A strong version of Cobham's theorem

Philipp Hieronymi

One World Numeration Seminar, September 2021

UNIVERSITÄT BONN

Universität Bonn

Mathematisches Institut

Cobham's theorem (1969). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ is both k-recognizable and ℓ-recognizable if and only if it is ultimately periodic.

Cobham's theorem (1969). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ is both k-recognizable and ℓ-recognizable if and only if it is ultimately periodic.

A set $X \subseteq \mathbb{N}$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Cobham's theorem (1969). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ is both k-recognizable and ℓ-recognizable if and only if it is ultimately periodic.

A set $X \subseteq \mathbb{N}$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Examples.

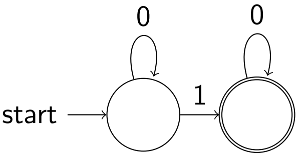
- $k^{\mathbb{N}}$ is k-recognizable,

Cobham's theorem (1969). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ is both k-recognizable and ℓ-recognizable if and only if it is ultimately periodic.

A set $X \subseteq \mathbb{N}$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Examples.

- $k^{\mathbb{N}}$ is k-recognizable,

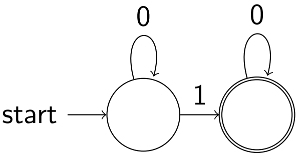


Cobham's theorem (1969). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ is both k-recognizable and ℓ-recognizable if and only if it is ultimately periodic.

A set $X \subseteq \mathbb{N}$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Examples.

- $k^{\mathbb{N}}$ is k-recognizable,
- $\{n \in \mathbb{N} \ : \ s_2(n) \text{ is even }\}$ is 2-recognizable, where $s_2(n)$ is the binary digit sum - **Thue-Morse set**.

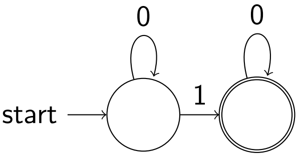


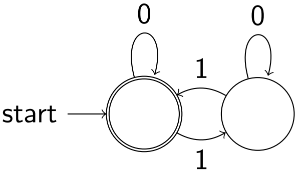
Cobham's theorem (1969). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ is both k-recognizable and ℓ-recognizable if and only if it is ultimately periodic.

A set $X \subseteq \mathbb{N}$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Examples.

- $k^{\mathbb{N}}$ is k-recognizable,
- $\{n \in \mathbb{N} \ : \ s_2(n) \text{ is even }\}$ is 2-recognizable, where $s_2(n)$ is the binary digit sum - **Thue-Morse set**.





Let $n \geq 1$. A base k representation of a tuple $(x_1, \ldots, x_n) \in \mathbb{N}^n$ is a word over the alphabet $\{0, 1, \ldots, k-1\}^n$. For example, a base 2 representation of $\begin{bmatrix} 6 \\ 3 \end{bmatrix}$ is $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Let $n \geq 1$. A base k representation of a tuple $(x_1, \ldots, x_n) \in \mathbb{N}^n$ is a word over the alphabet $\{0, 1, \ldots, k-1\}^n$. For example, a base 2 representation of $\begin{bmatrix} 6 \\ 3 \end{bmatrix}$ is $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

A set $X \subseteq \mathbb{N}^n$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Let $n \geq 1$. A base k representation of a tuple $(x_1, \ldots, x_n) \in \mathbb{N}^n$ is a word over the alphabet $\{0, 1, \ldots, k-1\}^n$. For example, a base 2 representation of $\begin{bmatrix} 6 \\ 3 \end{bmatrix}$ is $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

A set $X \subseteq \mathbb{N}^n$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Semenov (1977). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. A set $X \subseteq \mathbb{N}^n$ is both k-recognizable and ℓ-recognizable if and only if it is semilinear.

Let $n \geq 1$. A base k representation of a tuple $(x_1, \ldots, x_n) \in \mathbb{N}^n$ is a word over the alphabet $\{0, 1, \ldots, k-1\}^n$. For example, a base 2 representation of $\begin{bmatrix} 6 \\ 3 \end{bmatrix}$ is $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

A set $X \subseteq \mathbb{N}^n$ is k-**recognizable** if the language consisting of the base-k representations of the elements of X is accepted by a finite automaton.

Semenov (1977). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. A set $X \subseteq \mathbb{N}^n$ is both k-recognizable and ℓ-recognizable if and only if it is semilinear.

Definition. A subset of $\mathbb{N}^n$ is **semilinear** if it is finite union of the form

$$\Big\{ \boldsymbol{v} + \sum_{i=1}^{m} k_i \boldsymbol{v}_i \ : \ k_1, \ldots, k_m \in \mathbb{N} \Big\},$$

where $m \in \mathbb{N}$ and $\boldsymbol{v}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \mathbb{N}^n$.

Presburger arithmetic. A subset of $\mathbb{N}^n$ is semilinear if and only if it is definable in $(\mathbb{N}, +)$.

