Is Büchi's theorem useful for you?

Michel Rigo

http://www.discmath.ulg.ac.be/
http://orbi.ulg.ac.be/

27th May 2015

Université
de Liège

- In the 90's, V. Bruyère promoted a lot the "logical setting" but mostly in relation with the *theorem of Cobham from 1969* and the *recognizable sets of integers*
  - V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Bull. BMS 1992
  - G. Hansel, V. Bruyère, TCS 1997
  - C. Michaux, R. Villemaire, APAL 1996
  - A. Bès, JSL 2000
  - F. Point, V. Bruyère, ToCS 1997
- 2010–2012 Renewal of interest mostly by J. Shallit and his co-authors but oriented towards *decidability in combinatorics on words*
  - J.-P. Allouche, N. Rampersad, J. Shallit, TCS 2009
  - E. Charlier, N. Rampersad, J. Shallit, IJCS 2012
- Then move to "automatic theorem-proving"
  - D. Goč, D. Henshall, J. Shallit, 2012
  - D. Goč, H. Mousavi, J. Shallit, 2012
  - D. Goč, L. Schaeffer, J. Shallit, 2013
  - D. Goč, N. Rampersad, P. Salimov, M.R., 2013
  - H. Mousavi, J. Shallit, arxiv 2014, ...

Mention Flyspeck project, Hales'formal proof of *Kepler conjecture* (densest sphere packing)

M. Presburger (1929)

The first order theory $Th(\langle \mathbb{N}, + \rangle)$ of the natural numbers with addition is decidable.

Proof: $\langle \mathbb{N}, + \rangle$ admits quantifier elimination
→ *check a finite number of equalities (possibly modulo m)*
or inequalities of linear combination of integers and variables.

$=,\ (\exists x),\ \neg,\ \vee$

Example of formula (here, a sentence)

$$(\exists x)(\exists y)\neg(\exists z)\neg\{\neg(x + y = z \vee x = y + y) \\ \vee(\forall u)[(x = u) \vee \neg(y = u + z)]\}$$

All variables are in the scope of a quantifier → `True`/`False`.

M. Presburger (1929)

The first order theory $Th(\langle \mathbb{N}, + \rangle)$ of the natural numbers with addition is decidable.

Proof: $\langle \mathbb{N}, + \rangle$ admits quantifier elimination
$\rightarrow$ *check a finite number of equalities (possibly modulo m) or inequalities of linear combination of integers and variables.*

$$\boxed{=,\ (\exists x),\ \neg,\ \vee,\ (\forall x),\ \wedge,\ \rightarrow,\ \leftrightarrow,\ \leq, <}$$

$$x \leq y \equiv (\exists z)(x + z = y)$$

$$x < y \equiv (x \leq y) \wedge \neg(x = y)$$

Example of formula (here, a sentence)

$$(\exists x)(\exists y)(\forall z)\big\{(x + y = z \vee x = y + y) \\ \rightarrow (\forall u)[(x = u) \vee \neg(y = u + z)]\big\}$$

All variables are in the scope of a quantifier $\rightarrow$ `True`/`False`.

Example

The following sentence is true

$$(\forall x)(\exists y)[x = y + y \vee x = \mathcal{S}(y + y)]$$

where $\mathcal{S}(x) = y \equiv (x < y) \wedge (\forall z)(x < z \rightarrow (y \leq z))$.

We can define *constants*

$$x = 0 \equiv (\forall y)(x \leq y), \quad 1 = \mathcal{S}(0), \quad 2 = \mathcal{S}(1), \ldots$$

and we can define *multiplication by a constant* and *congruences*

$$2x \equiv x + x, \quad k.x = \underbrace{x + \cdots + x}_{k \text{ times}},$$

$$x \equiv_k y \ \equiv \ (\exists z)(x = y + k.z \vee y = x + k.z).$$

A less trivial example (Frobenius' problem)

Chicken McNuggets can be purchased only in 6, 9, or 20 pieces.
The largest number of nuggets that cannot be purchased is 43.

$$(\forall n)(n > 43 \rightarrow (\exists x, y, z \geq 0)(n = 6x + 9y + 20z))$$
$$\wedge \neg((\exists x, y, z \geq 0)(43 = 6x + 9y + 20z)) .$$

We can also define subsets of $\mathbb{N}$

Defining a subset of $\mathbb{N}$

$$\varphi(x) \equiv (\exists y)[\overbrace{\quad x \quad}^{\text{free variable}} = \mathcal{S}(y+y)]$$

$$\{n \in \mathbb{N} \mid \langle \mathbb{N}, + \rangle \models \varphi(n)\} = 2\mathbb{N} + 1$$

Remark

A subset of $\mathbb{N}$ is definable in $\langle \mathbb{N}, + \rangle$ if and only if it is ultimately periodic, i.e., a finite union of arithmetic progressions along with a finite set.

