable. In A. Ferreira and H. Reichel, eds., *Proceedings 18th Symposium on Theoretical Aspects of Computer Science (STACS'2001)*, Dresden, Germany, Volume 2010 of *Lecture Notes in Computer Science*, pp. 39–50. Springer-Verlag, 2001.

[4] J.A. Bergstra and J. Heering. Which data types have ω-complete initial algebra specifications? *Theoretical Computer Science*, 124(1):149–168, 1994.

[5] S.L. Bloom and R. Tindell. Varieties of "if-then-else". *SIAM Journal on Computing*, 12(4):677–707, 1983.

[6] A. Bockmayr and F. Eisenbrand. Combining logic and optimization in cutting plane theory. In H. Kirchner and C. Ringeissen, eds., *Proceedings 3rd Workshop on Frontiers of Combining Systems (FroCos'00)*, Nancy, France, Volume 1794 of *Lecture Notes in Computer Science*, pp.1–17. Springer-Verlag, 2000

[7] V. Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4:305–337, 1973.

[8] J.H. Conway. *Regular Algebra and Finite Machines*. Mathematics Series (R. Brown and J. De Wet, eds.), Chapman and Hall, 1971.

[9] S. Crvenković, I. Dolinka, and Z. Ésik. The variety of Kleene algebras with conversion is not finitely based. *Theoretical Computer Science*, 230(1-2):235–245, 2000.

[10] R.E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64:275–278, 1958.

[11] R. Gurevič. Equational theory of positive natural numbers with exponentiation is not finitely axiomatizable. *Annals of Pure and Applied Logic*, 49:1–30, 1990.

[12] L. Henkin. The logic of equality. *American Mathematical Monthly*, 84(8):597–612, 1977.

[13] R.C. Lyndon. Identities in two-valued calculi. *Transactions of the American Mathematical Society*, 71:457–465, 1951.

[14] E.G. Manes. Guard modules. *Algebra Universalis*, 21(1):103–110, 1985.

[15] R.N. McKenzie. Tarski's finite basis problem is undecidable. *International Journal of Algebra and Computation*, 6(1):49–104, 1996.

[16] R.N. McKenzie, G. McNulty, and W. Taylor. *Algebras, Varieties, Lattices*. Wadsworth & Brooks/Cole, 1987.

[17] V.L. Murskiĭ. The existence in the three-valued logic of a closed class with a finite basis having no finite complete system of identities. *Doklady Akademii Nauk SSSR*, 163:815–818, 1965. In Russian.

[18] V.L. Murskiĭ. The existence of a finite basis of identities, and other properties of "almost all" finite algebras. *Problemy Kibernetiki*, 30:43–56, 1975. In Russian.

[19] A. Schrijver. On cutting planes. In M. Deza and I.G. Rosenberg, eds., *Proceedings Combinatorics'79 Colloquium*, Montreal, Canada, Volume 9 of *Annals of Discrete Mathematics*, pp. 291–296. North-Holland, 1980.

[20] A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, 1998.

[21] A.J. Wilkie. On exponentiation - a solution to Tarski's high school algebra problem. *Quaderni di Matematica*, 6:107–129, 2000.

[22] H. Zantema. Termination. In Terese, ed., *Term Rewring Systems*, Volume 55 of *Cambridge Tracts in Theoretical Computer Science*, Chapter 6, pp. 181–259. Cambridge University Press, 2003.

CWI, Department of Software Engineering, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

E-mail address: wan@cwi.nl

URL: http://homepages.cwi.nl/~wan/

CWI, Department of Software Engineering, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

E-mail address: vdpol@cwi.nl

URL: http://homepages.cwi.nl/~vdpol/

Rutgers, The State University of New Jersey, Department of Mathematics, 110 Frelinghuysen Rd, Piscataway, NJ 08854-8019

E-mail address: sujith@math.rutgers.edu

URL: http://www.math.rutgers.edu/~sujith/