Decidability, Logic and Numeration Systems

Émilie Charlier

Département de Mathématique, Université de Liège

CANT 2016 - Marseille, November 28 - December 2

Sets of numbers and their representations

In this course we will be interested in sets of numbers.

In computer science, we are concerned by the question: how do we have such sets at our disposal?

This is why numeration systems come into play.

The basic consideration is as follows: properties of numbers are translated into syntactical (or combinatorial) properties of their representations.

Simple sets of numbers

Are the following sets of naturals simple ?

- $X_1 = \{n^2 : n \in \mathbb{N}\}$
- $X_2 = \{n \in \mathbb{N} : n \text{ is prime}\}$
- $X_3 = \{n \in \mathbb{N} : n \text{ is even}\}$
- $X_4 = \{2^n : n \in \mathbb{N}\}$
- $X_5 = \{n \in \mathbb{N} : \exists m \in \mathbb{N}, n^2 + n + 1 = 3m\}$
- $X_6 = \{n \in \mathbb{N} : \exists m \in \mathbb{N}, n^2 + n + 1 = 3m^2\}$

Non-trivial properties of numbers are dependent of the base, or the chosen numeration system.

Combinatorics on words

Numbers are represented by words.

Usually integers are represented by finite words while real numbers are represented by infinite words.

This is not true anymore when we consider non-standard numeration systems...

On the other hand, infinite words may also represent sets of numbers: the characteristic sequence of $X \subseteq \mathbb{N}$ is a binary infinite word.

This notion can be extended to subsets of $\mathbb{N}^d$.

Recognizable sets of integers

A subset X of $\mathbb{N}$ is recognizable w.r.t. a numeration system if the language

$$\{\mathrm{rep}(n)\colon n \in X\} \subseteq A^*$$

is accepted by a finite automaton.

Multidimensional case:

A subset X of $\mathbb{N}^d$ is recognizable w.r.t. a numeration system if the language

$$\{(\mathrm{rep}(n_1), \ldots, \mathrm{rep}(n_d))\colon (n_1, \ldots, n_d) \in X\}^{\#} \subseteq ((A \cup \{\#\})^d)^*,$$

where the padding symbol $\#$ is not contained in the numeration alphabet A, is accepted by a finite automaton.

Products of free monoids

If $A_1, \ldots, A_d$ are finite alphabets then

- For all i, A_i^* are free monoids.
- For $d \geq 2$, $A_1^* \times \cdots \times A_d^*$ is a monoid (for componentwise concatenation) which is not free:

$$\text{for } d = 2, \text{one has } (a_1, a_2) = (a_1, \varepsilon)(\varepsilon, a_2).$$

- $(A_1 \times \cdots \times A_d)^*$ is a free monoid – letters are elements of $A_1 \times \cdots \times A_d$.
- $(A_1 \times \cdots \times A_d)^*$ is a submonoid of $A_1^* \times \cdots \times A_d^*$.

- $\mathbb{N}$ is a free monoid.
- $\mathbb{N}^d$ is a monoid which is not free.
- Question: How to represent subsets of $\mathbb{N}^d$?
- If $X \subseteq \mathbb{N}^d$ then $\{(\mathrm{rep}(n_1), \ldots, \mathrm{rep}(n_d)) : (n_1, \ldots, n_d) \in X\}$ is *not a language*.

Example (d=3)

$$\begin{bmatrix} 101 \\ 1001 \\ 1 \end{bmatrix}^{\#} = \begin{bmatrix} \# & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ \# & \# & \# & 1 \end{bmatrix} = \begin{bmatrix} \# \\ 1 \\ \# \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ \# \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \# \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Depending on the context, we can interpret this word differently. For example, we can see this word as the binary representation of the triplet (5,9,1). In the Fibonacci numeration system, it is (4,6,1).

A range of numeration systems

Integer base representations

Let $b \geq 2$ be an integer. A natural number n is represented by the finite word $\mathrm{rep}_b(n) = c_\ell \cdots c_1 c_0$ over the alphabet $A_b = \{0, 1, \ldots, b-1\}$ obtained from the greedy algorithm:

$$n = \sum_{i=0}^{\ell} c_i b^i.$$

The greedy algorithm only imposes to have a nonzero leading digit c_ℓ and the set of all possible representations is

$$\mathcal{L}_b = \{1, \ldots, b-1\}\{0, \cdots, b-1\}^* \cup \{\varepsilon\}.$$

In this case, we talk about b-recognizable sets of $\mathbb{N}^d$.

Alternative definitions of b-recognizable sets

There exist several equivalent definitions of b-recognizable sets of integers using

- logic
- uniform morphisms
- finiteness of the b-kernel
- algebraic formal series
- recognizable/rational formal series

See the survey of Bruyère-Hansel-Michaux-Villemaire.

Unary representations

A natural number n is represented by $\mathrm{rep}_1(n) = a^n$, where a is any letter. The set of all possible representations is $\mathcal{L}_1 = a^*$.

In this case, we talk about 1-recognizable sets of $\mathbb{N}^d$.

In dimension 1, they correspond exactly to ultimately periodic sets (easy to see).

In the multidimensional case, it is more complicated to capture the essence of 1-recognizable sets.

Fibonacci representations

Let $F = (F_i)_{i \geq 0} = (1, 2, 3, 5, 8, \ldots)$ be the sequence obtained from the rules:

$$F_0 = 1, \ F_1 = 2 \text{ and } F_{i+2} = F_{i+1} + F_i \text{ for } i \geq 0.$$

A natural number n is represented by the finite word $\mathrm{rep}_F(n) = c_\ell \cdots c_1 c_0$ over the alphabet $A_F = \{0, 1\}$ obtained from the greedy algorithm:

$$n = \sum_{i=0}^{\ell} c_i F_i.$$

The greedy algorithm imposes, in addition to having a nonzero leading digit c_ℓ, that the valid representations do not contain two consecutive digits 1. The set of all possible representations is

$$\mathcal{L}_F = 1\{0, 01\}^* \cup \{\varepsilon\}.$$

Positional representations

Let $U = (U_i)_{i\geq 0} = (1, 2, 3, 5, 8, \ldots)$ be a base sequence, that is, an increasing sequence of positive integers satisfying:

$$U_0 = 1 \text{ and } C_U = \sup_{i\geq 0} \frac{U_{i+1}}{U_i} < +\infty.$$

A natural number n is represented by the finite word $\mathrm{rep}_U(n) = c_\ell \cdots c_1 c_0$ over the alphabet $A_U = \{0, 1, \ldots, \lceil C_U \rceil - 1\}$ obtained from the greedy algorithm:

$$n = \sum_{i=0}^{\ell} c_i U_i.$$

In this case, we talk about U-recognizable sets of integers.