We can also define subsets of $\mathbb{N}^d$

Presburger definable sets

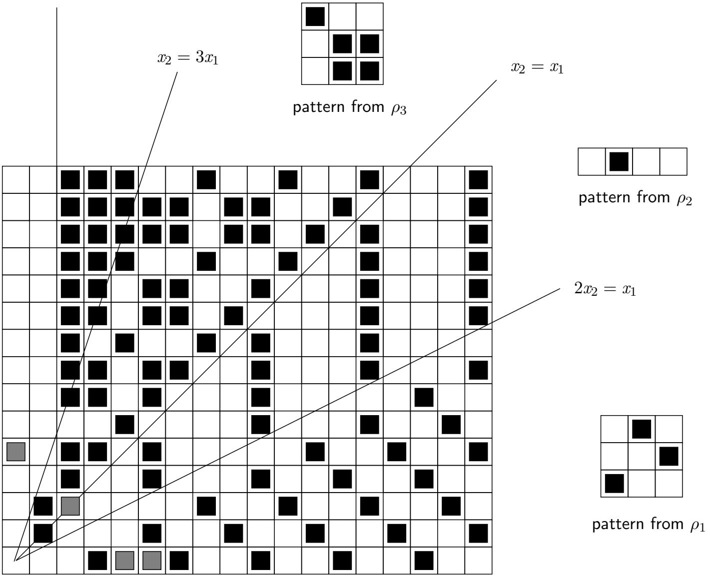
A formula $\varphi(x_1, \ldots, x_d)$ with d free variables,

$$\{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid \langle \mathbb{N}, + \rangle \models \varphi(n_1, \ldots, n_d)\}$$

$\varphi(x_1, x_2) \equiv \rho_1(x_1, x_2) \vee \rho_2(x_1, x_2) \vee \rho_3(x_1, x_2) \vee \rho_4(x_1, x_2) \vee \phi(x_1, x_2)$
where

$$\begin{aligned}
\rho_1(x_1, x_2) &\equiv (2x_2 < x_1) \wedge (x_1 + x_2 \equiv_3 0), \\
\rho_2(x_1, x_2) &\equiv (2x_2 \geq x_1) \wedge (x_2 < x_1) \wedge (x_1 \equiv_4 1), \\
\rho_3(x_1, x_2) &\equiv \underbrace{(x_2 > x_1) \wedge (x_2 < 3x_1)}_{\text{a region}} \wedge \underbrace{((2x_1 + x_2 \equiv_3 1) \vee (x_1 + x_2 \equiv_3 0))}_{\text{a pattern}}, \\
\rho_4(x_1, x_2) &\equiv (x_2 \geq 3x_1) \wedge (x_1 \geq 2), \\
\phi(x_1, x_2) &\equiv (x_1 = 0 \wedge x_2 = 4) \vee (x_1 = 2 \wedge x_2 = 2) \vee (x_1 = 4 \wedge x_2 = 0) \\
&\quad \underbrace{\vee (x_1 = 5 \wedge x_2 = 0)}_{\text{a few isolated points}}.
\end{aligned}$$

Generalization of ultimately periodic sets



Extension

J.R. Büchi 1960

Using finite automata constructions, the first order theory of the extension of $\langle\mathbb{N},+\rangle$ with V_k is still decidable.

Let $k \ge 2$, $V_k(x)$ is the largest power of k dividing x; $V_k(0) = 1$.

Corollary

Logical characterization of k-automatic sequences.

The infinite word $\mathbf{x}$ over A is k-automatic if and only if, for each $a \in A$, there exists a formula $\varphi_a(n)$ of $\langle\mathbb{N},+,V_k\rangle$ such that $\varphi_a(n)$ holds if and only if $\mathbf{x}(n) = a$.

