Linear arithmetic theories:
automata-based procedures

Christoph Haase Alessio Mansutti

ESSLLI 2023

Today's lecture

Automata-based decision procedures for arithmetic theories:

- A problem of Sloane
- Finite-state automata for Presburger arithmetic
- Büchi arithmetic
- Tool presentation: WALNUT
- Sëmenov arithmetic

A problem of Sloane

The connoisseur of number sequences

©John Smock for Quanta Magazine

Neil Sloane (*1939)

The On-Line Encyclopedia of Integer Sequences (OEIS)

The OEIS is supported by [*the many generous donors to the OEIS Foundation*].

THE ON–LINE ENCYCLOPEDIA
OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane

The On-Line Encyclopedia of Integer Sequences® (OEIS®)

Enter a sequence, word, or sequence number:

0, 1, 3, 4, 6, 7, 9, 11, 13, 15, 17, 19

Neil Sloan on Numberphile

Problems with Powers of Two - Numberphile

Numberphile
4.21M subscribers

Subscribed

8.9K

Share

Thanks

Problems with powers of two

Given a set of integers $S \subseteq \mathbb{Z}$, denote by $b(S)$ the number of powers of two that can be obtained as the sum of two elements of S.

Examples:

- $S = \{1, 3\}$: $b(S) = 1$
- $S = \{-1, 3, 5\}$: $b(S) = 3$
- $S = \{-3, -1, 3, 5\}$: $b(S) = 4$

Problems with powers of two

Denote by $a(n)$ the largest value of $b(S)$ that can be achieved for a set $S \subseteq \mathbb{Z}$ with n elements.

n	1	2	3	4	5	6	7	8	9	10	11	12
$a(n)$	0	1	3	4	6	7	9	11	13	15	17	19

- Largest known value: $a(18) = 34$

OEIS A352178

The OEIS is supported by the many generous donors to the OEIS Foundation.

THE ON-LINE ENCYCLOPEDIA OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane

Search Hints

(Greetings from The On-Line Encyclopedia of Integer Sequences!)

A352178 Let S = {t_1, t_2, ..., t_n} be a set of n distinct integers and consider the sums t_i + t_j (i<j); a(n) is the maximum number of such sums that are powers of 2, over all choices for S. 4

0, 1, 3, 4, 6, 7, 9, 11, 13, 15, 17, 19, 21, 24, 26, 29, 31, 34 (list; graph; refs; listen; history; text; internal format)

OFFSET 1,3

COMMENTS

```
Given distinct integers t_1, ..., t_n, form a graph G with n vertices labeled by
  the t_i, and with an edge from t_i to t_j, labeled t_i + t_j, whenever t_i + t_j
  is a power of 2.
See the Pratt link for the best lower bounds known, and examples of sets achieving
  these bounds, for 1 <= n <= 100. - N. J. A. Sloane, Sep 26 2022
The following remarkable theorem is due to M. S. Smith (email of Mar 06 2022).
Theorem: G contains no 4-cycles.
Proof. Suppose the contrary, and assume the vertices t_1, t_2, t_3, t_4 form a
  4-cycle, with edges labeled b_1 = t_1+t_2, b_2 = t_2+t_3, b_3 = t_3+t_4, b_4 =
  t_4+t_1. The b_i are powers of 2.
Since the t_i are distinct, b_1 != b_4, b_2 != b_1, b_3 != b_2, and b_4 != b_3.
We also have
```

Open problems and challenges

- How does A352178 continue? Not known, but lower and upper bounds are known.
- Is it possible to continue A352178, at least in theory? Iterating over all n-element subsets of $\mathbb{Z}$ is not possible.
- How do different powers relate to each other? Is there some structure in $a(n)$ if base is variable instead of two?