Presburger arithmetic. A subset of $\mathbb{N}^n$ is semilinear if and only if it is definable in $(\mathbb{N}, +)$.

Definable sets. A set defined by a formula obtained from

- finite number of variables taking values in the given domain (here: in $\mathbb{N}$),
- equality and other given predicates (here: just $=$),
- functions (repeatedly) applied to variables (here: $+$),
- logical connectives such as $\mathrm{and}, \mathrm{or}$ and not,
- universal and existential quantifiers.

Presburger arithmetic. A subset of $\mathbb{N}^n$ is semilinear if and only if it is definable in $(\mathbb{N}, +)$.

Definable sets. A set defined by a formula obtained from

- finite number of variables taking values in the given domain (here: in $\mathbb{N}$),
- equality and other given predicates (here: just $=$),
- functions (repeatedly) applied to variables (here: $+$),
- logical connectives such as $\mathrm{and}, \mathrm{or}$ and not,
- universal and existential quantifiers.

Example. The order relation is definable in $(\mathbb{N}, +)$:

$$\{(x, y) \in \mathbb{N}^2 \ : \ x < y\} = \{(x, y) \in \mathbb{N}^2 \ : \ \exists z \in \mathbb{N} \, \neg(z + z = z) \ \wedge \ y = x + z\}$$

Presburger arithmetic. A subset of $\mathbb{N}^n$ is semilinear if and only if it is definable in $(\mathbb{N}, +)$.

Definable sets. A set defined by a formula obtained from

- finite number of variables taking values in the given domain (here: in $\mathbb{N}$),
- equality and other given predicates (here: just $=$),
- functions (repeatedly) applied to variables (here: $+$),
- logical connectives such as $\mathrm{and}, \mathrm{or}$ and not,
- universal and existential quantifiers.

Example. The order relation is definable in $(\mathbb{N}, +)$:

$$\{(x, y) \in \mathbb{N}^2 \ : \ x < y\} = \{(x, y) \in \mathbb{N}^2 \ : \ \exists z \in \mathbb{N} \ \neg(z + z = z) \ \wedge \ y = x + z\}$$

Semilinear sets are definable:

$$\{u \in \mathbb{N} \ : \ \exists x, y, z \in \mathbb{N} \ u = 6x + 9y + 20z\}$$

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi(1960)-Bruyère(1985). Let $k \in \mathbb{N}_{\geq 2}$ and $X \subseteq \mathbb{N}^n$. Then X is k-recognizable if and only if X is definable in $(\mathbb{N}, <, +, V_k)$.

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi(1960)-Bruyère(1985). Let $k \in \mathbb{N}_{\geq 2}$ and $X \subseteq \mathbb{N}^n$. Then X is k-recognizable if and only if X is definable in $(\mathbb{N}, <, +, V_k)$.

Example 1. $k^{\mathbb{N}} = \{x \in \mathbb{N} \ : \ V_k(x) = x\}$.

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi(1960)-Bruyère(1985). Let $k \in \mathbb{N}_{\geq 2}$ and $X \subseteq \mathbb{N}^n$. Then X is k-recognizable if and only if X is definable in $(\mathbb{N}, <, +, V_k)$.

Example 1. $k^{\mathbb{N}} = \{x \in \mathbb{N} \ : \ V_k(x) = x\}$.

Example 2. Let X be the set of all (x, y) such that $x \in 2^{\mathbb{N}}$ and x appears in the binary expansion of y.

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi(1960)-Bruyère(1985). Let $k \in \mathbb{N}_{\geq 2}$ and $X \subseteq \mathbb{N}^n$. Then X is k-recognizable if and only if X is definable in $(\mathbb{N}, <, +, V_k)$.

Example 1. $k^{\mathbb{N}} = \{x \in \mathbb{N} \ : \ V_k(x) = x\}$.

Example 2. Let X be the set of all (x, y) such that $x \in 2^{\mathbb{N}}$ and x appears in the binary expansion of y. Then $(x, y) \in X$ if and only if and only if

$$V_2(x) = x \ \wedge \ \Big(\exists z, t\big(z < x \ \wedge \ V_2(t) > x \ \wedge \ y = z + x + t\big) \ \vee \ \exists z\big(z < x \ \wedge \ y = z + x\big)\Big).$$

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi(1960)-Bruyère(1985). Let $k \in \mathbb{N}_{\geq 2}$ and $X \subseteq \mathbb{N}^n$. Then X is k-recognizable if and only if X is definable in $(\mathbb{N}, <, +, V_k)$.

Example 1. $k^{\mathbb{N}} = \{x \in \mathbb{N} \ : \ V_k(x) = x\}$.