We can still define subsets of $\mathbb{N}$ or $\mathbb{N}^d$, e.g.,

$$\mathit{fiber}_a(\mathbf{x}) = \{n \in \mathbb{N} \mid \langle\mathbb{N},+,V_k\rangle \models \varphi_a(n)\}$$

Example 1 in $\langle \mathbb{N}, + \rangle$

Let $A = \{a, b\}$ and $\varphi_a(n) \equiv (\exists y)(n = 2y)$.
We get the sequence $(ab)^\omega = abababab \cdots$ which is k-automatic for all $k \geq 2$.

$$f : a \mapsto aba, \;\; b \mapsto bab$$

Example 2 in $\langle \mathbb{N}, +, V_2 \rangle$

Let $A = \{a, b, c\}$ and

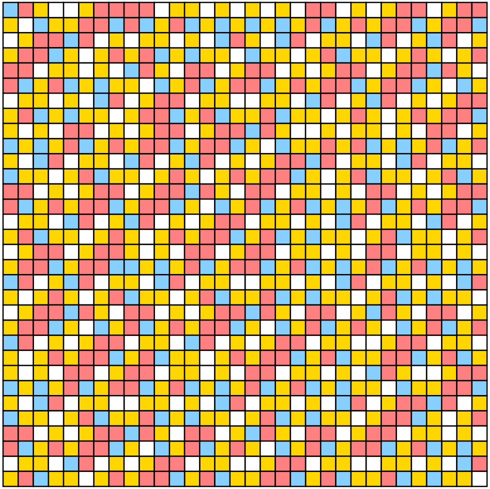
$$\varphi_b(n) \equiv V_2(n) = n, \quad \varphi_c(n) \equiv (n \geq 1) \wedge \neg\varphi_b(n).$$

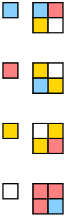
$$f : a \mapsto ab, \;\; b \mapsto bc, \;\; c \mapsto cc, \quad g : b \mapsto 1, \; a, c \mapsto 0$$

$$f^\omega(a) = abbcbcccbcccccccbcccc \cdots$$

$g(f^\omega(a))$ is the characteristic sequence of $\{2^n \mid n \geq 1\}$.

An example of 2-dimensional 2-automatic sequence





We have four formulas of the kind $\varphi_{\square}(x, y)$,
$\{(x, y) \in \mathbb{N}^2 \mid \langle \mathbb{N}, +, V_k \rangle \models \varphi_{\square}(x, y)\}$

Sketch of the proof of Büchi's thm.

From automata to formula

Idea: given a DFA accepting r-tuples of base-k expansions *conveniently padded*, obtain a formula ψ from $\langle \mathbb{N}, +, V_k \rangle$ with r free variables coding exactly the behaviour of the automaton:

$$\psi(x_1, \ldots, x_r) \equiv (\exists n_1) \cdots (\exists n_{\#Q}) \varphi(x_1, \ldots, x_r, n_1, \ldots, n_{\#Q}).$$

Similar to the proof showing that every function computable by a Turing machine is recursive.

- states are coded by vectors in $\{0, 1\}^{\#Q}$
- a path is thus coded by $\#Q$ base-k expansions of integers
- start in the initial state (least significant digits)
- end in a final state (most significant digits)
- compatible with the transition function of the DFA

See, for instance, Bruyère, Hansel, Michaux, Villemaire (1992).

from formula to automata (i.e., the most interesting part for us)

Example

Consider $\varphi(n) \equiv (\exists x)(\exists y)(V_2(x) = x \wedge n = x + 3.y)$.
Find a DFA accepting the base-2 expansions of the elements in

$$\{n \in \mathbb{N} \mid \langle \mathbb{N}, +, V_2 \rangle \models \varphi(n)\}$$

$1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, \ldots$

Example

Consider
$\psi(n, m) \equiv \varphi(n) \wedge (n \equiv_2 0 \to m = 2.n) \wedge (n \equiv_2 1 \to m = 3.n)$.
Find a DFA accepting the base-2 expansions of the elements in

$$\{(n_1, n_2) \in \mathbb{N} \mid \langle \mathbb{N}, +, V_2 \rangle \models \psi(n_1, n_2)\}$$

1	2	4	5	7	8	10	11	13	14	16	17	19	20	...
3	4	8	15	21	16	20	33	39	28	32	51	57	40	...