The set of all possible representations is denoted by

$$\mathcal{L}_U = \{\mathrm{rep}_U(n) \colon n \in \mathbb{N}\}.$$

Of course a description of the numeration language $\mathcal{L}_U$ highly depends on the base sequence U.

Given such a system U, other choices of representations could be made: lazy algorithm, or even, considering all possible representations of a given integer.

Part 1

First order theory in base b and automata

b-recognizable sets of integers

Fix an integer $b \geq 2$.

We let $\mathrm{rep}_b(n_1, \ldots, n_d) = (\mathrm{rep}_b(n_1), \ldots, \mathrm{rep}_b(n_d))^{\#}$.

A set $X \subseteq \mathbb{N}^d$ is b-recognizable if the language

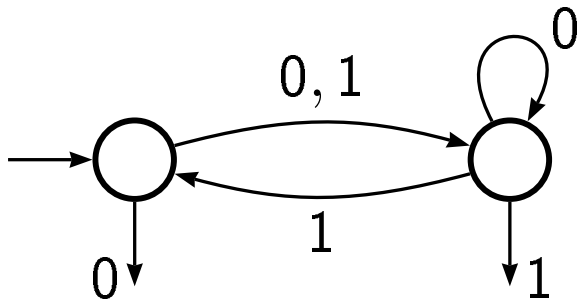
$$\mathrm{rep}_b(X) = \{\mathrm{rep}_b(n_1, \ldots, n_d) : (n_1, \ldots, n_d) \in X\}$$

is regular.

For $d = 1$, this is equivalent to say that its characteristic sequence $\chi_X \in \{0,1\}^{\mathbb{N}}$ is b-automatic: there exists a DFAO that on input $\mathrm{rep}_b(n)$ ouputs 1 if $n \in X$, and outputs 0 otherwise.

Example

The DFAO



generates the sequence

$$011010111\cdots$$

when reading 2-representations of integers, which corresponds to the subset of integers

$$\{1, 2, 4, 6, 7, 8, \ldots\}.$$

Cobham-Semenov theorem

Semi-linear sets of $\mathbb{N}^d$ are finite unions of sets of the form

$$p_0 + p_1\,\mathbb{N} + \cdots + p_\ell\,\mathbb{N}$$

where $p_0, p_1, \ldots, p_\ell \in \mathbb{N}^d$.

Theorem (Cobham 1969, Semenov 1977)

Let b and b' be multiplicatively independent bases. If a subset of $\mathbb{N}^d$ is simultaneously b-recognizable and b'-recognizable, then it is semi-linear.

Theorem (Cobham 1969, Semenov 1977)

Let b and b' be multiplicatively independent bases. If a subset of $\mathbb{N}^d$ is simultaneously b-recognizable and b'-recognizable, then it is semi-linear.

As linear sets are b-recognizable for all $b \geq 2$, we obtain that a subset of $\mathbb{N}^d$ is b-recognizable for all $b \geq 2$ iff it is semi-linear.

Theorem (Cobham 1969, Semenov 1977)

Let b and b' be multiplicatively independent bases. If a subset of $\mathbb{N}^d$ is simultaneously b-recognizable and b'-recognizable, then it is semi-linear.

As linear sets are b-recognizable for all $b \geq 2$, we obtain that a subset of $\mathbb{N}^d$ is b-recognizable for all $b \geq 2$ iff it is semi-linear.

NB: We can't replace $b \geq 2$ by $b \geq 1$!

Theorem (Cobham 1969, Semenov 1977)

Let b and b' be multiplicatively independent bases. If a subset of $\mathbb{N}^d$ is simultaneously b-recognizable and b'-recognizable, then it is semi-linear.

As linear sets are b-recognizable for all $b \geq 2$, we obtain that a subset of $\mathbb{N}^d$ is b-recognizable for all $b \geq 2$ iff it is semi-linear.

NB: We can't replace $b \geq 2$ by $b \geq 1$!

Theorem (Cobham 1969, Semenov 1977)

Let b and b' be multiplicatively independent bases. If a subset of $\mathbb{N}^d$ is simultaneously b-recognizable and b'-recognizable, then it is semi-linear.

As linear sets are b-recognizable for all $b \geq 2$, we obtain that a subset of $\mathbb{N}^d$ is b-recognizable for all $b \geq 2$ iff it is semi-linear.

NB: We can't replace $b \geq 2$ by $b \geq 1$!

The linear set $X = \{(n, 2n) : n \in \mathbb{N}\} = (1, 2)\,\mathbb{N}$ is not 1-recognizable since the language

$$\mathrm{rep}_1(X) = \{(\#^n a^n, a^{2n}) : n \in \mathbb{N}\} = \{(\#, a)^n (a, a)^n : n \in \mathbb{N}\}$$

is not regular (apply the pumping lemma).

Characterizing b-recognizable sets with logic

Theorem (Büchi 1960, Bruyère 1985)

Let $b \geq 2$ be an integer. A subset X of $\mathbb{N}^d$ is b-recognizable iff it is b-definable.

Definable sets

Let $\mathcal{S}$ be a logical structure whose domain is D and let $n \geq 1$. A set $X \subseteq D^n$ is definable in $\mathcal{S}$ if there exists a first-order formula $\varphi(x_1, \ldots, x_n)$ of $\mathcal{S}$, so that, for all $(d_1, \ldots, d_n) \in D^n$, $\varphi(d_1, \ldots, d_n)$ is true iff $(d_1, \ldots, d_n) \in X$:

$$X = \{(d_1, \ldots, d_n) \in D^n : \mathcal{S} \vDash \varphi(d_1, \ldots, d_n)\}.$$

A first-order formula is defined recursively from

- variables $x_1, x_2, x_3, \ldots$ describing elements of the domain D
- the equality $=$
- the relations and functions given in the structure $\mathcal{S}$
- the connectives $\vee, \wedge, \implies, \iff, \neg$
- the quantifiers $\forall, \exists$ on variables.

Presburger arithmetic $\langle \mathbb{N}, + \rangle$

$x \leq y$ is definable by $(\exists z)\ (x + z = y)$. Not true in $\langle \mathbb{Z}, + \rangle$.

$x = y$ is definable by $x \leq y \wedge y \leq x$. Not true in $\langle \mathbb{Z}, + \rangle$.

$x = 0$ is definable by $x + x = x$. OK in $\langle \mathbb{Z}, + \rangle$.

$x = 1$ is definable by $(\forall y)\ (y = 0 \vee x \leq y)$. Not true in $\langle \mathbb{Z}, + \rangle$.

Inductively, $x = c$ is definable for every $c \in \mathbb{N}$.