Example 2. Let X be the set of all (x, y) such that $x \in 2^{\mathbb{N}}$ and x appears in the binary expansion of y. Then $(x, y) \in X$ if and only if and only if

$$V_2(x) = x \ \wedge \ \Big(\exists z, t\big(z < x \ \wedge \ V_2(t) > x \ \wedge \ y = z + x + t\big) \ \vee \ \exists z\big(z < x \ \wedge \ y = z + x\big)\Big).$$

Büchi (1960). The theory of $(\mathbb{N}, +, V_k)$ is decidable. In particular, for each k-recognizable $X \subseteq \mathbb{N}^d$, the theory of $(\mathbb{N}, +, X)$ is decidable.

Büchi arithmetic. For $k \in \mathbb{N}_{\geq 2}$, let $V_k(x) : \mathbb{N} \to k^{\mathbb{N}}$ be the function that maps x to the largest power of k dividing x.

Büchi(1960)-Bruyère(1985). Let $k \in \mathbb{N}_{\geq 2}$ and $X \subseteq \mathbb{N}^n$. Then X is k-recognizable if and only if X is definable in $(\mathbb{N}, <, +, V_k)$.

Example 1. $k^{\mathbb{N}} = \{x \in \mathbb{N} \ : \ V_k(x) = x\}$.

Example 2. Let X be the set of all (x, y) such that $x \in 2^{\mathbb{N}}$ and x appears in the binary expansion of y. Then $(x, y) \in X$ if and only if and only if

$$V_2(x) = x \ \wedge \ \Big(\exists z, t\big(z < x \ \wedge \ V_2(t) > x \ \wedge \ y = z + x + t\big) \ \vee \ \exists z\big(z < x \ \wedge \ y = z + x\big)\Big).$$

Büchi (1960). The theory of $(\mathbb{N}, +, V_k)$ is decidable. In particular, for each k-recognizable $X \subseteq \mathbb{N}^d$, the theory of $(\mathbb{N}, +, X)$ is decidable.

Cobham-Semenov restated. Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. A set $X \subseteq \mathbb{N}^n$ is definable in both $(\mathbb{N}, +, V_k)$ and $(\mathbb{N}, +, V_\ell)$ if and only if it is definable in $(\mathbb{N}, +)$.

H.-Schulz (2019-). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is k-recognizable, but not semilinear,
- Y is ℓ-recognizable, but not semilinear.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

H.-Schulz (2019-). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is k-recognizable, but not semilinear,
- Y is ℓ-recognizable, but not semilinear.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

H.-Schulz restated. Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$,
- Y is definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

H.-Schulz (2019-). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is k-recognizable, but not semilinear,
- Y is ℓ-recognizable, but not semilinear.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

H.-Schulz restated. Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$,
- Y is definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

Proof of Cobham-Semenov.

Suppose $X \subseteq \mathbb{N}^n$ is definable in both $(\mathbb{N}, +, V_k)$ and $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$. Then the theory of $(\mathbb{N}, +, X, X)$ is undecidable. However, then the theory of $(\mathbb{N}, +, V_k)$ is undecidable.

Villemaire (1992). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. The theory of $(\mathbb{N}, +, V_k, V_\ell)$ is undecidable.

Villemaire (1992). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. The theory of $(\mathbb{N}, +, V_k, V_\ell)$ is undecidable.

Bès (1996). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let Y be definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$. Then the theory of $(\mathbb{N}, +, V_k, Y)$ is undecidable.

Villemaire (1992). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. The theory of $(\mathbb{N}, +, V_k, V_\ell)$ is undecidable.

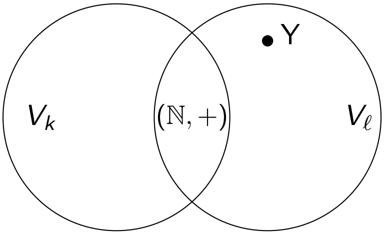
Bès (1996). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let Y be definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$. Then the theory of $(\mathbb{N}, +, V_k, Y)$ is undecidable.

In both cases $(\mathbb{N}, +, V_k, V_\ell)$ and $(\mathbb{N}, +, V_k, Y)$ define multiplication. Hence undecidability follows from Gödel's theorem that the theory of $(\mathbb{N}, +, \cdot)$ is undecidable.

Villemaire (1992). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. The theory of $(\mathbb{N}, +, V_k, V_\ell)$ is undecidable.

Bès (1996). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let Y be definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$. Then the theory of $(\mathbb{N}, +, V_k, Y)$ is undecidable.

In both cases $(\mathbb{N}, +, V_k, V_\ell)$ and $(\mathbb{N}, +, V_k, Y)$ define multiplication. Hence undecidability follows from Gödel's theorem that the theory of $(\mathbb{N}, +, \cdot)$ is undecidable.



H.-Schulz (2019). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$
- Y is definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

H.-Schulz (2019). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$
- Y is definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

Bès (1996). Let $k \in \mathbb{N}_{\geq 2}$, and let $X \subseteq \mathbb{N}^n$ be definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$. Then $(\mathbb{N}, +, X)$ defines $k^{\mathbb{N}}$.

