From substitutions to number theory

and backwards

Boris Adamczewski

CNRS & Institut Camille Jordan, Lyon

Introduction

—

Substitutive sequences

Substitutions and their fixed points

Let $\mathcal{A}$ and $\mathcal{B}$ be two finite sets. A map σ from $\mathcal{A}$ to $\mathcal{B}^*$ extends uniquely to a homomorphism between the free monoids $\mathcal{A}^*$ and $\mathcal{B}^*$ (that is, with the rule $\sigma(w_1 w_2 \cdots w_r) = \sigma(w_1)\sigma(w_2)\cdots\sigma(w_r)$).

Such a homomorphism from $\mathcal{A}^*$ to $\mathcal{B}^*$ is usually called a substitution or a morphism.

Substitutions and their fixed points

Let $\mathcal{A}$ and $\mathcal{B}$ be two finite sets. A map σ from $\mathcal{A}$ to $\mathcal{B}^*$ extends uniquely to a homomorphism between the free monoids $\mathcal{A}^*$ and $\mathcal{B}^*$ (that is, with the rule $\sigma(w_1 w_2 \cdots w_r) = \sigma(w_1)\sigma(w_2)\cdots\sigma(w_r)$).

Such a homomorphism from $\mathcal{A}^*$ to $\mathcal{B}^*$ is usually called a substitution or a morphism.

Fixed points. A substitution σ from $\mathcal{A}^*$ to itself is said to be prolongable if there exists a letter a such that $\sigma(a) = aw$, where the word w is such that $\sigma^n(w)$ is a nonempty word for every $n \geq 0$.

In that case, the sequence of finite words $(\sigma^n(a))_{n\geq 0}$ converges in $\mathcal{A}^\infty = \mathcal{A}^* \cup \mathcal{A}^{\mathbb{N}}$ (endowed with its usual topology) to an infinite word denoted $\sigma^\infty(a)$.

This infinite word is clearly a fixed point for σ (extended by continuity to infinite words) and we say that $\sigma^\infty(a)$ is generated by the morphism σ.

Substitutions and their fixed points

Let $\mathcal{A}$ and $\mathcal{B}$ be two finite sets. A map σ from $\mathcal{A}$ to $\mathcal{B}^*$ extends uniquely to a homomorphism between the free monoids $\mathcal{A}^*$ and $\mathcal{B}^*$ (that is, with the rule $\sigma(w_1 w_2 \cdots w_r) = \sigma(w_1)\sigma(w_2)\cdots\sigma(w_r)$).

Such a homomorphism from $\mathcal{A}^*$ to $\mathcal{B}^*$ is usually called a substitution or a morphism.

Fixed points. A substitution σ from $\mathcal{A}^*$ to itself is said to be prolongable if there exists a letter a such that $\sigma(a) = aw$, where the word w is such that $\sigma^n(w)$ is a nonempty word for every $n \geq 0$.

In that case, the sequence of finite words $(\sigma^n(a))_{n\geq 0}$ converges in $\mathcal{A}^\infty = \mathcal{A}^* \cup \mathcal{A}^{\mathbb{N}}$ (endowed with its usual topology) to an infinite word denoted $\sigma^\infty(a)$.

This infinite word is clearly a fixed point for σ (extended by continuity to infinite words) and we say that $\sigma^\infty(a)$ is generated by the morphism σ.

Example. The morphism τ defined over the alphabet $\{0,1\}$ by $\tau(0) = 01$ and $\tau(1) = 10$ generates the Thue–Morse word

$$\mathbf{t} = \tau^\infty(0) = 01101001100101\cdots .$$

Primitivity versus uniformity

Primitivity versus uniformity

Primitive substitutions. A substitution σ from $\mathcal{A}^*$ to itself is said to be primitive if there exists a positive integer n such that for all pairs $(a, b) \in \mathcal{A}^2$, the letter b occurs in the word $\sigma^n(a)$.

Primitivity versus uniformity

Primitive substitutions. A substitution σ from $\mathcal{A}^*$ to itself is said to be primitive if there exists a positive integer n such that for all pairs $(a, b) \in \mathcal{A}^2$, the letter b occurs in the word $\sigma^n(a)$.

Example. The substitution σ defined over the alphabet $\{0, 1\}$ by $\sigma(0) = 01$ and $\sigma(1) = 0$ is a primitive substitution which generates the Fibonacci sequence

$$\mathbf{f} = \sigma^\infty(0) = 0100101001 \cdots .$$

Primitivity versus uniformity

Primitive substitutions. A substitution σ from $\mathcal{A}^*$ to itself is said to be primitive if there exists a positive integer n such that for all pairs $(a, b) \in \mathcal{A}^2$, the letter b occurs in the word $\sigma^n(a)$.

Example. The substitution σ defined over the alphabet $\{0, 1\}$ by $\sigma(0) = 01$ and $\sigma(1) = 0$ is a primitive substitution which generates the Fibonacci sequence

$$\mathbf{f} = \sigma^\infty(0) = 0100101001 \cdots .$$

Uniform substitution. If there is a positive integer k such that each element of $\mathcal{A}$ is mapped to a word of length k, then the substitution is called k-uniform.