Formulas are defined inductively, thus start with atomic formulas, proceed by induction on the length of the formula.
Construction of automata, at least, for $\neg$, $\vee$, $=$, $(\exists x)$, V_k, $+$

- complementation of automata
- union of automata

$\longrightarrow$ Build bigger automata from smaller ones, determinize when needed, and also minimize.

Remark

This provides an alternative proof of Presburger's result. Given a sentence, there is an outermost quantifier, e.g., $(\exists x)\varphi(x)$.

Deciding if a DFA accepts at least one word is decidable (empty problem/universality problem for DFA).

Formulas are defined inductively, thus start with atomic formulas, proceed by induction on the length of the formula.
Construction of automata, at least, for $\neg$, $\vee$, $=$, $(\exists x)$, V_k, $+$

- complementation of automata
- union of automata

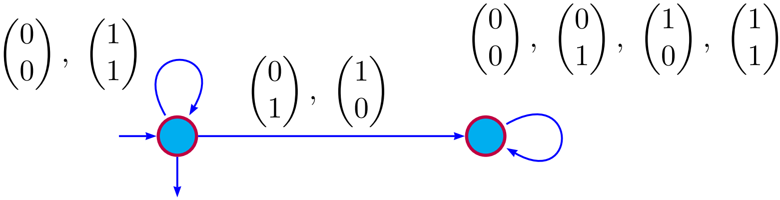
$\longrightarrow$ Build bigger automata from smaller ones, determinize when needed, and also minimize.

Remark

This provides an alternative proof of Presburger's result. Given a sentence, there is an outermost quantifier, e.g., $(\exists x)\varphi(x)$.

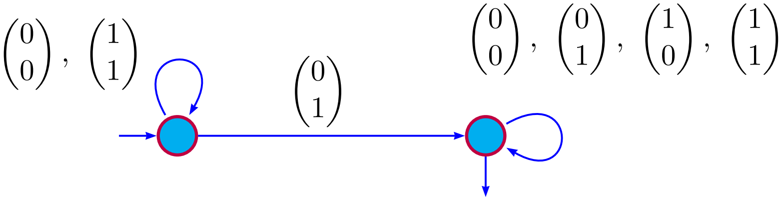
Deciding if a DFA accepts at least one word is decidable (empty problem/universality problem for DFA).

- DFA for $=$, $\{(x,y) \in \mathbb{N}^2 \mid x = y\}$



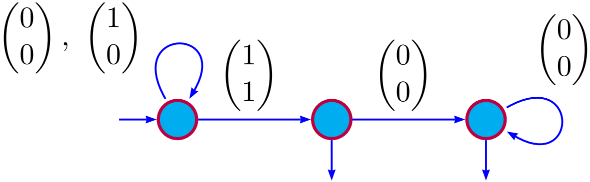
In every figure, we will consider base-2 expansions

- DFA reading m.s.d. first for $<$ (extra construction), $\{(x,y) \in \mathbb{N}^2 \mid x < y\}$



$$x < y \Leftrightarrow \mathsf{rep}_2(x) <_{\text{gen}} \mathsf{rep}_2(y).$$

- DFA reading m.s.d. first for V_k, $\{(x,y) \in \mathbb{N}^2 \mid y = V_2(x)\}$



$$\begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{matrix}$$

about existential quantifier

$$\begin{pmatrix} x \\ y_1 \\ \vdots \\ y_r \end{pmatrix}$$

$\varphi(x, y_1, \ldots, y_r)$

$$\begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}$$

$(\exists x)\varphi(x, y_1, \ldots, y_r)$

Get a nondeterministic automaton!

about existential quantifier

$$\begin{pmatrix} x \\ y_1 \\ \vdots \\ y_r \end{pmatrix}$$

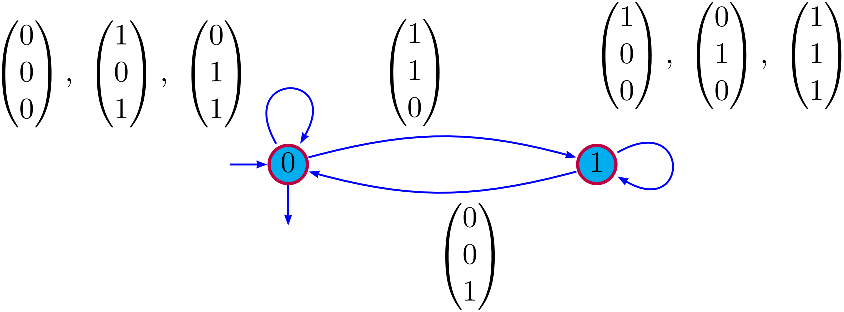
$$\varphi(x, y_1, \ldots, y_r)$$

$$\begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}$$

$$(\exists x)\varphi(x, y_1, \ldots, y_r)$$

Get a nondeterministic automaton!