H.-Schulz (2019). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$
- Y is definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

Bès (1996). Let $k \in \mathbb{N}_{\geq 2}$, and let $X \subseteq \mathbb{N}^n$ be definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$. Then $(\mathbb{N}, +, X)$ defines $k^{\mathbb{N}}$.

Left to show:

Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. Then the theory of $(\mathbb{N}, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ is undecidable.

H.-Schulz (2019). Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent, and let $X \subseteq \mathbb{N}^m$ and $Y \subseteq \mathbb{N}^n$ be such that

- X is definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$
- Y is definable in $(\mathbb{N}, +, V_\ell)$, but not in $(\mathbb{N}, +)$.

Then the theory of $(\mathbb{N}, +, X, Y)$ is undecidable.

Bès (1996). Let $k \in \mathbb{N}_{\geq 2}$, and let $X \subseteq \mathbb{N}^n$ be definable in $(\mathbb{N}, +, V_k)$, but not in $(\mathbb{N}, +)$. Then $(\mathbb{N}, +, X)$ defines $k^{\mathbb{N}}$.

Left to show:

Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. Then the theory of $(\mathbb{N}, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ is undecidable.

This question is an old question. Bruyère, Cherlin and van den Dries asked this question as early as 1985, and it has been restated in the literature many times.

This is kind of unfortunate. Even the theory of $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ includes many non-trivial number-theoretic statements about 2 and 3.

This is kind of unfortunate. Even the theory of $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ includes many non-trivial number-theoretic statements about 2 and 3.

Corollary of Baker's theorem on linear forms. For every $m \in \mathbb{N}$, there exists $C(m)$ such that if $n_1, n_2 \in \mathbb{N}$ with $2^{n_1} - 3^{n_2} = m$, then $n_1, n_2 \leq C$.

This is kind of unfortunate. Even the theory of $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ includes many non-trivial number-theoretic statements about 2 and 3.

Corollary of Baker's theorem on linear forms. For every $m \in \mathbb{N}$, there exists $C(m)$ such that if $n_1, n_2 \in \mathbb{N}$ with $2^{n_1} - 3^{n_2} = m$, then $n_1, n_2 \leq C$.

In $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$:

$$\forall u \exists v \forall x \in k^{\mathbb{N}} \forall y \in \ell^{\mathbb{N}} \; (x \geq v \;\wedge\; y \geq v) \rightarrow |x - y| > u.$$

This is kind of unfortunate. Even the theory of $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ includes many non-trivial number-theoretic statements about 2 and 3.

Corollary of Baker's theorem on linear forms. For every $m \in \mathbb{N}$, there exists $C(m)$ such that if $n_1, n_2 \in \mathbb{N}$ with $2^{n_1} - 3^{n_2} = m$, then $n_1, n_2 \leq C$.

In $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$:

$$\forall u \exists v \forall x \in k^{\mathbb{N}} \forall y \in \ell^{\mathbb{N}} \ (x \geq v \ \wedge \ y \geq v) \rightarrow |x - y| > u.$$

What does that mean?

You probably can't automatically prove theorems worth a Fields medal.

This is kind of unfortunate. Even the theory of $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ includes many non-trivial number-theoretic statements about 2 and 3.

Corollary of Baker's theorem on linear forms. For every $m \in \mathbb{N}$, there exists $C(m)$ such that if $n_1, n_2 \in \mathbb{N}$ with $2^{n_1} - 3^{n_2} = m$, then $n_1, n_2 \leq C$.

In $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$:

$$\forall u \exists v \forall x \in k^{\mathbb{N}} \forall y \in \ell^{\mathbb{N}} \ (x \geq v \ \wedge \ y \geq v) \to |x - y| > u.$$

What does that mean?

You probably can't automatically prove theorems worth a Fields medal.

Open question. What fragments of the theory of $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$ are decidable?

For simplicity, let $k = 2$ and $\ell = 3$. So consider $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$.

For simplicity, let $k = 2$ and $\ell = 3$. So consider $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$.

Let $\lambda : \mathbb{N} \to 2^{\mathbb{N}}$ map x to the unique element $2^m \in 2^{\mathbb{N}}$ with $2^m \leq x < 2^{m+1}$.

For simplicity, let $k = 2$ and $\ell = 3$. So consider $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$.

Let $\lambda : \mathbb{N} \to 2^{\mathbb{N}}$ map x to the unique element $2^m \in 2^{\mathbb{N}}$ with $2^m \leq x < 2^{m+1}$.

For $y \in 2^{\mathbb{N}}$, define $S(y)$ to be the set of all $x \in 3^{\mathbb{N}}$ such that $\lambda(x - \lambda(x)) = y$.

In words: $S(y)$ is the set of all powers of 3 for which y is the second largest power of 2 that appears in the binary representation of x.

For simplicity, let $k = 2$ and $\ell = 3$. So consider $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$.

Let $\lambda : \mathbb{N} \to 2^{\mathbb{N}}$ map x to the unique element $2^m \in 2^{\mathbb{N}}$ with $2^m \leq x < 2^{m+1}$.