Primitivity versus uniformity

Primitive substitutions. A substitution σ from $\mathcal{A}^*$ to itself is said to be primitive if there exists a positive integer n such that for all pairs $(a, b) \in \mathcal{A}^2$, the letter b occurs in the word $\sigma^n(a)$.

Example. The substitution σ defined over the alphabet $\{0, 1\}$ by $\sigma(0) = 01$ and $\sigma(1) = 0$ is a primitive substitution which generates the Fibonacci sequence

$$\mathbf{f} = \sigma^\infty(0) = 0100101001 \cdots .$$

Uniform substitution. If there is a positive integer k such that each element of $\mathcal{A}$ is mapped to a word of length k, then the substitution is called k-uniform.

Example. The substitution κ defined over the alphabet $\{0, 1\}$ by $\kappa(0) = 010$ and $\kappa(1) = 111$ is a non-primitive 3-uniform substitution which generates the Cantor sequence

$$\mathbf{k} = \kappa^\infty(0) = 0100101001 \cdots .$$

Primitivity versus uniformity

Primitive substitutions. A substitution σ from $\mathcal{A}^*$ to itself is said to be primitive if there exists a positive integer n such that for all pairs $(a, b) \in \mathcal{A}^2$, the letter b occurs in the word $\sigma^n(a)$.

Example. The substitution σ defined over the alphabet $\{0, 1\}$ by $\sigma(0) = 01$ and $\sigma(1) = 0$ is a primitive substitution which generates the Fibonacci sequence

$$\mathbf{f} = \sigma^\infty(0) = 0100101001 \cdots .$$

Uniform substitution. If there is a positive integer k such that each element of $\mathcal{A}$ is mapped to a word of length k, then the substitution is called k-uniform.

Example. The substitution κ defined over the alphabet $\{0, 1\}$ by $\kappa(0) = 010$ and $\kappa(1) = 111$ is a non-primitive 3-uniform substitution which generates the Cantor sequence

$$\mathbf{k} = \kappa^\infty(0) = 0100101001 \cdots .$$

The substitution φ defined over the alphabet $\{0, 1, 2\}$ by $\varphi(0) = 012$, $\varphi(1) = 12$ and $\varphi(2) = 2$ is neither primitive nor uniform.

Substitutive sequences and related object

Substitutive sequence. A sequence is said to be substitutive if it is the image by a substitution of a word generated by a substitution.

Substitutive sequences and related object

Substitutive sequence. A sequence is said to be substitutive if it is the image by a substitution of a word generated by a substitution.

Substitutive sequences have a number of nice properties such as :

- they enjoy some self-similarity,
- they have a low complexity but are not necessarily periodic,
- they contain repetitive patterns and have often strong recurrence properties...

Substitutive sequences and related object

Substitutive sequence. A sequence is said to be substitutive if it is the image by a substitution of a word generated by a substitution.

Substitutive sequences have a number of nice properties such as :

- they enjoy some self-similarity,
- they have a low complexity but are not necessarily periodic,
- they contain repetitive patterns and have often strong recurrence properties...

Many people in the audience make use of substitutions as a way to construct interesting objects which reflects these nice properties (such as substitutive dynamical systems, substitutive tilings, fractals...).

Number theorists also use substitutive sequences to construct numbers.

Part I. From substitutions to number theory

—

Real numbers arising from substitutions

Substitutive real numbers

Real numbers can naturally be attached to finite or infinite words by considering numeration systems (here, base-b expansions and continued fractions).

Words are then though of as sequences of digits.

Substitutive real numbers

Real numbers can naturally be attached to finite or infinite words by considering numeration systems (here, base-b expansions and continued fractions).

Words are then though of as sequences of digits.

Why substitutive numbers would be interesting ?

- They are far from randomness (Borel's conjecture, Lang's conjecture)
- Most of them can be computed in linear time (low algorithmic complexity, Hartmanis–Stearns problem)
- One can hope that the structure of their sequence of digits is simple enough to understand them.

Substitutive real numbers

Real numbers can naturally be attached to finite or infinite words by considering numeration systems (here, base-b expansions and continued fractions).

Words are then though of as sequences of digits.

Why substitutive numbers would be interesting ?

- They are far from randomness (Borel's conjecture, Lang's conjecture)
- Most of them can be computed in linear time (low algorithmic complexity, Hartmanis–Stearns problem)
- One can hope that the structure of their sequence of digits is simple enough to understand them.

General (unformal) principle. A real number associated with a non-ultimately periodic substitutive word should be transcendental.

A basic example : the Fibonacci binary number

The Fibonacci binary number is defined by

$$\xi_{\mathbf{f}} := \underbrace{01001}\underbrace{01001}\underbrace{0}\cdots$$

Note that the block of digits 01001 is repeated $2 + 1/5$ times.