- DFA reading l.s.d. first for $+$, $\{(x,y,z) \in \mathbb{N}^3 \mid x+y=z\}$

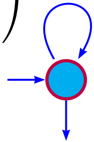


Such a DFA is easily obtained in every base (no carry propagation).

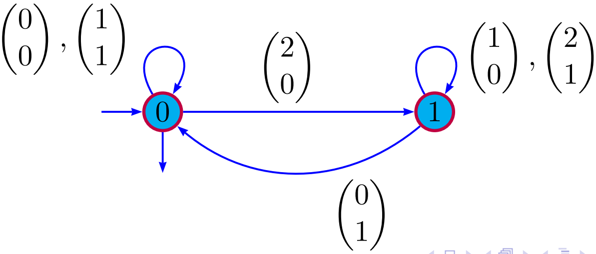
Remark about normalization

(i) add digit without carry (alphabet twice bigger)

$$\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}$$



(ii) *normalize*, DFA reading l.s.d. first, e.g. $(0121, 1001)$



Without logical techniques

Ultimate periodicity problem

INSTANCE: a k-uniform morphism f prolongable on a, a coding g
DECIDE whether $\mathbf{x} = g(f^\omega(a))$ is ultimately periodic?

J. Honkala, RAIRO 1986

Since $\mathbf{x}$ is k-automatic, for each a in A, we have a formula $\chi_{\mathbf{x},a}(n)$ which holds iff $\mathbf{x}(n) = a$.

$$\mathrm{eq}_{\mathbf{x}}(i,j) \equiv \bigvee_{a \in A} (\chi_{\mathbf{x},a}(i) \wedge \chi_{\mathbf{x},a}(j))$$

$$(\exists p)(\exists N)(\forall i \geq N)\, \mathrm{eq}_{\mathbf{x}}(i, i+p)$$

We can decide with automata.

$$(\exists p)(\exists N)(\forall i \geq N)\ \mathbf{x}(i) = \mathbf{x}(i+p).$$

Without logical techniques

ULTIMATE PERIODICITY PROBLEM

INSTANCE: a k-uniform morphism f prolongable on a, a coding g
DECIDE whether $\mathbf{x} = g(f^\omega(a))$ is ultimately periodic?

J. Honkala, RAIRO 1986

Since $\mathbf{x}$ is k-automatic, for each a in A, we have a formula $\chi_{\mathbf{x},a}(n)$ which holds iff $\mathbf{x}(n) = a$.

$$\mathrm{eq}_{\mathbf{x}}(i,j) \equiv \bigvee_{a \in A} (\chi_{\mathbf{x},a}(i) \wedge \chi_{\mathbf{x},a}(j))$$

$$(\exists p)(\exists N)(\forall i \geq N)\, \mathrm{eq}_{\mathbf{x}}(i, i+p)$$

We can decide with automata.

$$(\exists p)(\exists N)(\forall i \geq N)\ \mathbf{x}(i) = \mathbf{x}(i+p).$$

Without logical techniques

ULTIMATE PERIODICITY PROBLEM

INSTANCE: a k-uniform morphism f prolongable on a, a coding g
DECIDE whether $\mathbf{x} = g(f^\omega(a))$ is ultimately periodic?

J. Honkala, RAIRO 1986

Since $\mathbf{x}$ is k-automatic, for each a in A, we have a formula $\chi_{\mathbf{x},a}(n)$ which holds iff $\mathbf{x}(n) = a$.

$$\mathsf{eq}_{\mathbf{x}}(i,j) \equiv \bigvee_{a \in A} (\chi_{\mathbf{x},a}(i) \wedge \chi_{\mathbf{x},a}(j))$$

$$(\exists p)(\exists N)(\forall i \geq N)\, \mathsf{eq}_{\mathbf{x}}(i, i+p)$$

We can decide with automata.

$$(\exists p)(\exists N)(\forall i \geq N)\ \mathbf{x}(i) = \mathbf{x}(i+p).$$

As a summary

Reformulation by Charlier, Rampersad, Shallit

Theorem

Let $k \geq 2$. If one can express a property of a k-automatic sequence $\mathbf{x}$ using:

quantifiers, logical operations, integer variables,
addition, subtraction,
indexing into $\mathbf{x}$ and comparison of integers or elements of $\mathbf{x}$,

then this property is decidable.