A logicians view on the problem

To determine whether $a(n) \geq k$:

- Find integers n integers:

$$\exists z_1, z_2, \ldots, z_n$$

- For every pair $i < j$ an indicator variable $x_{i,j} \in \{0,1\}$ assigning 1 to $x_{i,j}$ exactly when $z_i + z_j$ is a power of two:

$$\exists x_{1,2}, x_{1,3}, \ldots, x_{n-1,n} P_2(z_1 + z_2) \rightarrow x_{1,2} = 1 \wedge \\ \wedge \neg P_2(z_1 + z_2) \rightarrow x_{1,2} = 0 \wedge \cdots \wedge \neg P_2(x_{n,n-1}) \rightarrow x_{n,n-1} = 0$$

- The sum of all indicator variables is at least k:

$$x_{1,2} + x_{1,3} + \cdots + x_{n-1,n} \geq k$$

Finite-state automata for Presburger arithmetic

Finite-state automata

For most parts of this lecture, Presburger arithmetic is the first-order theory of $\langle \mathbb{N}, 0, 1, +, \leq \rangle$

Finite-state automata

For most parts of this lecture, Presburger arithmetic is the first-order theory of $\langle \mathbb{N}, 0, 1, +, \leq \rangle$

A deterministic finite-state automaton is a tuple $M = (Q, \Sigma, \delta, q_i, F)$, where

- Q is a finite state of states,
- Σ is a finite alphabet,
- $\delta \colon Q \times \Sigma \to Q$ is the transition function,
- $q_i \in Q$ is the initial state, and
- $F \subseteq Q$ is the set of final states.

Finite-state automata

For most parts of this lecture, Presburger arithmetic is the first-order theory of $\langle \mathbb{N}, 0, 1, +, \leq \rangle$

A deterministic finite-state automaton is a tuple $M = (Q, \Sigma, \delta, q_i, F)$, where

- Q is a finite state of states,
- Σ is a finite alphabet,
- $\delta \colon Q \times \Sigma \to Q$ is the transition function,
- $q_i \in Q$ is the initial state, and
- $F \subseteq Q$ is the set of final states.

Goal: construct DFA whose language encodes all solutions of a Presburger formula

Encoding numbers as strings

- Unique mapping between strings in $\{0,1\}^n$ and natural numbers in $\{0,\ldots,2^n-1\}$
- Given $w = b_{n-1}\cdots b_1 b_0 \in \{0,1\}^{n+1}$, in MSDF encoding, w represents

$$\sum_{i=0}^{n-1} 2^i b_i$$

- So 111 1110 encodes 126

Encoding tuples of numbers as strings

Problem: Can only encode single numbers using alphabet $\{0, 1\}$

Encoding tuples of numbers as strings

Problem: Can only encode single numbers using alphabet $\{0, 1\}$

Solution: Alphabet $\{0, 1\}^d$ can encode d numbers simultaneously

Encoding tuples of numbers as strings

Problem: Can only encode single numbers using alphabet $\{0, 1\}$

Solution: Alphabet $\{0, 1\}^d$ can encode d numbers simultaneously

Example

For $d = 2$, 126 and 5 can simultaneously be encoded as

$$\begin{array}{|c|c|c|c|c|c|c|} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}$$

Encoding a linear equation

Given linear equation $\boldsymbol{a} \cdot \boldsymbol{x} = c$, define DFA accepting all solutions:

$M = (Q, \{0,1\}^d, \delta, q_i, F)$ defined such that

- $Q = \mathbb{Z} \cup \{\perp\}$,
- $q_i = 0$, and
- $\delta(z, \boldsymbol{u}) = 2z + \boldsymbol{a} \cdot \boldsymbol{u}$ for all $z \in \mathbb{Z}$,
- $\delta(\perp, \boldsymbol{u}) = \perp$ for all $\boldsymbol{u} \in \{0,1\}^d$,
- $F = \{c\}$.