The sets $a\,\mathbb{N} + b$ are definable: $a\,\mathbb{N} + b = \{x : (\exists y)\ (x = ay + b)\}$ where ay stands for $y + y + \cdots y$ (a times).

In fact, a subset $X \subseteq \mathbb{N}$ is definable in $\langle \mathbb{N}, + \rangle$ iff it is a finite union of arithmetic progressions, or equivalently, ultimately periodic.

A subset $X \subseteq \mathbb{N}^d$ is definable in $\langle \mathbb{N}, + \rangle$ iff it is semi-linear.

b-definable sets

A set $X \subseteq \mathbb{N}^d$ is b-definable if it is definable in the structure $\langle \mathbb{N}, +, V_b \rangle$, where

- $+(x, y, z)$ is the ternary relation defined by $x + y = z$,
- $V_b(x)$ is the unary function defined as the largest power of b dividing x if $x \geq 1$ and $V_b(0) = 1$.

For example, the set $X = \{x \in \mathbb{N} : x \text{ is a power of } b\}$ is definable by $V_b(x) = x$.

It can be shown that the structures $\langle \mathbb{N}, +, V_b \rangle$ and $\langle \mathbb{N}, +, P_b \rangle$ are not equivalent, where $P_b(x)$ is 1 if x is a power of b and 0 otherwise.

Büchi-Bruyère's theorem

Theorem (Büchi 1960, Bruyère 1985)

Let $b \geq 2$ be an integer. A subset X of $\mathbb{N}^d$ is b-recognizable iff it is b-definable. Moreover, both directions are effective.

Sketch of the proof.

- From an automaton accepting $\mathrm{rep}_b(X)$, construct a first-order formula φ of the structure $\langle \mathbb{N}, +, V_b \rangle$ defining X, that is, such that $\varphi(x_1, \ldots, x_d)$ is true iff $(x_1, \ldots, x_d) \in X$.
- Conversely, given a first-order formula φ of the structure $\langle \mathbb{N}, +, V_b \rangle$ defining X, build an automaton accepting the language $\mathrm{rep}_b(X)$.

Büchi-Bruyère's theorem

Theorem (Büchi 1960, Bruyère 1985)

Let $b \geq 2$ be an integer. A subset X of $\mathbb{N}^d$ is b-recognizable iff it is b-definable. Moreover, both directions are effective.

Sketch of the proof.

- From an automaton accepting $\mathrm{rep}_b(X)$, construct a first-order formula φ of the structure $\langle \mathbb{N}, +, V_b \rangle$ defining X, that is, such that $\varphi(x_1, \ldots, x_d)$ is true iff $(x_1, \ldots, x_d) \in X$.
- Conversely, given a first-order formula φ of the structure $\langle \mathbb{N}, +, V_b \rangle$ defining X, build an automaton accepting the language $\mathrm{rep}_b(X)$.

Proof of the second part on the board...

Corollary: The first order theory of $\langle \mathbb{N}, +, V_b \rangle$ is decidable

We have to show that, given any closed first-order formula of $\langle \mathbb{N}, +, V_b \rangle$, we can decide whether it is true or false in $\mathbb{N}$.

Since there is no constant in the structure, a closed formula of $\langle \mathbb{N}, +, V_b \rangle$ is necessarily of the form $\exists x \varphi(x)$ or $\forall x \varphi(x)$.

The set

$$X_\varphi = \{x \in \mathbb{N} : \langle \mathbb{N}, +, V_b \rangle \models \varphi(x)\}$$

is b-definable, so it is b-recognizable by Büchi-Bruyère's theorem. This means that we can effectively construct a finite automaton accepting $\mathrm{rep}_b(X_\varphi)$.

The closed formula $\exists x \varphi(x)$ is true if $\mathrm{rep}_b(X_\varphi)$ is nonempty, and false otherwise.

As the emptiness of the language accepted by a finite automaton is decidable, we can decide if $\exists x \varphi(x)$ is true.

The case $\forall x \varphi(x)$ reduces to the previous one since $\forall x \varphi(x)$ is logically equivalent to $\neg \exists x \neg \varphi(x)$. We can again construct a finite automaton accepting the base-b representations of

$$X_{\neg\varphi} = \{x \in \mathbb{N} \colon \langle \mathbb{N}, +, V_b \rangle \nvDash \varphi(x)\}.$$

The language it accepts is empty iff the formula $\forall x \varphi(x)$ is true.

Applications to decidability questions for automatic sequences

Corollary

If we can express a property $P(n)$ of an integer n using quantifiers, logical operations, the operations of addition, subtraction, and comparison of integers or elements of a b-automatic sequence x, then $\exists n P(n)$, $\exists^{\infty} n P(n)$ and $\forall n P(n)$ are decidable.

We just have to convince ourselves that those properties P can all be expressed by a first-order formula of $\langle \mathbb{N}, +, V_b \rangle$.

In particular, what about the property $x[i] = x[j]$?

If x is b-automatic then, for all letters a occurring in x, the subsets $x^{-1}(a)$ of $\mathbb{N}$ are b-recognizable.

Hence they are definable by some first-order formulae ψ_a of $\langle \mathbb{N}, +, V_b \rangle$ (by Büchi-Bruyère theorem): $\psi_a(n)$ is true iff $x[n] = a$.

Therefore, we can express $x[i] = x[j]$ by the first-order formula $\varphi(i,j)$ of $\langle \mathbb{N}, +, V_b \rangle$:

$$\varphi(i,j) \equiv \bigvee_a (\psi_a(i) \wedge \psi_a(j)).$$

In particular, what about the property $x[i] = x[j]$?

In practice, given a DFAO M computing x, we can directly compute a finite automaton recognizing the pairs $(i, j) \in \mathbb{N}^2$ such that $x[i] = x[j]$.

We simply do the product of automata $M \times M$, simulate i on the first component and j on the second component, and we accept if the outputs of M after reading $\text{rep}_b(i)$ and $\text{rep}_b(j)$ are the same, and reject otherwise.

Applications

Consider the property of having an overlap.

A sequence $x = x[0]x[1]\ldots$ has an overlap beginning at position i iff $(\exists \ell \geq 1)\ (\forall j \leq \ell)\ x[i+j] = x[i+\ell+j]$.

Now suppose that x is b-automatic.

Given a DFAO M_1 generating x, we first create an NFA M_2 that on input (i, ℓ) accepts if $(\exists j \leq \ell)\ x[i+j] \neq x[i+j+\ell]$.

To do this, M_2 guesses the base-b representation of j, digit-by-digit, verifies that $j \leq \ell$, computes $i+j$ and $i+j+\ell$ on the fly, and accepts if $x[i+j] \neq x[i+j+\ell]$.