For $y \in 2^{\mathbb{N}}$, define $S(y)$ to be the set of all $x \in 3^{\mathbb{N}}$ such that $\lambda(x - \lambda(x)) = y$.

In words: $S(y)$ is the set of all powers of 3 for which y is the second largest power of 2 that appears in the binary representation of x.

For example: $27 = 16 + 8 + 2 + 1$. So $27 \in S(8)$.

For simplicity, let $k = 2$ and $\ell = 3$. So consider $(\mathbb{N}, +, 2^{\mathbb{N}}, 3^{\mathbb{N}})$.

Let $\lambda : \mathbb{N} \to 2^{\mathbb{N}}$ map x to the unique element $2^m \in 2^{\mathbb{N}}$ with $2^m \leq x < 2^{m+1}$.

For $y \in 2^{\mathbb{N}}$, define $S(y)$ to be the set of all $x \in 3^{\mathbb{N}}$ such that $\lambda(x - \lambda(x)) = y$.

In words: $S(y)$ is the set of all powers of 3 for which y is the second largest power of 2 that appears in the binary representation of x.

For example: $27 = 16 + 8 + 2 + 1$. So $27 \in S(8)$.

Fact. For all $y \in 2^{\mathbb{N}}$, $S(y)$ is finite. However, for all $m, n \in \mathbb{N}$ there is $y \in 2^{\mathbb{N}}$ such that $y > m$ and $|S(y)| > n$.

Main Lemma. Let $m, n \in \mathbb{N}$, let $Z_1, \ldots, Z_m$ be a partition of $\{1, \ldots, n\}$. Then there are $s \in \mathbb{N}_{>0}$ and $t_1 < \cdots < t_n$ such that for $i = 1, \ldots, m$

$$S(2^{s+i}) \cap [3^{t_1}, 3^{t_n}] = \{3^{t_j} \ : j \in Z_i\}.$$

Main Lemma. Let $m, n \in \mathbb{N}$, let $Z_1, \ldots, Z_m$ be a partition of $\{1, \ldots, n\}$. Then there are $s \in \mathbb{N}_{>0}$ and $t_1 < \cdots < t_n$ such that for $i = 1, \ldots, m$

$$S(2^{s+i}) \cap [3^{t_1}, 3^{t_n}] = \{3^{t_j} \ : j \in Z_i\}.$$

$Z_1 = 1, 3, 5,$

$Z_2 = 2, 6, 7,$

$Z_3 = 4$

	3^{t_1}	3^{t_2}	3^{t_3}	3^{t_4}	3^{t_5}	3^{t_6}	3^{t_7}
2^{s+1}							
2^{s+2}							
2^{s+3}							

Main Lemma. Let $m, n \in \mathbb{N}$, let $Z_1, \dots, Z_m$ be a partition of $\{1, \dots, n\}$. Then there are $s \in \mathbb{N}_{>0}$ and $t_1 < \dots < t_n$ such that for $i = 1, \dots, m$

$$S(2^{s+i}) \cap [3^{t_1}, 3^{t_n}] = \{3^{t_j} \; : j \in Z_i\}.$$

$Z_1 = 1, 3, 5,$

$Z_2 = 2, 6, 7,$

$Z_3 = 4$

	3^{t_1}	3^{t_2}	3^{t_3}	3^{t_4}	3^{t_5}	3^{t_6}	3^{t_7}
2^{s+1}							
2^{s+2}							
2^{s+3}							

- Proof of Main Lemma just uses density of $2^{-\mathbb{N}}3^{\mathbb{N}}$ in $\mathbb{R}_{>0}$.

Main Lemma. Let $m, n \in \mathbb{N}$, let $Z_1, \dots, Z_m$ be a partition of $\{1, \dots, n\}$. Then there are $s \in \mathbb{N}_{>0}$ and $t_1 < \cdots < t_n$ such that for $i = 1, \dots, m$

$$S(2^{s+i}) \cap [3^{t_1}, 3^{t_n}] = \{3^{t_j} : j \in Z_i\}.$$

$Z_1 = 1, 3, 5,$

$Z_2 = 2, 6, 7,$

$Z_3 = 4$

	3^{t_1}	3^{t_2}	3^{t_3}	3^{t_4}	3^{t_5}	3^{t_6}	3^{t_7}
2^{s+1}							
2^{s+2}							
2^{s+3}							

- Proof of Main Lemma just uses density of $2^{-\mathbb{N}}3^{\mathbb{N}}$ in $\mathbb{R}_{>0}$.
- This allows us to code/interpret arbitrary large finite subsets of $\mathbb{N}^2$.