Some applications

A. Thue

The Thue–Morse word is overlap-free.

See for instance, Lothaire 1983

$$\neg(\exists i)(\exists \ell \geq 1)[(\forall j < \ell)(\mathbf{t}(i+j) = \mathbf{t}(i+\ell+j)) \wedge \mathbf{t}(i) = \mathbf{t}(i+2\ell)]$$

Exercise

Write a formula that expresses the (non)existence of a square, a cube, a fixed n-power, in a k-automatic word.

Some applications

A. Thue

The Thue–Morse word is overlap-free.

See for instance, Lothaire 1983

$$\neg(\exists i)(\exists \ell \geq 1)[(\forall j < \ell)(\mathbf{t}(i+j) = \mathbf{t}(i+\ell+j)) \wedge \mathbf{t}(i) = \mathbf{t}(i+2\ell)]$$

Exercise

Write a formula that expresses the (non)existence of a square, a cube, a fixed n-power, in a k-automatic word.

Exercise (from Narad's talk)

Write a formula that expresses the (non)existence of xxx^R in a k-automatic word.

Charlier-Rampersad-Shallit

It is decidable if a k-automatic sequence contains powers of arbitrarily large exponent.

The formula

$$\psi(n,j) \equiv (\exists i)(\forall t < n)\mathbf{x}(i+t) = \mathbf{x}(i+j+t)$$

should hold for arbitrarily large n/j

How to check $(\forall i)(\exists n)(\exists j)[n > j.k^i \wedge \psi(n,j)]$?

If the DFA for $\psi(n,j)$ reads l.s.d. first, we should have strings ending in

$$\cdots \underbrace{\binom{\star}{0}\binom{\star}{0}\cdots\binom{\star}{0}}_{i}\binom{\neq 0}{0}$$

One can decide if a DFA accepts such arbitrarily long strings.

Charlier-Rampersad-Shallit

It is decidable if a k-automatic sequence contains powers of arbitrarily large exponent.

The formula

$$\psi(n,j) \equiv (\exists i)(\forall t < n)\mathbf{x}(i+t) = \mathbf{x}(i+j+t)$$

should hold for arbitrarily large n/j

How to check $(\forall i)(\exists n)(\exists j)[n > j.k^i \wedge \psi(n,j)]$?

If the DFA for $\psi(n,j)$ reads l.s.d. first, we should have strings ending in

$$\cdots \underbrace{\binom{\star}{0}\binom{\star}{0}\cdots\binom{\star}{0}}_{i}\binom{\neq 0}{0}$$

One can decide if a DFA accepts such arbitrarily long strings.

Quite a few properties that can be checked for k-automatic sequences

- (arbitrarily large) unbordered factors
- reccurrent word
- linearly recurrent word
- $\mathrm{Fac}(\mathbf{x}) \subset \mathrm{Fac}(\mathbf{y})$
- $\mathrm{Fac}(\mathbf{x}) = \mathrm{Fac}(\mathbf{y})$
- existence of an unbordered factor of length n

$\vdots$

A Glimpse at enumeration

Let $\mathbf{x}$ be a k-automatic sequence.

- Same factor of length n occurring in position i and j

$$F_{\mathbf{x}}(n, i, j) \equiv (\forall k < n)(\mathbf{x}(i + k) = \mathbf{x}(j + k))$$

- First occurrence of a factor of length n occurring in position i

$$P_{\mathbf{x}}(n, i) \equiv (\forall j < i) \neg F_{\mathbf{x}}(n, i, j)$$

The set $\{(n, i) \mid P_{\mathbf{x}}(n, i) \text{ true}\}$ is k-recognizable and

$$\forall n \geq 0, \quad \#\{i \mid P_{\mathbf{x}}(n, i) \text{ true}\} = p_{\mathbf{x}}(n).$$

- See the paper by Charlier, Rampersad and Shallit $\rightarrow$ k-regular sequences

k-automatic $<$ k-synchronized $<$ k-regular sequence

- D. Goč, L. Schaeffer, J. Shallit, Subword Complexity and k-Synchronization (DLT 2013)

Let $\mathbf{x}$ be a k-automatic sequence.