We now convert M_2 to a DFA M_3 using the subset construction, and inverse the final status of each state, obtaining a DFA M_3 which accepts those pairs (i, ℓ) such that $(\forall j \leq \ell)\ x[i+j] = x[i+j+\ell]$.

Now we create an NFA M_4 that on input i guesses $\ell \geq 1$ and accepts if M_3 accepts (i, ℓ).

As we can decide if M_4 accepts anything, we have obtained that

Proposition

It is decidable if a b-automatic sequence has an overlap.

Many decidability results for automatic sequences

- It is decidable whether a b-automatic sequence has k-powers (for a fixed k).
- It is decidable whether a b-automatic sequence is ultimately periodic.
- Given two b-automatic sequences x and y, it is decidable whether $\mathrm{Fac}(\mathrm{x}) \subseteq \mathrm{Fac}(\mathrm{y})$.
- ...

What about deciding whether a b-automatic sequence is Toeplitz (see Samuel Petite's lecture)?

The predicate

$$\forall n \; \exists p \geq 1 \; \forall \ell \; x[n] = x[n + \ell p]$$

is not a first order formula in $\langle \mathbb{N}, +, V_b \rangle$. Why? Is this property b-definable? What about the case where the periods p are restricted to powers of the base b?

A negative result by Schaeffer

If x is an arbitrary b-automatic sequence, then the predicate

$$\text{“}x[i, i + 2n - 1] \text{ is an abelian square”}$$

is not expressible in the logical theory $\langle \mathbb{N}, +, V_b \rangle$.

Complexity issues

This method for deciding first-order expressible properties of b-automatic sequences is very bad in terms of complexity.

In the worst case, we have a tower of exponentials:

$$2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}$$

where n is the number of states of the given DFAO and the height of the tower is the number of alternating quantifiers if the first-order predicate.

This procedure was implemented by Goc, Henshall, Mousavi, and Shallit. In practice, they were able to run their programs in order to prove (and reprove) many results about k-automatic sequences, in a purely mechanical way.

Part 2

Enumeration: counting first-order properties of b-automatic sequences is b-regular

On the blackboard...

Part 3

Logic and other numeration systems

Positional numeration systems

Let $U = (U_i)_{i\geq 0} = (1, 2, 3, 5, 8, \ldots)$ be a base sequence, that is, an increasing sequence of positive integers satisfying:

$$U_0 = 1 \text{ and } C_U = \sup_{i\geq 0} \frac{U_{i+1}}{U_i} < +\infty.$$

A natural number n is represented by the finite word $\mathrm{rep}_U(n) = c_\ell \cdots c_1 c_0$ over the alphabet $A_U = \{0, 1, \ldots, \lceil C_U \rceil - 1\}$ obtained from the greedy algorithm:

$$n = \sum_{i=0}^{\ell} c_i U_i.$$

The set of all possible representations is denoted by $\mathcal{L}_U = \{\mathrm{rep}_U(n) : n \geq 0\}$.

In this case, we talk about *U*-recognizable sets of integers.

A logical framework for positional numeration systems

Two problems:

- In general, $\mathbb{N}$ is not U-recognizable.
- The addition is not recognized by finite automaton.

Pisot systems

A Pisot number is an algebraic integer > 1 such that all of its Galois conjugates have absolute value < 1.

Working Hypothesis : U satifies a linear recurrence whose characteristic polynomial is the minimal polynomial of a Pisot number.

For such systems, Frougny showed that $\mathbb{N}$ and the addition are recognizable by finite automata.

A logical framework for Pisot systems

U-definable sets are subsets of $\mathbb{N}^d$ that are definable in the logical structure $\langle \mathbb{N}, +, V_U \rangle$, where, for $n \geq 1$, $V_U(n)$ denotes the smallest U_i occurring in $\mathrm{rep}_U(n)$ with a nonzero coefficient and $V_U(0) = 1$.

Theorem (Bruyère-Hansel 1997)

Under WH, the U-recognizable sets of integers coincide with the U-definable sets of integers.

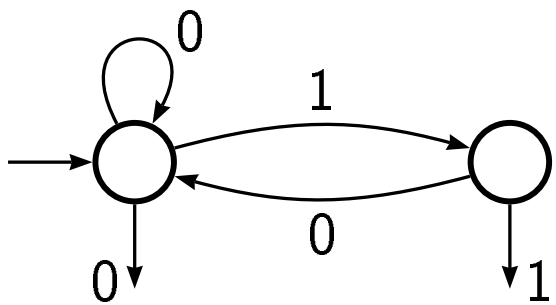
Corollary: The first order theory of $\langle \mathbb{N}, +, V_U \rangle$ is decidable

This result implies that there exist algorithms to decide U-definable properties for U-automatic sequences.

As an application, one can prove (and reprove, or verify) many results about the Fibonacci infinite word

$$\mathbf{f} = 0100101001001010010100100101001010\cdots$$

(which is the fixed point of $0 \mapsto 01,\ 1 \mapsto 0$).



Concrete applications (among many others)

In a purely mechanical way, Mousavi, Schaeffer and Shallit show:

- $\mathbf{f}$ is not ultimately periodic.
- $\mathbf{f}$ contains no fourth powers.
- Characterizations of squares, cubes, antisquares, palindromes, antipalindromes of $\mathbf{f}$.
- $\mathbf{f}$ is mirror-invariant.
- Factors of $\mathbf{f}$: least periods of factors, unbordered factors, Lyndon factors, special factors ...
- $\mathbf{f}$ is linearly recurrent.
- Computation of the critical exponant and ice.
- The lexicographically least element in $\mathcal{S}(\mathbf{f})$ is $0\mathbf{f}$.
- ...

Representing real numbers

In general real numbers are represented by infinite words.

In this context, we consider Büchi automata. An infinite word is accepted when the corresponding path goes infinitely many times through an accepting state.

We talk about ω-languages and ω-regular languages.

Regular languages vs ω-regular languages

Regular and ω-regular languages share some important properties: they both are stable under

- complementation
- finite union
- finite intersection
- morphic image
- inverse image under a morphism.

Nevertheless, they differ by some other aspects. One of them is determinism.

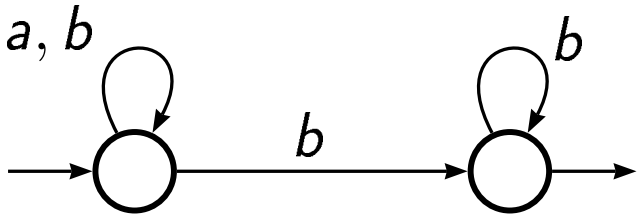
Deterministic Büchi automata

As for DFAs, we can define deterministic Büchi automata.

But one has to be careful as the family of ω-languages that are accepted by deterministic Büchi automata is strictly included in that of ω-regular languages.