A basic example : the Fibonacci binary number

The Fibonacci binary number is defined by

$$\xi_{\mathsf{f}} := \underbrace{01001}\,\underbrace{01001}\,\underbrace{\ 0\ }\cdots$$

Note that the block of digits 01001 is repeated $2 + 1/5$ times.

This implies that ξ_{f} is well approximated by the rational number

$$\frac{p_0}{q_0} = 0.\overline{01001} = 0.01001010010100101001\cdots.$$

More precisely,

$$\left| \xi_{\mathsf{f}} - \frac{p_0}{q_0} \right| < \frac{1}{2^9}.$$

A basic example : the Fibonacci binary number

The Fibonacci binary number is defined by

$$\xi_{\mathbf{f}} := \underbrace{01001}\,\underbrace{01001}\,\underbrace{0}\,\cdots$$

Note that the block of digits 01001 is repeated $2 + 1/5$ times.

This implies that $\xi_{\mathbf{f}}$ is well approximated by the rational number

$$\frac{p_0}{q_0} = 0.\overline{01001} = 0.0100101001010010100 1\cdots.$$

More precisely,

$$\left| \xi_{\mathbf{f}} - \frac{p_0}{q_0} \right| < \frac{1}{2^9}.$$

Using the self-similarity arising from the Fibonacci substitution σ, we obtain a full sequence of good rational approximations

$$\frac{p_n}{q_n} = 0.\overline{\sigma^n(01001)}.$$

Indeed, $\xi_{\mathbf{f}}$ also begins with the block of digits $\sigma^n(01001)\,\sigma^n(01001)\,\sigma^n(0)$.

A basic example : the Fibonacci binary number

More precisely, an easy computation allows one to show that

$$\left|\xi_{\mathbf{f}} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{2+1/5}}$$

More precisely, an easy computation allows one to show that

$$\left|\xi_{\mathbf{f}} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^{2+1/5}}$$

and Roth's theorem thus implies that $\xi_{\mathbf{f}}$ is transcendental.

Roth's Theorem. Let ξ be an algebraic real number and $\varepsilon > 0$. Then the inequality

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

has only a finite number of rational solutions p/q.

K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika, 1955.

Integer base expansions

The approach briefly outlined can actually be generalized to prove rather general results. Roth's theorem is then replaced by much stronger tools from Diophantine approximation such as the Schmidt subspace theorem.

Integer base expansions

The approach briefly outlined can actually be generalized to prove rather general results. Roth's theorem is then replaced by much stronger tools from Diophantine approximation such as the Schmidt subspace theorem.

The following result generalizes previous ones obtained in particular by Ferenczi and Mauduit and by Allouche and Zamboni.

Theorem. Let $\mathbf{a} = a_1 a_2 \ldots \in \{0, 1, \ldots, b-1\}^{\mathbb{N}}$ be a non-ultimately periodic substitutive word generated by a primitive or by a uniform substitution. Then the real number

$$\xi_{\mathbf{a}} := 0.a_1 a_2 \cdots$$

is transcendental.

B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers I. Expansions in integer bases*, Annals of Math., 2007.

Integer base expansions

The approach briefly outlined can actually be generalized to prove rather general results. Roth's theorem is then replaced by much stronger tools from Diophantine approximation such as the Schmidt subspace theorem.

The following result generalizes previous ones obtained in particular by Ferenczi and Mauduit and by Allouche and Zamboni.

Theorem. Let $\mathbf{a} = a_1 a_2 \ldots \in \{0, 1, \ldots, b-1\}^{\mathbb{N}}$ be a non-ultimately periodic substitutive word generated by a primitive or by a uniform substitution. Then the real number

$$\xi_{\mathbf{a}} := 0.a_1 a_2 \cdots$$

is transcendental.

B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers I. Expansions in integer bases*, Annals of Math., 2007.

The case of uniform substitutions confirms an old conjecture of Cobham : the base-b expansion of an algebraic irrational number cannot be generated by a finite automaton.

Integer base expansions

The approach briefly outlined can actually be generalized to prove rather general results. Roth's theorem is then replaced by much stronger tools from Diophantine approximation such as the Schmidt subspace theorem.

The following result generalizes previous ones obtained in particular by Ferenczi and Mauduit and by Allouche and Zamboni.

Theorem. Let $\mathbf{a} = a_1 a_2 \ldots \in \{0, 1, \ldots, b-1\}^{\mathbb{N}}$ be a non-ultimately periodic substitutive word generated by a primitive or by a uniform substitution. Then the real number

$$\xi_{\mathbf{a}} := 0.a_1 a_2 \cdots$$

is transcendental.

B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers I. Expansions in integer bases*, Annals of Math., 2007.

The case of uniform substitutions confirms an old conjecture of Cobham : the base-b expansion of an algebraic irrational number cannot be generated by a finite automaton.

Open problem. Prove that irrational real numbers whose base-b expansion is substitutive are transcendental.