Encoding a linear equation

Given linear equation $\boldsymbol{a} \cdot \boldsymbol{x} = c$, define DFA accepting all solutions:

$M = (Q, \{0,1\}^d, \delta, q_i, F)$ defined such that

- $Q = \mathbb{Z} \cup \{\perp\}$,
- $q_i = 0$, and
- $\delta(z, \boldsymbol{u}) = 2z + \boldsymbol{a} \cdot \boldsymbol{u}$ for all $z \in \mathbb{Z}$,
- $\delta(\perp, \boldsymbol{u}) = \perp$ for all $\boldsymbol{u} \in \{0,1\}^d$,
- $F = \{c\}$.

After reading $\boldsymbol{u}_{n-1} \cdots \boldsymbol{u}_0$, state of automaton equals

$$\sum_{i=0}^{n-1} 2^i \boldsymbol{a} \cdot \boldsymbol{u}_i$$

Encoding a linear equation

Given linear equation $\boldsymbol{a} \cdot \boldsymbol{x} = c$, define DFA accepting all solutions:

$M = (Q, \{0,1\}^d, \delta, q_i, F)$ defined such that

- $Q = \mathbb{Z} \cup \{\bot\}$,
- $q_i = 0$, and
- $\delta(z, \boldsymbol{u}) = 2z + \boldsymbol{a} \cdot \boldsymbol{u}$ for all $z \in \mathbb{Z}$,
- $\delta(\bot, \boldsymbol{u}) = \bot$ for all $\boldsymbol{u} \in \{0,1\}^d$,
- $F = \{c\}$.

After reading $\boldsymbol{u}_{n-1} \cdots \boldsymbol{u}_0$, state of automaton equals

$$\sum_{i=0}^{n-1} 2^i \boldsymbol{a} \cdot \boldsymbol{u}_i$$

Problem: State space infinite

Encoding a linear equation

Given linear equation $\boldsymbol{a} \cdot \boldsymbol{x} = c$, define DFA accepting all solutions:

$M = (Q, \{0,1\}^d, \delta, q_i, F)$ defined such that

- $Q = \mathbb{Z} \cup \{\bot\}$,
- $q_i = 0$, and
- $\delta(z, \boldsymbol{u}) = 2z + \boldsymbol{a} \cdot \boldsymbol{u}$ for all $z \in \mathbb{Z}$,
- $\delta(\bot, \boldsymbol{u}) = \bot$ for all $\boldsymbol{u} \in \{0,1\}^d$,
- $F = \{c\}$.

After reading $\boldsymbol{u}_{n-1} \cdots \boldsymbol{u}_0$, state of automaton equals

$$\sum_{i=0}^{n-1} 2^i \boldsymbol{a} \cdot \boldsymbol{u}_i$$

Problem: State space infinite

Solution: Observe $|z| > \|\boldsymbol{a}\|_1$ implies $2z + \boldsymbol{a} \cdot \boldsymbol{u} > |z|$

Deciding full Presburger arithmetic

Deciding arbitrary formulas via operations on NFA:

- Conjunction: intersection of two NFA
- Disjunction: union of two NFA
- Existential quantification: apply homomorphism to NFA
- Universal quantification: $\forall x : \Phi(x) \equiv \neg \exists x : \neg \Phi(x)$

Deciding full Presburger arithmetic

Deciding arbitrary formulas via operations on NFA:

- Conjunction: intersection of two NFA
- Disjunction: union of two NFA
- Existential quantification: apply homomorphism to NFA
- Universal quantification: $\forall x : \Phi(x) \equiv \neg\exists x : \neg\Phi(x)$

Remarks:

- can be shown to run in triply exponential time [Durand-Gasselin & Habermehl, 2010]
- projection easy, complementation "difficult"
- generalizes to any base
- Cobham-Semënov: if $S \subseteq \mathbb{N}^d$ recognizable in co-prime bases k and l then S definable in Presburger arithmetic
- Can be adapted to work for $\mathbb{R}$ instead of $\mathbb{Z}$ (but not $\mathbb{Q}$)