Example

No deterministic Büchi automaton accepts the language accepted by



β-representation of real numbers

Let $\beta > 1$ be a real number and let $C \subset \mathbb{Z}$ be an alphabet. For a real number x, any infinite word $u = u_k \cdots u_1 u_0 \star u_{-1} u_{-2} \cdots$ over $C \cup \{\star\}$ such that

$$\mathrm{val}_\beta(u) := \sum_{-\infty < i \leq k} u_i \, \beta^i = x$$

is a β-representation of x.

In general, this is not unique.

Example ($\beta = \frac{1+\sqrt{5}}{2}$, the golden ratio)

Consider $x = \sum_{i \geq 1} \beta^{-2i}$.

As we also have $x = \sum_{i \geq 3} \beta^{-i}$, the words

$$u = 0 \star 001111 \cdots$$

and

$$v = 0 \star 0101010 \cdots$$

are both β-representations of x.

β-expansions of real numbers

For $x \geq 0$, among all such β-representations of x, we distinguish the β-expansion

$$d_\beta(x) = x_k \cdots x_1 x_0 \star x_{-1} x_{-2} \cdots$$

which is the infinite word over $A_\beta = \{0, \ldots, \lceil \beta \rceil - 1\}$ containing exactly one symbol $\star$ and obtained by the greedy algorithm.

Reals in $[0, 1)$ have a β-expansion of the form $0 \star u$ with $u \in A_\beta^\omega$.

In particular $d_\beta(0) = 0 \star 0^\omega$.

Parry's criterion

Theorem (Parry 1960)

An infinite word u is such that $0 \star u_1 u_2 \cdots$ is the β-expansion of a real number in $[0,1)$ iff for all $k \geq 1$, $u_k u_{k+1} \cdots <_{\text{lex}} d_\beta^*(1)$.

Here $d_\beta^*(1)$ denotes the lexicographically greatest $w \in A_\beta^\omega$ not ending in 0^ω such that $\text{val}_\beta(0 \star w) = 1$.

Example ($\beta = \frac{1+\sqrt{5}}{2}$, the Golden ratio)

We have seen that the words $u = 0 \star 001111 \cdots$ and $v = 0 \star 0101010 \cdots$ are both β-representations of $x = \sum_{i \geq 1} \beta^{-2i}$.

We have $d^*_\beta(1) = (10)^\omega$.

Thanks to Parry's theorem, the β-expansions of real numbers in $[0, 1)$ are of the form $0 \star u$, where $u \in \{0, 1\}^\omega$ does not contain 11 as a factor.

So v is *the* β-expansion of x.

Representing negative numbers

In order to deal with negative numbers, $\overline{a}$ denotes the integer $-a$ for all $a \in \mathbb{Z}$. Moreover we write

$$\overline{u\,v} = \overline{u}\,\overline{v}, \quad \overline{u \star v} = \overline{u} \star \overline{v} \quad \text{and } \overline{\overline{u}} = u.$$

For $x < 0$, the β-expansion of x is defined as

$$d_\beta(x) = \overline{d_\beta(-x)}.$$

We let $\overline{A_\beta} = \{\overline{0}, \overline{1}, \ldots, \overline{\lceil \beta \rceil - 1}\}$ and $\tilde{A}_\beta = A_\beta \cup \overline{A_\beta}$ (with $\overline{0} = 0$).

Multidimensional framework

Let $\beta = \frac{1+\sqrt{5}}{2}$.

Consider $\mathbf{x} = (x_1, x_2) = (\frac{1+\sqrt{5}}{4}, 2+\sqrt{5})$. We have

$$d_\beta(\mathbf{x}) = \begin{array}{cccccccccc} 0 & 0 & 0 & \star & 1 & 0 & 0 & 1 & 0 & 0 & \cdots \\ 1 & 0 & 1 & \star & 0 & 1 & 0 & 1 & 0 & 1 & \cdots \end{array}$$

where the first β-expansion is padded with some leading zeroes.

With $\mathbf{y} = (x_1, x_2) = (\frac{1+\sqrt{5}}{4}, -\frac{1}{2})$, we get

$$d_\beta(\mathbf{y}) = \begin{array}{cccccccccc} 0 & \star & 1 & 0 & 0 & 1 & 0 & 0 & \cdots \\ 0 & \star & 0 & \overline{1} & 0 & 0 & \overline{1} & 0 & \cdots \end{array}$$

β-recognizable subsets of $\mathbb{R}^d$

A set $X \subseteq \mathbb{R}^d$ is β-recognizable if $d_\beta(X)$ is accepted by some Büchi automaton.

Theorem

Let $X \subseteq \mathbb{R}^d$. The following are equivalent:

1. *X is β-recognizable.*
2. *$\mathbf{0}^* d_\beta(X)$ is ω-regular.*
3. *For some map $m : \mathbf{x} \to \mathbb{N}$, $\{\mathbf{0}^{m(\mathbf{x})} d_\beta(\mathbf{x}) : \mathbf{x} \in X\}$ is ω-regular.*

Parry numbers

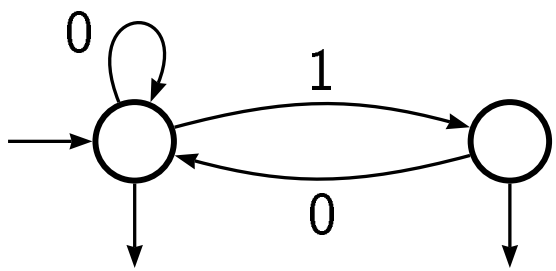
A Parry number is a real number $\beta > 1$ for which $d^*_\beta(1)$ is ultimately periodic.

Corollary (of Parry's theorem)

If β is a Parry number then $d_\beta([0,1)^d)$ is accepted by a deterministic Büchi automaton.

Example ($\beta = \frac{1+\sqrt{5}}{2}$, the Golden ratio)

The ω-language $d_\beta([0,1))$ is accepted by



First order theory for mixed real and β-integer variables

A real number x is a β-integer if $d_\beta(x)$ is of the kind $u \star 0^\omega$. The set of β-integers is denoted by $\mathbb{Z}_\beta$.

A subset of $\mathbb{R}^d$ is β-definable if it is definable by a first-order formula of

$$\langle \mathbb{R}, +, \leq, \mathbb{Z}_\beta, X_\beta \rangle,$$

where X_β is the finite collection of binary predicates $\{X_{\beta,a} : a \in \tilde{A}_\beta\}$ defined by $X_{\beta,a}(x, y)$ iff $y = \beta^i$ for some $i \in \mathbb{Z}$, and

- either $|x| < y$ and $a = 0$,
- or $|x| \geq y$, $i \leq k$ and $x_i = a$.