Continued fractions

Considering approximations by quadratic numbers instead of rational approximations, the same kind of idea can be applied to some family of substitutive continued fractions.

Continued fractions

Considering approximations by quadratic numbers instead of rational approximations, the same kind of idea can be applied to some family of substitutive continued fractions.

Theorem. Let $\mathbf{a} = a_1 a_2 \dots$ be a non-ultimately periodic substitutive word generated by a primitive substitution and whose letters are positive integers. Then the real number

$$\xi_{\mathbf{a}} := [0, a_1, a_2, \dots]$$

is transcendental.

B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers II. Continued fractions*, Acta Math., 2005.

Continued fractions

Considering approximations by quadratic numbers instead of rational approximations, the same kind of idea can be applied to some family of substitutive continued fractions.

Theorem. Let $\mathbf{a} = a_1 a_2 \ldots$ be a non-ultimately periodic substitutive word generated by a primitive substitution and whose letters are positive integers. Then the real number

$$\xi_{\mathbf{a}} := [0, a_1, a_2, \ldots]$$

is transcendental.

B. Adamczewski and Y. Bugeaud, *On the complexity of algebraic numbers II. Continued fractions*, Acta Math., 2005.

Open problem. Prove that the continued fraction expansion of an algebraic real number of degree at least 3 cannot be generated by a finite automaton.

Part II. From number theory to substitutions

Classical Diophantine approximation

—

Uniform distribution and $n\alpha$ sequences

Let α be an irrational number and let us define a sequence of 1's and -1's as follows :

$$u_n = \begin{cases} 1 \text{ if } \{n\alpha\} \leq 1/2\,, \\ -1 \text{ otherwise.} \end{cases}$$

We would like to estimate as precisely as possible the sum

$$S_N(\alpha) := \sum_{n=0}^{N-1} u_n\,.$$

Let α be an irrational number and let us define a sequence of 1's and -1's as follows :

$$u_n = \begin{cases} 1 \text{ if } \{n\alpha\} \leq 1/2\,, \\ -1 \text{ otherwise.} \end{cases}$$

We would like to estimate as precisely as possible the sum

$$S_N(\alpha) := \sum_{n=0}^{N-1} u_n\,.$$

A first result. It follows from Weyl criterion that the sequence $\{n\alpha\}$ is uniformly distributed, that is

$$\frac{1}{N}\sum_{n=0}^{N-1} \chi_{[0,\beta[}(\{n\alpha\}) \to \beta\,,$$

for all $\beta \in (0,1)$.

Let α be an irrational number and let us define a sequence of 1's and -1's as follows :

$$u_n = \begin{cases} 1 \text{ if } \{n\alpha\} \leq 1/2\,, \\ -1 \text{ otherwise.} \end{cases}$$

We would like to estimate as precisely as possible the sum

$$S_N(\alpha) := \sum_{n=0}^{N-1} u_n\,.$$

A first result. It follows from Weyl criterion that the sequence $\{n\alpha\}$ is uniformly distributed, that is

$$\frac{1}{N}\sum_{n=0}^{N-1} \chi_{[0,\beta[}(\{n\alpha\}) \to \beta\,,$$

for all $\beta \in (0,1)$.

This implies that

$$\frac{S_N(\alpha)}{N} \to 0\,.$$

Let α be an irrational number and let us define a sequence of 1's and -1's as follows :

$$u_n = \begin{cases} 1 \text{ if } \{n\alpha\} \leq 1/2\,, \\ -1 \text{ otherwise.} \end{cases}$$

We would like to estimate as precisely as possible the sum

$$S_N(\alpha) := \sum_{n=0}^{N-1} u_n\,.$$

A first result. It follows from Weyl criterion that the sequence $\{n\alpha\}$ is uniformly distributed, that is

$$\frac{1}{N}\sum_{n=0}^{N-1} \chi_{[0,\beta[}(\{n\alpha\}) \to \beta\,,$$

for all $\beta \in (0,1)$.

This implies that

$$\frac{S_N(\alpha)}{N} \to 0\,.$$

Classical approach for finer results. Use the continued fraction expansion of α and the Ostrowski expansion of β.

In 1984, Rauzy suggested a completely different approach based on substitutions and dynamical systems.

In 1984, Rauzy suggested a completely different approach based on substitutions and dynamical systems.

Let $\alpha = (\sqrt{3} - 1)/2$.

In 1984, Rauzy suggested a completely different approach based on substitutions and dynamical systems.

Let $\alpha = (\sqrt{3} - 1)/2$. Let σ be the substitution defined over the alphabet $\{1, 2, 3\}$ by

$$\begin{array}{ccc} 1 & \mapsto & 13 \\ 2 & \mapsto & 13223 \\ 3 & \mapsto & 13 \end{array}$$

This substitution as a unique fixed point $\sigma^{\infty}(1)$.

In 1984, Rauzy suggested a completely different approach based on substitutions and dynamical systems.