Main Lemma. Let $m, n \in \mathbb{N}$, let $Z_1, \dots, Z_m$ be a partition of $\{1, \dots, n\}$. Then there are $s \in \mathbb{N}_{>0}$ and $t_1 < \dots < t_n$ such that for $i = 1, \dots, m$

$$S(2^{s+i}) \cap [3^{t_1}, 3^{t_n}] = \{3^{t_j} \ : j \in Z_i\}.$$

$Z_1 = 1, 3, 5,$

$Z_2 = 2, 6, 7,$

$Z_3 = 4$

	3^{t_1}	3^{t_2}	3^{t_3}	3^{t_4}	3^{t_5}	3^{t_6}	3^{t_7}
2^{s+1}							
2^{s+2}							
2^{s+3}							

- Proof of Main Lemma just uses density of $2^{-\mathbb{N}}3^{\mathbb{N}}$ in $\mathbb{R}_{>0}$.
- This allows us to code/interpret arbitrary large finite subsets of $\mathbb{N}^2$.
- Such theories are known to be undecidable, as the halting problem or the tiling problem can be encoded in such theories.

Remark 1. The proof does not dependent on $\mathbb{N}$. The theory of $(\mathbb{R}, <, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ is undecidable whenever k and ℓ are multiplicatively independent.

Remark 1. The proof does not dependent on $\mathbb{N}$. The theory of $(\mathbb{R}, <, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ is undecidable whenever k and ℓ are multiplicatively independent.

Remark 2. In contrast to Villemaire's and Bès' results, we know that $(\mathbb{N}, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ does *not* define multiplication when k and ℓ are multiplicatively independent.

Remark 1. The proof does not dependent on $\mathbb{N}$. The theory of $(\mathbb{R}, <, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ is undecidable whenever k and ℓ are multiplicatively independent.

Remark 2. In contrast to Villemaire's and Bès' results, we know that $(\mathbb{N}, +, k^{\mathbb{N}}, \ell^{\mathbb{N}})$ does *not* define multiplication when k and ℓ are multiplicatively independent.

Remark 3. We expect that this method can be extended to prove other variants of Cobham's theorem.

Combinatorics on words.

We observed that $\{n \in \mathbb{N} \ : \ s_2(n) \text{ is even } \}$ is 2-recognizable, where $s_2(n)$ is the binary digit sum. Thus the function $f : \mathbb{N} \to \{0, 1\}$ given by

$$n \mapsto \begin{cases} 0 & \text{if } s_2(n) \text{ is even} \\ 1 & \text{otherwise.} \end{cases}$$

is definable in $(\mathbb{N}, +, V_2)$.

Combinatorics on words.

We observed that $\{n \in \mathbb{N} \ : \ s_2(n) \text{ is even } \}$ is 2-recognizable, where $s_2(n)$ is the binary digit sum. Thus the function $f : \mathbb{N} \to \{0,1\}$ given by

$$n \mapsto \begin{cases} 0 & \text{if } s_2(n) \text{ is even} \\ 1 & \text{otherwise.} \end{cases}$$

is definable in $(\mathbb{N}, +, V_2)$.

The word $f(0)f(1)f(2)\dots$ is the **Thue-Morse sequence**.

Combinatorics on words.

We observed that $\{n \in \mathbb{N} \ : \ s_2(n) \text{ is even } \}$ is 2-recognizable, where $s_2(n)$ is the binary digit sum. Thus the function $f : \mathbb{N} \to \{0, 1\}$ given by

$$n \mapsto \begin{cases} 0 & \text{if } s_2(n) \text{ is even} \\ 1 & \text{otherwise.} \end{cases}$$

is definable in $(\mathbb{N}, +, V_2)$.

The word $f(0)f(1)f(2)\ldots$ is the **Thue-Morse sequence**.

Jeff Shallit's idea. Use decision procedure for $(\mathbb{N}, +, V_2)$ to decide statements about the Thue-Morse sequence.

Combinatorics on words.
We observed that $\{n \in \mathbb{N} \ : \ s_2(n) \text{ is even } \}$ is 2-recognizable, where $s_2(n)$ is the binary digit sum. Thus the function $f : \mathbb{N} \to \{0, 1\}$ given by

$$n \mapsto \begin{cases} 0 & \text{if } s_2(n) \text{ is even} \\ 1 & \text{otherwise.} \end{cases}$$

is definable in $(\mathbb{N}, +, V_2)$.

The word $f(0)f(1)f(2)\ldots$ is the **Thue-Morse sequence**.

Jeff Shallit's idea. Use decision procedure for $(\mathbb{N}, +, V_2)$ to decide statements about the Thue-Morse sequence.

Example. To check that the Thue-Morse sequence in not eventually periodic, we have to decide

$$(\mathbb{N}, +, V_2) \models \forall p \ (p > 0) \to \Big(\forall i \ \exists j \ j > i \ \wedge \ f(j) \neq f(j + p)\Big)$$

A **continued fraction expansion** $[a_0; a_1, \ldots, a_k, \ldots]$ is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

Let a be a real number with continued fraction expansion $[a_0; a_1, \ldots, a_k, \ldots]$.

A **continued fraction expansion** $[a_0; a_1, \ldots, a_k, \ldots]$ is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

Let a be a real number with continued fraction expansion $[a_0; a_1, \ldots, a_k, \ldots]$.

