Complex algebras of natural numbers

Ivo Düntsch Ian Pratt-Hartmann

Department of Computer Science
Brock University
St Catharines, Canada

School of Computer Science
Manchester University
Manchester, UK

Overview

1. Definitions of algebras of arithmetic circuits.
2. Circuit definable sets and functions.
3. Some algebraic properties.
4. Decidability questions.

The structures

$$\begin{array}{ll} \mathbb{N} := \langle \omega, +, 0, \cdot, 1 \rangle, & \mathfrak{Cm}(\mathbb{N}) := \langle 2^\omega, \cup, \cap, \emptyset, \omega, +, \{0\}, \bullet, \{1\} \rangle \\ \mathbb{N}^+ = \langle \omega, +, 0 \rangle, & \mathfrak{Cm}(\mathbb{N})^+ := \langle 2^\omega, \cup, \cap, \emptyset, \omega, +, \{0\} \rangle \\ \mathbb{N}^\cdot = \langle \omega, \cdot, 1 \rangle & \mathfrak{Cm}(\mathbb{N})^\bullet := \langle 2^\omega, \cup, \cap, \emptyset, \omega, \bullet, \{1\} \rangle \end{array}$$

$+$	$a + b$	$= \{n + m : n \in a,\ m \in b\}.$
$\cdot$	$a \bullet b$	$= \{n \cdot m : n \in a,\ m \in b\}.$
$\geq$	$\uparrow a$	$= \{k : (\exists n)[n \in a \text{ and } n \leq k\}.$
$\leq$	$\downarrow a$	$= \{k : (\exists n)[n \in a \text{ and } k \leq n\}.$

If $\mathfrak{A}$ is an atomic Boolean algebra with operators, we set

$$\mathfrak{A}_0 := \text{Subalgebra of } \mathfrak{A} \text{ generated by the constants,}$$

$$\mathfrak{A}_1 := \text{Subalgebra of } \mathfrak{A} \text{ generated by the atoms.}$$

The structures

$$\begin{array}{ll} \mathbb{N} := \langle \omega, +, 0, \cdot, 1 \rangle, & \mathfrak{Cm}(\mathbb{N}) := \langle 2^\omega, \cup, \cap, \emptyset, \omega, +, \{0\}, \bullet, \{1\} \rangle \\ \mathbb{N}^+ = \langle \omega, +, 0 \rangle, & \mathfrak{Cm}(\mathbb{N})^+ := \langle 2^\omega, \cup, \cap, \emptyset, \omega, +, \{0\} \rangle \\ \mathbb{N}^\cdot = \langle \omega, \cdot, 1 \rangle & \mathfrak{Cm}(\mathbb{N})^\bullet := \langle 2^\omega, \cup, \cap, \emptyset, \omega, \bullet, \{1\} \rangle \end{array}$$

$+$	$a + b$	$= \{n + m : n \in a, \ m \in b\}.$
$\cdot$	$a \bullet b$	$= \{n \cdot m : n \in a, \ m \in b\}.$
$\geq$	$\uparrow a$	$= \{k : (\exists n)[n \in a \text{ and } n \leq k\}.$
$\leq$	$\downarrow a$	$= \{k : (\exists n)[n \in a \text{ and } k \leq n\}.$

If $\mathfrak{A}$ is an atomic Boolean algebra with operators, we set

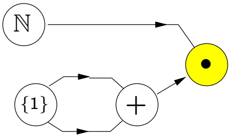
$$\mathfrak{A}_0 := \text{Subalgebra of } \mathfrak{A} \text{ generated by the constants,}$$

$$\mathfrak{A}_1 := \text{Subalgebra of } \mathfrak{A} \text{ generated by the atoms.}$$

The elements of $\mathfrak{Cm}(\mathbb{N})_0$ are called *arithmetic circuits* (McKenzie, Wagner, 2003,2007).

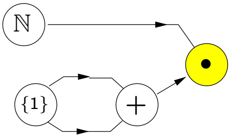
Arithmetic circuits can be displayed graphically

- $(\{1\} + \{1\}) \bullet \omega$, can be depicted as

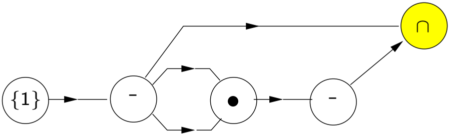


Arithmetic circuits can be displayed graphically

- $(\{1\} + \{1\}) \bullet \omega$, can be depicted as



- $\overline{\{1\}} \cap \overline{(\overline{\{1\}} \bullet \overline{\{1\}})}$ can be depicted as



- Some well-known mathematical conjectures can be 'expressed' in terms of arithmetic circuits.
- Consider the circuit

$$\tau_{\mathrm{g}} = \tau_{\mathrm{e}} \cap \overline{(\{0\} \cup (\{1\} + \{1\}) \cup (\tau_{\mathrm{p}} + \tau_{\mathrm{p}}))}$$

  where τ_{e} is the circuit defining the even numbers, and τ_{p} the circuit defining the primes.