Let $\alpha = (\sqrt{3} - 1)/2$. Let σ be the substitution defined over the alphabet $\{1, 2, 3\}$ by

$$\begin{array}{ccc} 1 & \mapsto & 13 \\ 2 & \mapsto & 13223 \\ 3 & \mapsto & 13 \end{array}$$

This substitution as a unique fixed point $\sigma^\infty(1)$. Define the substitution φ from $\{1, 2, 3\}^*$ to $\{1, -1\}^*$ by

$$\begin{array}{ccc} 1 & \mapsto & 1 \\ 2 & \mapsto & 1 - 1 - 1 \\ 3 & \mapsto & 1 - 1 \end{array}$$

In 1984, Rauzy suggested a completely different approach based on substitutions and dynamical systems.

Let $\alpha = (\sqrt{3} - 1)/2$. Let σ be the substitution defined over the alphabet $\{1, 2, 3\}$ by

$$\begin{array}{ccc} 1 & \mapsto & 13 \\ 2 & \mapsto & 13223 \\ 3 & \mapsto & 13 \end{array}$$

This substitution as a unique fixed point $\sigma^\infty(1)$. Define the substitution φ from $\{1, 2, 3\}^*$ to $\{1, -1\}^*$ by

$$\begin{array}{ccc} 1 & \mapsto & 1 \\ 2 & \mapsto & 1 - 1 - 1 \\ 3 & \mapsto & 1 - 1 \end{array}$$

Then, Rauzy proved that

$$u_n = \varphi(\sigma^\infty(1)) = 11(-1)11(-1)1(-1)(-1) \cdots .$$

In 1984, Rauzy suggested a completely different approach based on substitutions and dynamical systems.

Let $\alpha = (\sqrt{3}-1)/2$. Let σ be the substitution defined over the alphabet $\{1,2,3\}$ by

$$\begin{array}{ccc} 1 & \mapsto & 13 \\ 2 & \mapsto & 13223 \\ 3 & \mapsto & 13 \end{array}$$

This substitution as a unique fixed point $\sigma^\infty(1)$. Define the substitution φ from $\{1,2,3\}^*$ to $\{1,-1\}^*$ by

$$\begin{array}{ccc} 1 & \mapsto & 1 \\ 2 & \mapsto & 1-1-1 \\ 3 & \mapsto & 1-1 \end{array}$$

Then, Rauzy proved that

$$u_n = \varphi(\sigma^\infty(1)) = 11(-1)11(-1)1(-1)(-1)\cdots.$$

Using the Perron–Frobenius theorem, one can deduce that

$$|S_N(\alpha)| = O(\log N)$$

and even that

$$\limsup_{N\to\infty} \frac{S_N(\alpha)}{\log N} = \frac{1}{2\log(2+\sqrt{3})}.$$

Where does the substitution come from ? The proof is based on a use of the Rauzy induction for 3-interval exchange transformations and Poincaré first retrurn map.

Rauzy's approach can be generalized to describe precisely the behaviour of $S_N(\alpha)$ when α is a quadratic number.

B. Adamczewski, *Répartition des suites* $(n\alpha)$ *et substitutions*, Acta Arith., 2004.

Where does the substitution come from ? The proof is based on a use of the Rauzy induction for 3-interval exchange transformations and Poincaré first retrurn map.

Rauzy's approach can be generalized to describe precisely the behaviour of $S_N(\alpha)$ when α is a quadratic number.

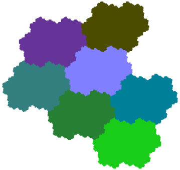
B. Adamczewski, *Répartition des suites* $(n\alpha)$ *et substitutions*, Acta Arith., 2004.

Open problem. Is it possible to use our knowledge on the Tribonacci substitution and the associated Rauzy fractal to obtain informations on sums such as

$$\sum_{n=0}^{N-1} \chi_{[0,\beta_1[\times[0,\beta_2[}(\{n\alpha\},\{n\alpha^2\}) - N\beta_1\beta_2\,,$$

where α is the unique real root of the polynomial

$$x^3 - x^2 - x - 1\,?$$



G. Rauzy, *Nombres algébriques et substitutions*, Bull. Soc. Math. France, 1982.

Rational numbers with a purely periodic β-expansion

Expansions of rational numbers in integer bases

One of the most basic results about decimal expansions is that a real number has an eventually periodic expansion if and only if it is rational.

Expansions of rational numbers in integer bases

One of the most basic results about decimal expansions is that a real number has an eventually periodic expansion if and only if it is rational.

In fact, much more is known for we can easily distinguish rationals with a purely periodic expansion : a rational number p/q in the interval $(0, 1)$, in lowest form, has a purely periodic decimal expansion if and only if q and 10 are relatively prime.

Thus, both rationals with a purely periodic expansion and rationals with a non-purely periodic expansion are, in some sense, uniformly spread on the unit interval.

Expansions of rational numbers in integer bases

One of the most basic results about decimal expansions is that a real number has an eventually periodic expansion if and only if it is rational.