0 and 1 are β-definable

$x = 0$ is defined by $x + x = x$.

$z = 1$ can be defined in $\langle \mathbb{R}, +, \leq, \mathbb{Z}_\beta, X_\beta \rangle$ by the formula

$$z \in \mathbb{Z}_\beta \ \wedge \ \big[(\forall x)\big(\big(x \in \mathbb{Z}_\beta \ \wedge \ x > 0\big) \implies x \geq z\big)\big]$$

The structure $\langle \mathbb{R}, +, \leq, 1, X_\beta \rangle$

The property of being an integer power of β is definable in $\langle \mathbb{R}, +, \leq, 1, X_\beta \rangle$ by the formula

$$x \text{ is a power of } \beta \iff (\exists y)\,(X_{\beta,1}(x, y) \ \wedge \ x = y)\,.$$

We can also define the properties of being a positive or negative power of β by adding $x > 1$ or $x < 1$ respectively.

Let b be a power of β. One can define the next (or the previous) power of β as follows:

$$\begin{aligned} b' = \beta b \iff & (b' \text{ is a power of } \beta) \\ & \wedge\, (b' > b) \\ & \wedge \ (\forall c)((c \text{ is a power of } \beta \ \wedge \ c > b) \implies c \geq b'). \end{aligned}$$

Consequently, any constant (positive or negative) power of β is definable in $\langle \mathbb{R}, +, \leq, 1, X_\beta \rangle$.

The two structures $\langle \mathbb{R}, +, \leq, 1, X_\beta \rangle$ and $\langle \mathbb{R}, +, \leq, \mathbb{Z}_\beta, X_\beta \rangle$ are equivalent.

The set $\mathbb{Z}_\beta$ can be defined in $\langle \mathbb{R}, +, \leq, 1, X_\beta \rangle$ by the formula

$$z \in \mathbb{Z}_\beta \Leftrightarrow (\forall y)\big[(y \text{ is a negative power of } \beta) \implies X_{\beta,0}(z, y)\big].$$

Multiplication (or division) by β is β-definable

$$y = \beta x \Leftrightarrow (\forall b)\Big[\bigwedge_{a \in \tilde{A}_\beta} (X_{\beta,a}(x,b) \implies X_{\beta,a}(y, \beta b))\Big].$$

Note that $X_{\beta,a}(x,b)$ implies that b is an integer power of β.

Consequently, multiplication (or division) by a constant power of β is β-definable.

First order theory for mixed real and integer variables

Here we suppose that $\beta = b \in \mathbb{N}$.

Theorem (Boigelot-Rassart-Wolper 1998)

A subset of $\mathbb{R}^d$ is b-recognizable iff it is b-definable.

As the emptiness of an ω-regular language is decidable, we obtain

Corollary

The first order theory of $\langle \mathbb{R}, +, \leq, \mathbb{Z}, X_b \rangle$ is decidable.

Deciding topological properties

The following properties of b-recognizable subsets X of $\mathbb{R}^d$ are decidable:

- X has a nonempty interior:

$$(\exists x \in X)\ (\exists \varepsilon > 0)\ (\forall y)\ (|x - y| < \varepsilon \implies y \in X).$$

- X is open:

$$(\forall x \in X)\ (\exists \varepsilon > 0)\ (\forall y)\ (|x - y| < \varepsilon \implies y \in X).$$

- X is closed: OK as $\mathbb{R}^d \setminus X$ is b-recognizable.
- ...

A Cobham theorem for real numbers

Theorem (Boigelot-Brusten-Bruyère-Jodogne-Leroux 2001, 2008, 2009)

Let b and b' be multiplicatively independent integer bases. A subset $X \subseteq \mathbb{R}^d$ is simultaneously weakly b-recognizable and b'-recognizable iff it is definable in $\langle \mathbb{R}, +, \leq, \mathbb{Z} \rangle$.

For $d = 1$, this result is equivalent to

Theorem (Adamczewski-Bell 2011)

Let $b, b' \geq 2$ be multiplicatively independent integers. A compact set $X \subseteq [0, 1]$ is simultaneously b-self-similar and b'-self-similar iff it is a finite union of closed intervals with rational endpoints.

b-self-similarity

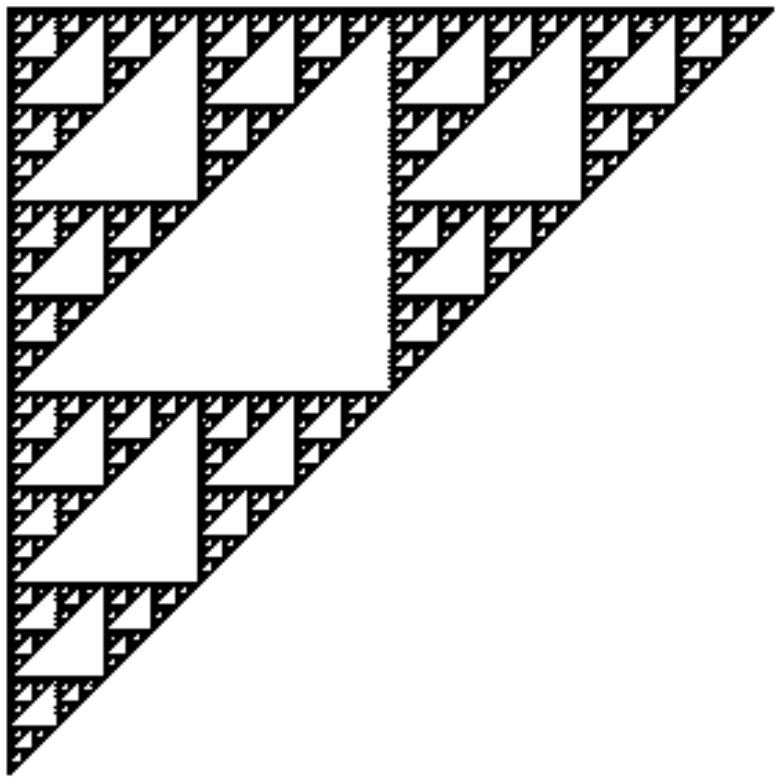
Let $b \geq 2$ be an integer.