- Some well-known mathematical conjectures can be ‘expressed’ in terms of arithmetic circuits.
- Consider the circuit

$$\tau_{\mathrm{g}} = \tau_{\mathrm{e}} \cap \overline{(\{0\} \cup (\{1\} + \{1\}) \cup (\tau_{\mathrm{p}} + \tau_{\mathrm{p}}))}$$

  where τ_{e} is the circuit defining the even numbers, and τ_{p} the circuit defining the primes.
- The set τ_{g} is empty if and only if Goldbach’s conjecture is true.

Functions

- Any circuit τ featuring variables $x_1, \ldots, x_k$ defines a function $\tau(x_1, \ldots x_k) : (2^\omega)^k \longrightarrow 2^\omega$ in the obvious way.
- Some circuit–definable functions:
  - The circuit $\tau_{\mathrm{u}}(x) = x + \omega$ defines the 'up'-function:

$$\uparrow x = \{n \in \omega : (\exists m \in x), m \leq n\}$$

Functions

- Any circuit τ featuring variables $x_1, \ldots, x_k$ defines a function $\tau(x_1, \ldots x_k) : (2^\omega)^k \to 2^\omega$ in the obvious way.
- Some circuit–definable functions:
  - The circuit $\tau_{\mathrm{u}}(x) = x + \omega$ defines the 'up'-function:

$$\uparrow x = \{n \in \omega : (\exists m \in x), m \leq n\}$$

  - The circuit $\tau_{\mathrm{d}}(x) = (\{0\} \bullet x) + \omega$ defines the discriminator function

$$\tau_d(x) = \begin{cases} \emptyset, & \text{if } x = \emptyset, \\ \omega, & \text{otherwise.} \end{cases}$$

Functions

- Any circuit τ featuring variables $x_1, \ldots, x_k$ defines a function $\tau(x_1, \ldots x_k) : (2^\omega)^k \to 2^\omega$ in the obvious way.
- Some circuit–definable functions:
  - The circuit $\tau_{\mathrm{u}}(x) = x + \omega$ defines the 'up'-function:

$$\uparrow x = \{n \in \omega : (\exists m \in x), m \leq n\}$$

  - The circuit $\tau_{\mathrm{d}}(x) = (\{0\} \bullet x) + \omega$ defines the discriminator function

$$\tau_d(x) = \begin{cases} \emptyset, & \text{if } x = \emptyset, \\ \omega, & \text{otherwise.} \end{cases}$$

  - The circuit $\tau_{\min}(x) = (\overline{(x + \omega)} + \{1\}) \cap x$ defines the minimum function for non–empty sets.

Some functions not definable by circuits

$$\downarrow s = \{n \in \omega : (\exists m \in s) n \leq m\}$$

Some functions not definable by circuits

$$\downarrow s = \{n \in \omega : (\exists m \in s) n \leq m\}$$

Some functions not definable by circuits

$$\downarrow s = \{n \in \omega : (\exists m \in s) n \leq m\}$$

Some functions not definable by circuits

$$\downarrow s = \{n \in \omega : (\exists m \in s) n \leq m\}$$

$$s \dot{-} t = \{k \in \omega : (\exists n, m \in \omega)[n \in s,\ m \in t,\ k = n - m]\}$$

$$F_{\max}(s) = \{\max(s)\} \quad \text{for finite, non-empty } s$$

$$F_{\mathrm{fin}}(s) = \begin{cases} \omega & \text{if } s \text{ is finite} \\ \emptyset & \text{otherwise} \end{cases}$$

Σs if s is finite

$|s|$ if s is finite.

Sets of formulas

Suppose that K is a class of algebras of the same type $\mathcal{O}$. We consider the following sets of formulas in the language of $\mathcal{O}$ (plus equality):

1. The *first-order theory* **FO** K *of* K: The set of first-order formulas in the language $\mathcal{O}$ true in all algebras in K.
2. The *equational theory* **Eq** K *of* K: The set of formulas in the language of the forms $\tau = \sigma$ whose universal closures are true in K.
3. The *satisfiable equations* **EqSat** K *of* K: The set of formulas of the forms $\tau = \sigma$ whose existential closures are true in each member of K.

Algebras and equations

- $\mathfrak{Cm}(\mathbb{N}^{+})_0 \cong \mathfrak{Cm}(\mathbb{N}^{\bullet})_0$, and their universe is the collection of finite or co–finite subsets of ω.

Algebras and equations

- $\mathfrak{Cm}(\mathbb{N}^+)_0 \cong \mathfrak{Cm}(\mathbb{N}^\bullet)_0$, and their universe is the collection of finite or co–finite subsets of ω.
- The congruences of $\mathfrak{Cm}(\mathbb{N}^+)$ form a chain of type $1 + \omega^*$.
- **Var** $\mathfrak{Cm}(\mathbb{N}^+)$ is generated by countably many finite finitely based subdirectly irreducible algebras.