Büchi arithmetic

For any fixed $p > 1$, extend Presburger arithmetic with binary predicate V_p such that

$$\mathcal{A} \models V_p(x, y) \iff \text{largest power of } p \text{ dividing } \mathcal{A}(y) \text{ is } \mathcal{A}(x)$$

Büchi arithmetic

For any fixed $p > 1$, extend Presburger arithmetic with binary predicate V_p such that

$$\mathcal{A} \models V_p(x, y) \iff \text{largest power of } p \text{ dividing } \mathcal{A}(y) \text{ is } \mathcal{A}(x)$$

Example: $V_2(8, 40)$ holds, but $V_2(8, 48)$ does not hold

Büchi arithmetic

For any fixed $p > 1$, extend Presburger arithmetic with binary predicate V_p such that

$$\mathcal{A} \models V_p(x, y) \iff \text{largest power of } p \text{ dividing } \mathcal{A}(y) \text{ is } \mathcal{A}(x)$$

Example: $V_2(8, 40)$ holds, but $V_2(8, 48)$ does not hold

Facts:

- Büchi, 1960: decidable using automata theoretic-approach
- Define power-of-p predicate as $P_p(x) := V_p(x, x)$
- Existential fragment has solutions of super-polynomial bit length
- $S \subseteq \mathbb{N}^d$ p-recognizable (regular) iff S is definable in Büchi arithmetic with predicate V_p, e.g. [Bruyère et al., 1994]

Büchi arithmetic and quantifier elimination

- Yesterday we saw that any quantified formula $\Phi(\boldsymbol{x})$ of Presburger arithmetic is equivalent to some $\exists \boldsymbol{y} : \Psi(\boldsymbol{x}, \boldsymbol{y})$ with Ψ quantifier free
- Presburger arithmetic is model complete

Büchi arithmetic and quantifier elimination

- Yesterday we saw that any quantified formula $\Phi(\boldsymbol{x})$ of Presburger arithmetic is equivalent to some $\exists \boldsymbol{y} : \Psi(\boldsymbol{x}, \boldsymbol{y})$ with Ψ quantifier free
- Presburger arithmetic is model complete

Theorem (H., Rozycki, 2021)

Büchi arithmetic is not model complete.

Use density argument: For $M \subseteq \mathbb{N}$, define $d_M(n) := \#\{2^{n-1}, \ldots, 2^n - 1\}$.

Büchi arithmetic and quantifier elimination

- Yesterday we saw that any quantified formula $\Phi(\boldsymbol{x})$ of Presburger arithmetic is equivalent to some $\exists \boldsymbol{y} : \Psi(\boldsymbol{x}, \boldsymbol{y})$ with Ψ quantifier free
- Presburger arithmetic is model complete

Theorem (H., Rozycki, 2021)

Büchi arithmetic is not model complete.

Use density argument: For $M \subseteq \mathbb{N}$, define $d_M(n) := \#\{2^{n-1}, \ldots, 2^n - 1\}$.

- For $M \subseteq \mathbb{N}$ the set of solutions of an existential formula of Büchi arithmetic $\Phi(x)$, have either
  - $d_M(n) \geq c \cdot 2^n$ for some constant $c > 0$ and infinitely many $n \in \mathbb{N}$
  - $d_M(n) = O(n^c)$ for some $c > 0$
- For $N \subseteq \mathbb{N}$ the set of numbers whose binary encoding is in $\{01, 10\}^*$, have $d_N(n) = \Theta(2^{n/2})$
- N is definable in Büchi arithmetic, but not by an existential formula

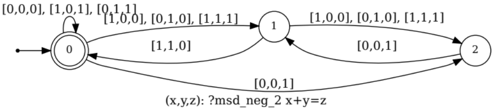
Encoding negative numbers

Recall that Sloane's problem requires quantifying over integers. Can use either:

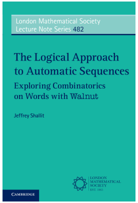
- Twos complement (first digit indicates whether number is negative)
- Negative bases, e.g., in base -2 we have:

$$23 = 1 \cdot (-2)^0 + 1 \cdot (-2)^1 + 0 \cdot (-2)^2 + 1 \cdot (-2)^3 + 0 \cdot (-2)^4 + 1 \cdot (-2)^5 + 1 \cdot (-2)^6$$