Set $q_{-1} := 0$ and $q_0 := 1$, and for $k \geq 0$,

$$q_{k+1} := a_{k+1} \cdot q_k + q_{k-1}.$$

A **continued fraction expansion** $[a_0; a_1, \ldots, a_k, \ldots]$ is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

Let a be a real number with continued fraction expansion $[a_0; a_1, \ldots, a_k, \ldots]$.

Set $q_{-1} := 0$ and $q_0 := 1$, and for $k \geq 0$,

$$q_{k+1} := a_{k+1} \cdot q_k + q_{k-1}.$$

Ostrowski (1918). Every natural number N can be written uniquely as

$$N = \sum_{k=0}^{n} b_{k+1} q_k,$$

where $b_k \in \mathbb{N}$ such that $b_1 < a_1$, $b_k \leq a_k$ and, if $b_k = a_k$, $b_{k-1} = 0$.

Let $V_a : \mathbb{N} \to \mathbb{N}$ be the function that maps $x \geq 1$ with Ostrowski representation $b_n \dots b_1$ to the least q_k with $b_{k+1} \neq 0$, and 0 to 1.

Let $V_a : \mathbb{N} \to \mathbb{N}$ be the function that maps $x \geq 1$ with Ostrowski representation $b_n \dots b_1$ to the least q_k with $b_{k+1} \neq 0$, and 0 to 1.

H.-Terry (2016). Let a be quadratic. The theory of $(\mathbb{N}, <, +, V_a)$ is decidable.

Let $V_a : \mathbb{N} \to \mathbb{N}$ be the function that maps $x \geq 1$ with Ostrowski representation $b_n \dots b_1$ to the least q_k with $b_{k+1} \neq 0$, and 0 to 1.

H.-Terry (2016). Let a be quadratic. The theory of $(\mathbb{N}, <, +, V_a)$ is decidable.

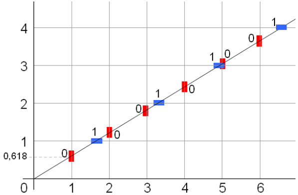
H.-Ma-Oei-Schaeffer-Schulz-Shallit (2021). The theory of

$$\{(\mathbb{N}, <, +, V_a) \ : \ a \in (0,1) \setminus \mathbb{Q}\}$$

is decidable.

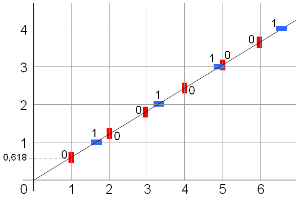
The **characteristic Sturmian word with slope** a is the infinite $\{0,1\}$-word $\mathrm{c_a} = c_a(0)c_a(1)c_a(2)\dots$ such that for all $n \in \mathbb{N}$

$$c_a(n) = \lfloor a(n+1) \rfloor - \lfloor an \rfloor - \lfloor a \rfloor.$$



The **characteristic Sturmian word with slope** a is the infinite $\{0,1\}$-word $\mathrm{c_a} = c_a(0)c_a(1)c_a(2)\ldots$ such that for all $n \in \mathbb{N}$

$$c_a(n) = \lfloor a(n+1) \rfloor - \lfloor an \rfloor - \lfloor a \rfloor.$$

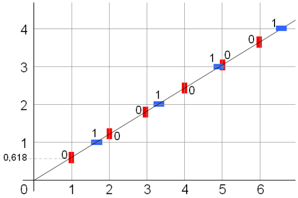


Fact. Let $n \in \mathbb{N}_{\geq 1}$. Then the following are equivalent:

- the n-th digit of the characteristic Sturmian word with slope a is 1.
- the a-Ostrowski representation of n ends with an odd number of 0's.

The **characteristic Sturmian word with slope** a is the infinite $\{0,1\}$-word $\mathrm{c_a} = c_a(0)c_a(1)c_a(2)\dots$ such that for all $n \in \mathbb{N}$

$$c_a(n) = \lfloor a(n+1) \rfloor - \lfloor an \rfloor - \lfloor a \rfloor.$$



Fact. Let $n \in \mathbb{N}_{\geq 1}$. Then the following are equivalent:

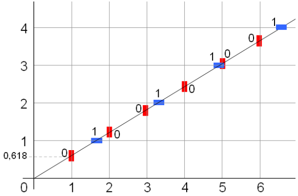
- the n-th digit of the characteristic Sturmian word with slope a is 1.
- the a-Ostrowski representation of n ends with an odd number of 0's.

Corollary. The set

$$\{n \in \mathbb{N} \ : \ c_a(n) = 1\}$$

is definable in $(\mathbb{N}, +, V_a)$.