Algebras and equations

- $\mathfrak{Cm}(\mathbb{N}^+)_0 \cong \mathfrak{Cm}(\mathbb{N}^\bullet)_0$, and their universe is the collection of finite or co–finite subsets of ω.
- The congruences of $\mathfrak{Cm}(\mathbb{N}^+)$ form a chain of type $1 + \omega^*$.
- **Var** $\mathfrak{Cm}(\mathbb{N}^+)$ is generated by countably many finite finitely based subdirectly irreducible algebras.
- **Eq** $\mathfrak{Cm}(\mathbb{N}^+)_0 =$ **Eq** $\mathfrak{Cm}(\mathbb{N}^+)$.
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})_0 \neq$ **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$.
- **FO** $\mathfrak{Cm}(\mathbb{N}^+)_0 \neq$ **FO** $\mathfrak{Cm}(\mathbb{N}^+)$.

Decidability questions 1

Membership problem: Given an arithmetic circuit τ and a number m, determine whether $m \in \tau$.

Emptiness problem: Given an arithmetic circuit τ, determine whether $\tau = \emptyset$.

Satisfiability problem: Given an n–ary term function $\tau(x_1, \ldots, x_n)$ and some $k \in \omega$, determine whether there are $k_1, \ldots, k_n \in \omega$ such that $k \in \tau(k_1, \ldots, k_n)$.

- Problems 1 and 2 are obviously computably equivalent: if one is decidable, so is the other. It is not known whether any of these problems is decidable.

- Variable-free arithmetic circuits without the $\bullet$-gate are called *integer expressions*.
- The membership and non-emptiness problems for integer expressions are $\mathrm{PS}\textsc{pace}$-complete (Stockmeyer and Meyer 1973).
- Complexity-theortic results for various collections of gates can be found in (McKenzie and Wagner 2003, 2007), (Yang 2000) (Glaßer *et al.* 2007, 2007)
- For results on equations involving integer expressions, see (Jeż and Okhotin 2008, 2008).

Decidability questions 2

- **EqSat** $\mathfrak{Cm}(\mathbb{N}^+)$ is co-r.e.-hard.

Decidability questions 2

- **EqSat** $\mathfrak{Cm}(\mathbb{N}^+)$ is co-r.e.-hard.
  Is **EqSat** $\mathfrak{Cm}(\mathbb{N}^+)$ co-r.e.?

Decidability questions 2

- **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ is co-r.e.-hard.
  Is **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ co-r.e.?
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ is r.e.-hard.

Decidability questions 2

- **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ is co-r.e.-hard.
  Is **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ co-r.e.?
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ is r.e.-hard.
  Is **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ r.e.?

Decidability questions 2

- **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ is co-r.e.-hard.
  Is **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ co-r.e.?
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ is r.e.-hard.
  Is **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ r.e.?
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+})$ is co–re.

Decidability questions 2

- **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ is co-r.e.-hard.
  Is **EqSat** $\mathfrak{Cm}(\mathbb{N}^{+})$ co-r.e.?
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ is r.e.-hard.
  Is **Eq** $\mathfrak{Cm}(\mathbb{N}^{+,d})$ r.e.?
- **Eq** $\mathfrak{Cm}(\mathbb{N}^{+})$ is co–re.
  Is **Eq** $\mathfrak{Cm}(\mathbb{N}^{+})$ r.e.?

Thank you
Dziękuję
Asante
Danke
Merci

- The recognition complexity for every *fixed* circuit-definable set is relatively low.

Theorem

Every circuit-definable set is in the bounded arithmetic hierarchy, BA (and hence its characteristic function is in $\mathcal{E}^0_*$).

- Hence, every circuit-definable set is certainly:
  - in the polynomial hierarchy, PH;
  - in $\textsc{DSpace}(n) = \mathcal{E}^2_*$.
- All circuit-definable sets are certainly context-sensitive. However, the set of primes, which is circuit-definable, is not context-free (Hartmanis and Shank 1968).
- Theorem 1 notwithstanding, no nice examples of non-circuit-definable sets are known!

- First main result: functions from $\mathbb{N}$ to $\mathbb{N}$ having (roughly speaking) infinite range and sublinear growth are not circuit-definable:

Theorem

Let $f : \mathbb{N} \to \mathbb{N}$ be a function. If the set

$$\{f(n) : n \in \mathbb{N},\ f(n) < n\}$$

is infinite, then f is not circuit-definable.

- Second main result: functions from $2^{\mathbb{N}}$ to $2^{\mathbb{N}}$ which (roughly speaking) have finite range and fail to converge on certain 'sparse' chains under inclusion are not circuit-definable.

Definition

Let s be a finite, non-empty set of numbers, t a set of numbers, and m a number. We write $s \sqsubseteq_m t$ if $m \geq \max(s)$ and $s = t \cap \{i \mid i \leq m\}$.

Theorem

Let $F : 2^{\mathbb{N}} \to 2^{\mathbb{N}}$ be a function with finite range. And suppose that, for all finite, non-empty $s \subseteq \mathbb{N}$ and all $m \geq \max(s)$, there exists $t \subseteq \mathbb{N}$ for which $s \sqsubseteq_m t$ and $F(t) \neq F(s)$. Then F is not circuit-definable.