In fact, much more is known for we can easily distinguish rationals with a purely periodic expansion : a rational number p/q in the interval $(0, 1)$, in lowest form, has a purely periodic decimal expansion if and only if q and 10 are relatively prime.

Thus, both rationals with a purely periodic expansion and rationals with a non-purely periodic expansion are, in some sense, uniformly spread on the unit interval.

These results extend *mutatis mutandis* to any integer base $b \geq 2$.

Expansions of rational numbers in integer bases

One of the most basic results about decimal expansions is that a real number has an eventually periodic expansion if and only if it is rational.

In fact, much more is known for we can easily distinguish rationals with a purely periodic expansion : a rational number p/q in the interval $(0, 1)$, in lowest form, has a purely periodic decimal expansion if and only if q and 10 are relatively prime.

Thus, both rationals with a purely periodic expansion and rationals with a non-purely periodic expansion are, in some sense, uniformly spread on the unit interval.

These results extend *mutatis mutandis* to any integer base $b \geq 2$.

However, if one replaces the integer b by an algebraic number that is not a rational integer, it may happen that the situation would be drastically different.

A first example

Let $\varphi := (1 + \sqrt{5})/2$.

A first example

Let $\varphi := (1 + \sqrt{5})/2$.

Every real number in $(0, 1)$ can be uniquely expanded as

$$\xi = \sum_{n \geq 1} \frac{a_n}{\varphi^n},$$

where a_n takes only the values 0 and 1, and with the additional condition that $a_n a_{n+1} = 0$ for every positive integer n.

The binary sequence $(a_n)_{n \geq 1}$ is termed the φ-expansion of ξ.

A first example

Let $\varphi := (1+\sqrt{5})/2$.

Every real number in $(0,1)$ can be uniquely expanded as

$$\xi = \sum_{n\geq 1} \frac{a_n}{\varphi^n},$$

where a_n takes only the values 0 and 1, and with the additional condition that $a_n a_{n+1} = 0$ for every positive integer n.

The binary sequence $(a_n)_{n\geq 1}$ is termed the φ-expansion of ξ.

In 1980, K. Schmidt proved the intriguing (somewhat surprising ?) result that :

every rational number in $(0,1)$ has a purely periodic φ-expansion.

A second example

The latter property seems to be quite exceptional.

Let us now consider $\theta = 1 + \varphi$.

Again, every real number ξ in $(0, 1)$ has a θ-expansion, that is, ξ can be uniquely expanded as

$$\xi = \sum_{n \geq 1} \frac{a_n}{\theta^n},$$

where a_n takes only the values 0, 1 and 2, (and with some extra conditions we do not care about here).

A second example

The latter property seems to be quite exceptional.

Let us now consider $\theta = 1 + \varphi$.

Again, every real number ξ in $(0, 1)$ has a θ-expansion, that is, ξ can be uniquely expanded as

$$\xi = \sum_{n \geq 1} \frac{a_n}{\theta^n},$$

where a_n takes only the values 0, 1 and 2, (and with some extra conditions we do not care about here).

In contrast to our first example, it was proved by Hama and Imahashi that :

no rational number in $(0, 1)$ has a purely periodic θ-expansion.

Both φ- and θ-expansions mentioned above are typical examples of the so-called β-expansions introduced by Rényi.

Both φ- and θ-expansions mentioned above are typical examples of the so-called β-expansions introduced by Rényi.

Set

$$\gamma(\beta) := \sup\{c \in [0,1) \mid \forall\, 0 \le p/q \le c,\ \ p/q \text{ has a purely periodic } \beta\text{-expansion}\}.$$

This quantity (and similar ones) have been studied by Akiyama, Berthé, Siegel...

Both φ- and θ-expansions mentioned above are typical examples of the so-called β-expansions introduced by Rényi.

Set

$$\gamma(\beta) := \sup\{c \in [0,1) \mid \forall\, 0 \leq p/q \leq c,\ p/q \text{ has a purely periodic } \beta\text{-expansion}\}.$$

This quantity (and similar ones) have been studied by Akiyama, Berthé, Siegel...

Note that with this definition, we have $\gamma(\varphi) = 1$, while $\gamma(\theta) = 0$.

Both φ- and θ-expansions mentioned above are typical examples of the so-called β-expansions introduced by Rényi.

Set

$$\gamma(\beta) := \sup\{c \in [0,1) \mid \forall\, 0 \le p/q \le c,\ \ p/q \text{ has a purely periodic } \beta\text{-expansion}\}.$$

This quantity (and similar ones) have been studied by Akiyama, Berthé, Siegel...

Note that with this definition, we have $\gamma(\varphi) = 1$, while $\gamma(\theta) = 0$.

We are interested here in those real numbers β with the curious property that all sufficiently small rational numbers have a purely periodic β-expansion, that is, such that

$$\gamma(\beta) > 0. \tag{1}$$

Both φ- and θ-expansions mentioned above are typical examples of the so-called β-expansions introduced by Rényi.