- $p_{\mathbf{x}}$ is a k-synchronized function
- the function counting the number of distinct length-n factors that are powers is k-synchronized
- the function counting the number of distinct length-n factors that are primitive words is k-synchronized

Also for morphic words?

Definition

A *Pisot number* is an algebraic integer $\alpha > 1$ whose conjugates have modulus less than one

Natural generalization of base-k numeration systems

Numeration basis

Let $U = (U_n)_{n\geq 0}$ be an increasing linear recurrent sequence of integers such that $U_0 = 1$.
Assume moreover that the characteristic polynomial of the recurrence relation is the minimal polynomial of a Pisot number.

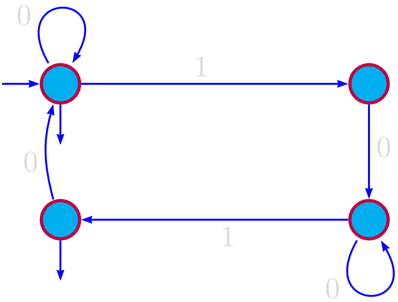
Example: Fibonacci/Zeckendorf numeration system $X^2 - X - 1$, $(1+\sqrt{5})/2 \simeq 1.618$, $|(1-\sqrt{5})/2| < 1$

Bruyere–Hansel

Let U be a "Pisot numeration basis".
A set of $\mathbb{N}^d$ is U-recognizable iff it is definable in $\langle \mathbb{N}, +, V_U \rangle$

$V_U(n)$ is the least U_j occurring in the U-expansion of n with a non-zero digit.

An example of U-recognizable set



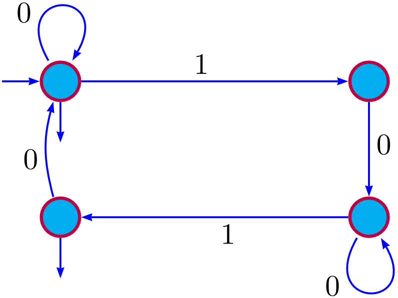
ε (0), 101 (4), 1001 (6), 1010 (7), 10001 (9), ...

Bruyere–Hansel

Let U be a "Pisot numeration basis".
A set of $\mathbb{N}^d$ is U-recognizable iff it is definable in $\langle \mathbb{N}, +, V_U \rangle$

$V_U(n)$ is the least U_j occurring in the U-expansion of n with a non-zero digit.

An example of U-recognizable set



ε (0), 101 (4), 1001 (6), 1010 (7), 10001 (9), ...

1) Let U be a "Pisot numeration basis".
The set of all greedy U-expansions is regular.
A bit more complicated than base-k (some technicalities).

2) Frougny's normalization (1985)

Let U be a "Pisot numeration basis".
Normalization (from any finite alphabet) and thus addition, are computable by finite automata.

3) Again, from formula to automata...
Construction of automata, at least, for $\neg$, $\vee$, $=$, $(\exists x)$, V_U, $+$

1) Let U be a "Pisot numeration basis".
The set of all greedy U-expansions is regular.
A bit more complicated than base-k (some technicalities).

2) Frougny's normalization (1985)

Let U be a "Pisot numeration basis".
Normalization (from any finite alphabet) and thus addition, are computable by finite automata.

3) Again, from formula to automata. . .
Construction of automata, at least, for $\neg$, $\vee$, $=$, $(\exists x)$, V_U, $+$

Application to (families of) words such as

$$abaababaabaababaababaabaababaabaab\cdots$$

$\varphi_a(n)$ definable in $\langle \mathbb{N}, +, V_F \rangle$

arXiv J. Shallit et al., Decision Algorithms for Fibonacci-Automatic Words, with Applications to Pattern Avoidance

$$abacabaabacababacabaabacabacabaac\cdots$$

$\varphi_a(n)$, $\varphi_b(n)$ definable in $\langle \mathbb{N}, +, V_T \rangle$

arXiv H. Mousavi, J. Shallit, Mechanical Proofs of Properties of the Tribonacci Word

Nothing left?