The **characteristic Sturmian word with slope** a is the infinite $\{0,1\}$-word $\mathrm{c_a} = c_a(0)c_a(1)c_a(2)\dots$ such that for all $n \in \mathbb{N}$



$$c_a(n) = \lfloor a(n+1) \rfloor - \lfloor an \rfloor - \lfloor a \rfloor.$$

Fact. Let $n \in \mathbb{N}_{\geq 1}$. Then the following are equivalent:

- the n-th digit of the characteristic Sturmian word with slope a is 1.
- the a-Ostrowski representation of n ends with an odd number of 0's.

Corollary. The set

$$\{n \in \mathbb{N} \ : \ c_a(n) = 1\}$$

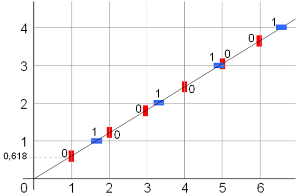
is definable in $(\mathbb{N}, +, V_a)$.

H.-Ma-Oei-Schaeffer-Schulz-Shallit (2021). The theory of

$$\{(\mathbb{N}, +, 0, 1, n \mapsto c_a(n)) \ : \ a \in (0,1) \setminus \mathbb{Q}\}$$

is decidable.

The **characteristic Sturmian word with slope** a is the infinite $\{0,1\}$-word $\mathrm{c_a} = c_a(0)c_a(1)c_a(2)\dots$ such that for all $n \in \mathbb{N}$



$$c_a(n) = \lfloor a(n+1) \rfloor - \lfloor an \rfloor - \lfloor a \rfloor.$$

Fact. Let $n \in \mathbb{N}_{\geq 1}$. Then the following are equivalent:

- the n-th digit of the characteristic Sturmian word with slope a is 1.
- the a-Ostrowski representation of n ends with an odd number of 0's.

Corollary. The set

$$\{n \in \mathbb{N} \ : \ c_a(n) = 1\}$$

is definable in $(\mathbb{N}, +, V_a)$.

H.-Ma-Oei-Schaeffer-Schulz-Shallit (2021). The theory of

$$\{(\mathbb{N}, +, 0, 1, n \mapsto c_a(n)) \ : \ a \in (0,1) \setminus \mathbb{Q}\}$$

is decidable.

Applications.

Let $\mathcal{L}_c$ be the language of $\mathcal{N}_a := (\mathbb{N}, +, 0, 1, n \mapsto c_a(n))$.

Applications.

Let $\mathcal{L}_c$ be the language of $\mathcal{N}_a := (\mathbb{N}, +, 0, 1, n \mapsto c_a(n))$. Consider the $\mathcal{L}_c$-sentence φ

$$\forall p \ (p > 0) \to \Big(\forall i \ \exists j \ j > i \ \wedge \ c(j) \neq c(j+p)\Big)$$

Applications.

Let $\mathcal{L}_c$ be the language of $\mathcal{N}_a := (\mathbb{N}, +, 0, 1, n \mapsto c_a(n))$. Consider the $\mathcal{L}_c$-sentence φ

$$\forall p\ (p > 0) \to \Big(\forall i\ \exists j\ j > i\ \wedge\ c(j) \neq c(j+p)\Big)$$

We observe that

$$\mathcal{N}_a \models \varphi \text{ if and only if } \mathrm{c_a} \text{ is not eventually periodic.}$$

Applications.

Let $\mathcal{L}_c$ be the language of $\mathcal{N}_a := (\mathbb{N}, +, 0, 1, n \mapsto c_a(n))$. Consider the $\mathcal{L}_c$-sentence φ

$$\forall p \ (p > 0) \rightarrow \Big(\forall i \ \exists j \ j > i \ \wedge \ c(j) \neq c(j+p)\Big)$$

We observe that

$$\mathcal{N}_a \models \varphi \text{ if and only if } \mathrm{c_a} \text{ is not eventually periodic.}$$

Thus

$$T_{\mathrm{Sturmian}} \models \varphi \text{ if and only if all Sturmian words are not evenutually periodic.}$$

Applications.

Let $\mathcal{L}_c$ be the language of $\mathcal{N}_a := (\mathbb{N}, +, 0, 1, n \mapsto c_a(n))$. Consider the $\mathcal{L}_c$-sentence φ

$$\forall p\ (p > 0) \rightarrow \Big(\forall i\ \exists j\ j > i\ \wedge\ c(j) \neq c(j+p)\Big)$$

We observe that

$$\mathcal{N}_a \models \varphi \text{ if and only if } \mathrm{c_a} \text{ is not eventually periodic.}$$

Thus

$$T_{\text{Sturmian}} \models \varphi \text{ if and only if all Sturmian words are not evenutually periodic.}$$

The decision procedure for T_{Sturmian} allows us to check that no Sturmian word is eventually periodic.

An implementation: **Pecan**

- Try Pecan at `http://reedoei.com/pecan`
- Git: `https://github.com/ReedOei/Pecan`

Pecan improves on **Walnut** by Mousavi, another automated theorem prover for deciding combinatorial properties of automatic words, by using Büchi automata instead of finite automata.

This difference enables Pecan to handle uncountable families of sequences, allowing us quantify over all Sturmian words.

Thank you!