Set

$$\gamma(\beta) := \sup\{c \in [0,1) \mid \forall\, 0 \leq p/q \leq c,\ p/q \text{ has a purely periodic } \beta\text{-expansion}\}.$$

This quantity (and similar ones) have been studied by Akiyama, Berthé, Siegel...

Note that with this definition, we have $\gamma(\varphi) = 1$, while $\gamma(\theta) = 0$.

We are interested here in those real numbers β with the curious property that all sufficiently small rational numbers have a purely periodic β-expansion, that is, such that

$$\gamma(\beta) > 0. \tag{1}$$

As one could expect, Condition (1) turns out to be very restrictive. One can actually prove that such real numbers β have to be Pisot units.

Both φ- and θ-expansions mentioned above are typical examples of the so-called β-expansions introduced by Rényi.

Set

$$\gamma(\beta) := \sup\{c \in [0,1) \mid \forall\, 0 \leq p/q \leq c,\ \ p/q \text{ has a purely periodic } \beta\text{-expansion}\}.$$

This quantity (and similar ones) have been studied by Akiyama, Berthé, Siegel...

Note that with this definition, we have $\gamma(\varphi) = 1$, while $\gamma(\theta) = 0$.

We are interested here in those real numbers β with the curious property that all sufficiently small rational numbers have a purely periodic β-expansion, that is, such that

$$\gamma(\beta) > 0. \tag{1}$$

As one could expect, Condition (1) turns out to be very restrictive. One can actually prove that such real numbers β have to be Pisot units.

For quadratic numbers β, it is known that one always has either $\gamma(\beta) = 1$ or $\gamma(\beta) = 0$.

However, Akiyama proved that the situation with cubic numbers is more subtile. Indeed, he obtained the surprising result that the smallest Pisot number η, which is the real root of the polynomial $x^3 - x - 1$, satisfies $0 < \gamma(\eta) < 1$.

S. Akiyama, Pisot number and greedy algorithm in *Number Theory*, de Gruyter, Berlin, 1998.

However, Akiyama proved that the situation with cubic numbers is more subtile. Indeed, he obtained the surprising result that the smallest Pisot number η, which is the real root of the polynomial $x^3 - x - 1$, satisfies $0 < \gamma(\eta) < 1$.

S. Akiyama, Pisot number and greedy algorithm in *Number Theory*, de Gruyter, Berlin, 1998.

More precisely, it was proved that $\gamma(\eta)$ is abnormally close to the rational number $2/3$ since one has

$$\gamma(\eta) = 0.666\,666\,666\,086 \cdots .$$

This intriguing phenomenon naturally leads to ask about the arithmetic nature of $\gamma(\eta)$.

However, Akiyama proved that the situation with cubic numbers is more subtile. Indeed, he obtained the surprising result that the smallest Pisot number η, which is the real root of the polynomial $x^3 - x - 1$, satisfies $0 < \gamma(\eta) < 1$.

S. Akiyama, Pisot number and greedy algorithm in *Number Theory*, de Gruyter, Berlin, 1998.

More precisely, it was proved that $\gamma(\eta)$ is abnormally close to the rational number $2/3$ since one has

$$\gamma(\eta) = 0.666\,666\,666\,086 \cdots .$$

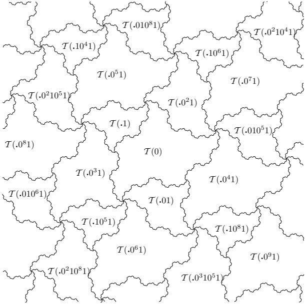
This intriguing phenomenon naturally leads to ask about the arithmetic nature of $\gamma(\eta)$.

In this direction, we proved the following result.

Theorem. The real number $\gamma(\eta)$ is irrational.

B. Adamczewski, C. Frougny, A. Siegel and W. Steiner, *Nombres algébriques et substitutions*, Bull. London Math. Soc., 2010.

Substitutive tilings associated with Pisot units

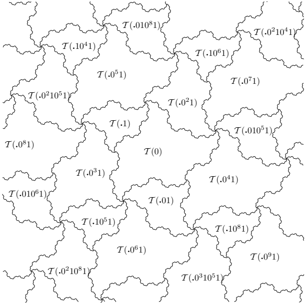


Our proof is based on a characterization of the real numbers having a purely periodic expansion given in terms of the Rauzy fractal (or central tile) associated with the Pisot unit η. This result is due to Ito and Rao (see also related works of Siegel and Berthé).

We also use the substitutive tiling associated with the smallest Pisot number η.

S. Ito and H. Rao, *Purely periodic β-expansion with Pisot base*, Proc. Amer. Math. Soc., 2005.

Substitutive tilings associated with Pisot units



Our proof is based on a characterization of the real numbers having a purely periodic expansion given in terms of the Rauzy fractal (or central tile) associated with the Pisot unit η. This result is due to Ito and Rao (see also related works of Siegel and Berthé).

We also use the substitutive tiling associated with the smallest Pisot number η.