What about abelian properties? e.g., J. Cassaigne, J. D. Currie, L. Schaeffer, J. Shallit, Avoiding Three Consecutive Blocks of the Same Size and Same Sum

- Two factors of length n occurring in position i and j are abelian equivalent

$$A_{\mathbf{x}}(n,i,j) \equiv (\exists \nu \in S_n)(\forall k < n)(\mathbf{x}(i+k) = \mathbf{x}(\nu(j+k)))$$

The length of the formula is $\simeq n!$ and grows with n.

- First occurrence (up to abelian equivalence) of a factor of length n occurring in position i

$$AP_{\mathbf{x}}(n,i) \equiv (\forall j < i)\neg A_{\mathbf{x}}(n,i,j)$$

For a constant n. The set $\{i \mid AP_{\mathbf{x}}(n,i) \text{ true}\}$ is k-recognizable and

$$\#\{i \mid AP_{\mathbf{x}}(n,i) \text{ true}\} = a_{\mathbf{x}}(n).$$

For instance, Henshall and Shallit ask

- *Can the techniques be applied to detect abelian powers in automatic sequences?*

L. Schaeffer: the set of occurrences of abelian squares in the (2-automatic) paperfolding word is <u>not</u> 2-recognizable.

Remark

The Thue–Morse word is abelian periodic, $\mathbf{t} \in \{ab, ba\}^\omega$, therefore abelian equivalence is “easy”.

Goč, Rampersad, R., Salimov, On the number of abelian bordered words, 2014

For instance, Henshall and Shallit ask

- *Can the techniques be applied to detect abelian powers in automatic sequences?*

L. Schaeffer: the set of occurrences of abelian squares in the (2-automatic) paperfolding word is not 2-recognizable.

Remark

The Thue–Morse word is abelian periodic, $\mathbf{t} \in \{ab, ba\}^\omega$, therefore abelian equivalence is "easy".

Goč, Rampersad, R., Salimov, On the number of abelian bordered words, 2014

Question: could we have some undecidability result about a suitable extension $\langle \mathbb{N}, +, V_k, \Box_{\mathtt{ab}} \rangle$?

Let us mention Villemaire's result $\langle \mathbb{N}, +, V_k, V_\ell \rangle$ is undecidable.

Complexity issues

Fischer and Rabin (1973) – beyond NP

There exists a constant $c > 0$ such that for every decision procedure (algorithm) $\mathtt{A}$ for Presburger arithmetic $\mathfrak{p}$, there exists an integer N so that for every $n > N$ there exists a sentence φ of length n for which $\mathtt{A}$ requires more than $2^{2^{cn}}$ computational steps to decide whether $\mathfrak{p} \models \varphi$. This statement applies also in the case of non-deterministic algorithms.

Starting with a N-state automaton, the subset construction could lead to

$$2^{2^{\cdot^{\cdot^{\cdot^{2^{p(N)}}}}}} \quad \text{states !}$$

a tower of exponentials depending on the number of quantifiers.

Complexity issues

Fischer and Rabin (1973) – beyond NP

There exists a constant $c > 0$ such that for every decision procedure (algorithm) $\mathtt{A}$ for Presburger arithmetic $\mathfrak{p}$, there exists an integer N so that for every $n > N$ there exists a sentence φ of length n for which $\mathtt{A}$ requires more than $2^{2^{cn}}$ computational steps to decide whether $\mathfrak{p} \models \varphi$. This statement applies also in the case of non-deterministic algorithms.

Starting with a N-state automaton, the subset construction could lead to

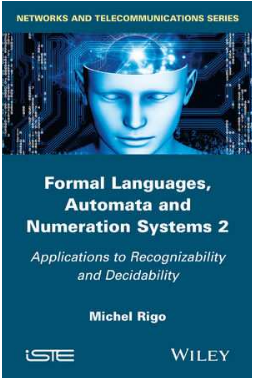
$$2^{2^{\cdot^{\cdot^{\cdot^{2^{p(N)}}}}}} \quad \text{states !}$$

a tower of exponentials depending on the number of quantifiers.

- F. Klaedtke, *Bounds on the automata size for Presburger arithmetic*, ACM Trans. Comput. Log. 9 (2008), Art. 11, 34.

Question: Study the (average) complexity with respect to formulae stemming from combinatorics on words.

On n'est jamais aussi bien servi que par soi-même. . .
We are our own best advocates, as the saying goes



From 28th November 2016 to 2nd December 2016
www.cant.ulg.ac.be/cant2016/