- Gadgets become more difficult, e.g., addition:

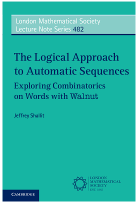


Tool presentation WALNUT



- Implements automata-based decision procedure for Büchi arithmetic
- Written by Hamoon Mousavi under guidance of Jeffrey Shallit
- Used to automatically prove dozens of statements, primarily in word combinatorics

Tool presentation Walnut



- Implements automata-based decision procedure for Büchi arithmetic
- Written by Hamoon Mousavi under guidance of Jeffrey Shallit
- Used to automatically prove dozens of statements, primarily in word combinatorics

```
eval odd_even "?msd_neg_2 Ax Ey ((x = 2*y | x = 2*y+1))";
eval power_congruence "?msd_2 Ey ($power2(x) & x - 5*y = 1)";
```

Automatic structure

In more general terms, Büchi arithmetic is an automatic structure. A relational structure $\langle \mathbb{D}, R_1, \ldots, R_k \rangle$ is automatic if (simplified)

- $\mathbb{D}$ is isomorphic to some regular language $L \subseteq \Sigma^*$
- Every R_i of arity n is isomorphic to some regular language $L_i \subseteq (\Sigma^n)^*$

Automatic structure

In more general terms, Büchi arithmetic is an automatic structure. A relational structure $\langle \mathbb{D}, R_1, \ldots, R_k \rangle$ is automatic if (simplified)

- $\mathbb{D}$ is isomorphic to some regular language $L \subseteq \Sigma^*$
- Every R_i of arity n is isomorphic to some regular language $L_i \subseteq (\Sigma^n)^*$

Some basic properties:

- Every automatic structure is decidable [Hodgson 1982; Khoussainov and Nerode 1995; Blumensath and Grädel, 2000]
- Constant growth lemma: If function f is automatic then there is $c \geq 0$ s.t.

$$|f(x_1, \ldots, x_n)| \leq |x_1| + \cdots + |x_n| + c$$

- Doubly-exponential blow-up when eliminating single universal quantifier in general unavoidable [H., Piorkowski 2023]

Beyond automatic structures: Semënov arithmetic

First-order theory of $\langle \mathbb{N}, 0, 1, +, 2^{(\cdot)} \rangle$:

- Decidable via automata-theoretic methods [Semënov 1980]
- Has quantifier elimination [Cherlin and Point 1986; Benedikt, Chistikov and Mansutti, 2023]
- Not regular since it violates constant growth lemma

Beyond automatic structures: Semënov arithmetic

First-order theory of $\langle \mathbb{N}, 0, 1, +, 2^{(\cdot)} \rangle$:

- Decidable via automata-theoretic methods [Semënov 1980]
- Has quantifier elimination [Cherlin and Point 1986; Benedikt, Chistikov and Mansutti, 2023]
- Not regular since it violates constant growth lemma

Requires a different notion of automaticity, affine vector addition systems with states:

- Equip finite-state automata with finite number of counters over natural numbers
- When transition is taken, automaton can apply affine function on every counter; blocks if result is negative
- Accept when in final state and counter values lie in quantifier-free Presburger formula

Semënov arithmetic

- Reachability in affine VASS is undecidable
- Affine VASS arising from formulas of existential Semënov arithmetic have strong structural resrictions

Semënov arithmetic

- Reachability in affine VASS is undecidable
- Affine VASS arising from formulas of existential Semënov arithmetic have strong structural resrictions

Theorem (Draghici, H. and Manea 2023)

Exisential Semënov arithmetic equipped with the Büchi V_2-predicate is decidable in EXPSPACE.

Agenda

Friday Geometric decision procedures, VC dimension of linear arithmetic theoires