A compact set $X \subset [0,1]^d$ is b-self-similar if its b-kernel

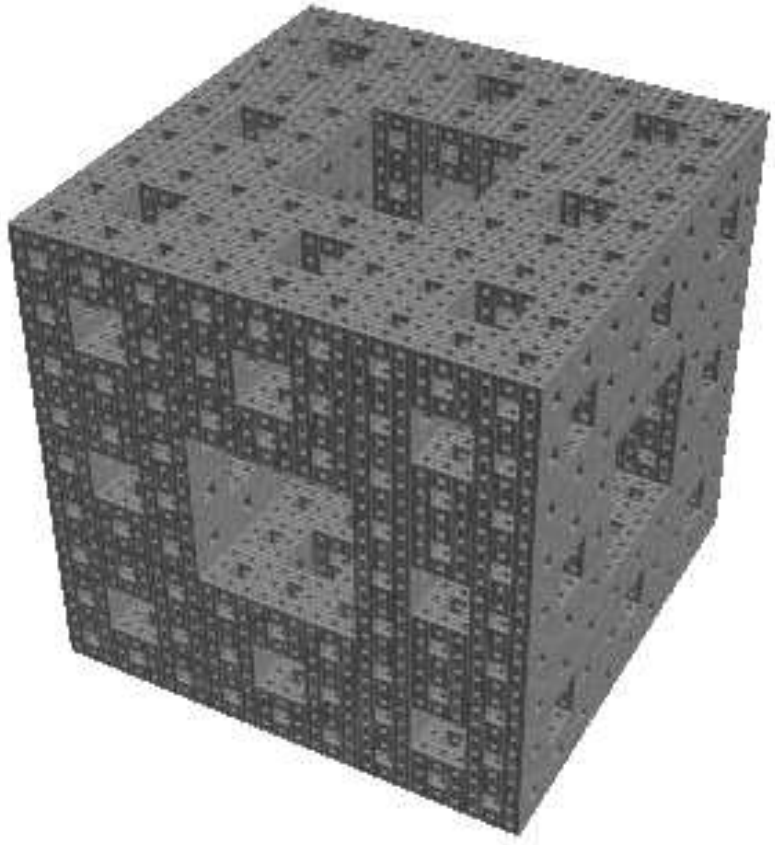
$$\left\{(b^k X - \mathbf{a}) \cap [0,1]^d : \quad k \geq 0,\ \mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d,\ (\forall i)\, 0 \leq a_i < b^k \right\}$$

is finite.

Pascal's triangle modulo 2 is 2-self-similar.



Menger sponge is 3-self-similar.



Sets of integers definable in $\langle \mathbb{R}, +, \leq, \mathbb{Z} \rangle$

A rational polyhedron is a region of $\mathbb{R}^d$ delimited by a finite number of hyperplanes whose equations have integer coefficients.

Any finite union of rational polyhedra is b-self-similar.

As it admits the elimination of quantifiers, a bounded subset $X \subseteq \mathbb{R}^d$ is definable in $\langle \mathbb{R}, +, \leq, \mathbb{Z} \rangle$ is a finite union of rational polyhedra.

In particular, for $d = 1$, a subset $X \subseteq [0, 1]$ is definable in $\langle \mathbb{R}, +, \leq, \mathbb{Z} \rangle$ iff it is a finite union of closed intervals with rational endpoints.

Linking b-self-similarity and b-recognizability

Theorem (C-Leroy-Rigo 2015)

A subset of $[0,1]^d$ is b-self-similar iff it is weakly b-recognizable.

Corollary (simultaneously obtained by Chan-Hare 2014)

Let $b, b' \geq 2$ be two multiplicatively independent integers.
A compact set $X \subset [0,1]^d$ is simultaneously b-self-similar and b'-self-similar iff it is a finite union of rational polyhedra.

In fact, we proved the above link in the more general case of a real Pisot base β.

Characterizing β-recognizable sets using logic

Theorem (C-Leroy-Rigo 2015)

- *If β is Parry then every β-recognizable $X \subseteq \mathbb{R}^d$ is β-definable.*
- *If β is Pisot then every β-definable $X \subseteq \mathbb{R}^d$ is β-recognizable.*

Again, the proof of the second item is by induction on the length of the formula defing X.

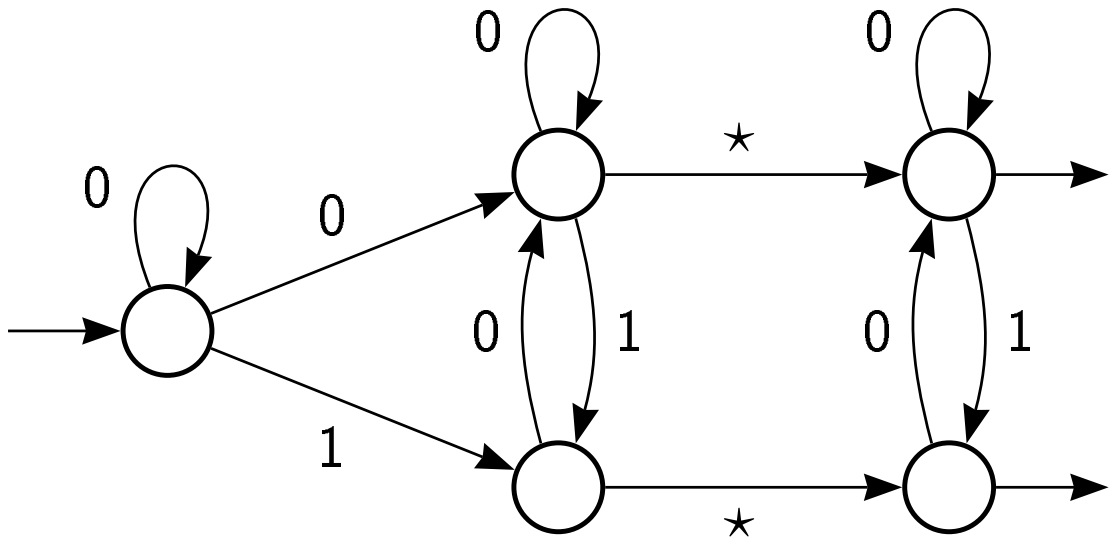
The induction step follows from the properties of ω-regular languages: they are stable under complementation, intersection, union, and projection on components.

What we have to check that the atomic formulas are all β-recognizable.

Lemma 1: If β is Parry then $\mathbb{R}$ is β-recognizable.

Example ($\beta = \frac{1+\sqrt{5}}{2}$)

The following Büchi automaton accepts the ω-language $0^* d_\beta(x \in \mathbb{R} : x \geq 0\}$.



To handle negative numbers, we make the union of two such automata.

Lemma 2: If β is Pisot then the addition is β-recognizable.

Let $C \subset \mathbb{Z}$ be finite. The normalization function is the function

$$\nu_{\beta,C} : C^+ \star C^\omega \to \tilde{A_\beta}^+ \star \tilde{A_\beta}^\omega$$

that maps any β-representation of a real number x onto $d_\beta(x)$.

Theorem (Frougny 1992)

Let β be a Pisot number and $C \subset \mathbb{Z}$ be finite. The normalization is realizable by a (non-deterministic) letter-to-letter transducer $\mathcal{T}$: $\forall u \in C^\omega \; \exists_1 v \in {A_\beta}^\omega \; (u, v) \in R_\mathcal{T}$. Further, $d_\beta(\mathrm{val}_\beta(0 \star u)) = 0 \star v$.

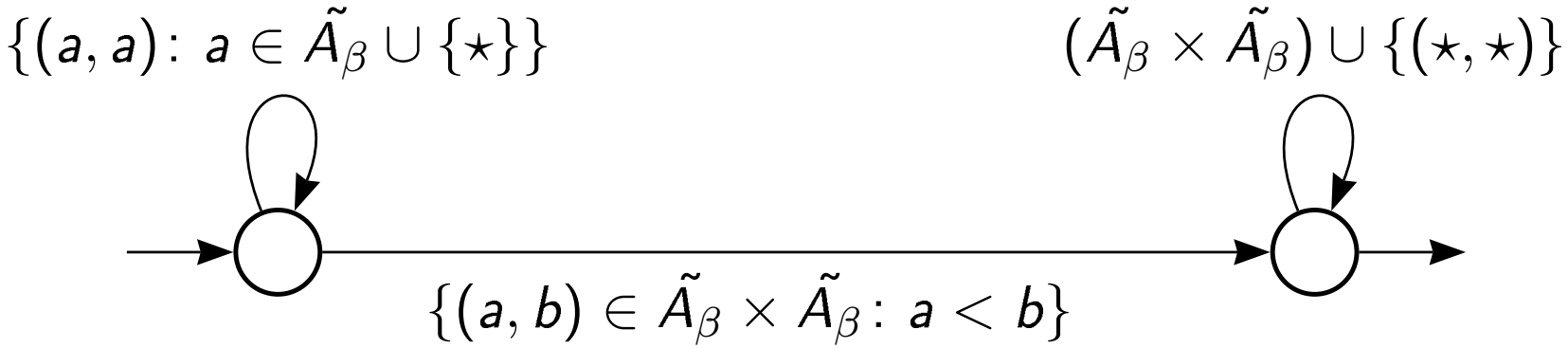
Corollary

If β is Pisot then the addition is β-recognizable.

Lemma 3: If β is Parry then $\{(x, y) \in \mathbb{R}^2 : x < y\}$ is β-recognizable.

Proof.

It is recognized by the intersection of the Büchi automaton accepting $d_\beta(\mathbb{R}^2)$ with



□

Lemma 4: If β is Parry then $\mathbb{Z}_\beta$ is β-recognizable.

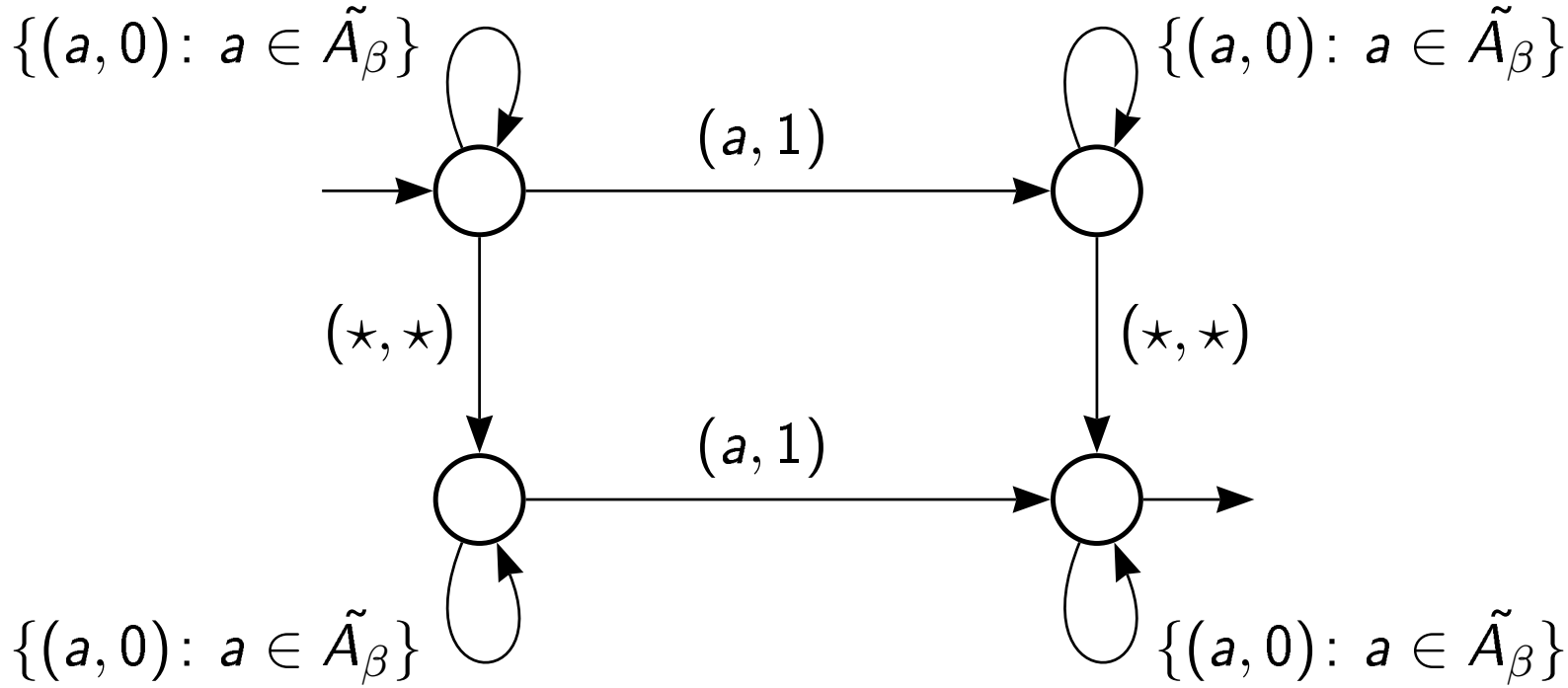
Proof.

The Büchi automaton recognizing $\mathbb{Z}_\beta$ is the intersection of the one recognizing $\mathbb{R}$ with the one accepting $\tilde{A_\beta}^+ \star 0^\omega$. $\square$

Lemma 5: If β is Parry then X_β is β-recognizable.

Proof.

For each $a \in \tilde{A}_\beta$, $d_\beta(X_{\beta,a})$ is accepted by the intersection of the Büchi automaton accepting $d_\beta(\mathbb{R}^2)$ with



Decidability

As a consequence of this and the fact that emptiness of an ω-language is decidable, we obtain

Corollary

The first order theory of $\langle \mathbb{R}, +, \leq, \mathbb{Z}_\beta, X_\beta \rangle$ *is decidable.*