S. Ito and H. Rao, *Purely periodic β-expansion with Pisot base*, Proc. Amer. Math. Soc., 2005.

Open problem. Prove or disprove. The number $\gamma(\eta)$ is transcendental.

Zeros of linear recurrences

Linear recurrences and zero sets

Let $\mathbb{K}$ be a field and $a(n)$ a $\mathbb{K}$-valued sequence. Then $a(n)$ satisfies a linear recurrence over $\mathbb{K}$ if there exists a natural number d and values $c_1, \ldots, c_d \in \mathbb{K}$ such that

$$a(n) = c_1 a(n-1) + c_2 a(n-2) + \cdots + c_d a(n-d)$$

for all sufficiently large values of n.

Linear recurrences and zero sets

Let $\mathbb{K}$ be a field and $a(n)$ a $\mathbb{K}$-valued sequence. Then $a(n)$ satisfies a linear recurrence over $\mathbb{K}$ if there exists a natural number d and values $c_1, \ldots, c_d \in \mathbb{K}$ such that

$$a(n) = c_1 a(n-1) + c_2 a(n-2) + \cdots + c_d a(n-d)$$

for all sufficiently large values of n.

The zero set of the linear recurrence a is defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid a(n) = 0\} \ .$$

Linear recurrences and zero sets

Let $\mathbb{K}$ be a field and $a(n)$ a $\mathbb{K}$-valued sequence. Then $a(n)$ satisfies a linear recurrence over $\mathbb{K}$ if there exists a natural number d and values $c_1, \ldots, c_d \in \mathbb{K}$ such that

$$a(n) = c_1 a(n-1) + c_2 a(n-2) + \cdots + c_d a(n-d)$$

for all sufficiently large values of n.

The zero set of the linear recurrence a is defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid a(n) = 0\} \ .$$

Examples. If $f(n)$ denotes the Fibonacci sequence, then

$$\mathcal{Z}(f) = \{0\},$$

while if $a(n) := 1 + (-1)^n$, then

$$\mathcal{Z}(a) = 2\mathbb{N} + 1 \, .$$

The Skolem–Mahler–Lech theorem

The zero set of the linear recurrence a is defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid a(n) = 0\} .$$

Theorem SML. Let a be a linear recurrence over a field of characteristic 0. Then $\mathcal{Z}(a)$ is a union of a finite set and a finite number of arithmetic progressions.

The Skolem–Mahler–Lech theorem

The zero set of the linear recurrence a is defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid a(n) = 0\} \ .$$

Theorem SML. Let a be a linear recurrence over a field of characteristic 0. Then $\mathcal{Z}(a)$ is a union of a finite set and a finite number of arithmetic progressions.

Comments.

- We can decide wether the zero set of a given linear recurrence is finite or not.

The Skolem–Mahler–Lech theorem

The zero set of the linear recurrence a is defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid a(n) = 0\} \ .$$

Theorem SML. Let a be a linear recurrence over a field of characteristic 0. Then $\mathcal{Z}(a)$ is a union of a finite set and a finite number of arithmetic progressions.

Comments.

- We can decide wether the zero set of a given linear recurrence is finite or not.
- We do not know wether one can decide if the zero set is empty or not.

The Skolem–Mahler–Lech theorem

The zero set of the linear recurrence a is defined by

$$\mathcal{Z}(a) := \{n \in \mathbb{N} \mid a(n) = 0\} \ .$$

Theorem SML. Let a be a linear recurrence over a field of characteristic 0. Then $\mathcal{Z}(a)$ is a union of a finite set and a finite number of arithmetic progressions.

Comments.

- We can decide wether the zero set of a given linear recurrence is finite or not.
- We do not know wether one can decide if the zero set is empty or not.
- All proofs use p-adic analysis at some point. This seems to the reason for which Theorem SML is not effective.

T. Tao, *Effective Skolem-Mahler-Lech theorem* in Structure and Randomness, Amer. Math. Soc., 2008.

Linear recurrences over fields of positive characteristic

If $\mathbb{K}$ denotes an infinite field of positive characteristic, then the situation is much more subtle.

If $\mathbb{K}$ denotes an infinite field of positive characteristic, then the situation is much more subtle.

Lech's example. Let

$$a(n) := (1+t)^n - t^n - 1 \in \mathbb{F}_p(t) \, .$$

One can show that the sequence a satisfies a linear recurrence while

$$\mathcal{Z}(\mathbf{a}) = \{1, p, p^2, p^3, \ldots\} \, .$$

Linear recurrences over fields of positive characteristic

If $\mathbb{K}$ denotes an infinite field of positive characteristic, then the situation is much more subtle.

Lech's example. Let

$$a(n) := (1+t)^n - t^n - 1 \in \mathbb{F}_p(t)\,.$$

One can show that the sequence a satisfies a linear recurrence while

$$\mathcal{Z}(\mathbf{a}) = \{1, p, p^2, p^3, \ldots\}\,.$$

In fact, Derksen produced more pathological examples and proved the remarkable result that the zero set of a linearly recurrent sequence can always be described in terms of automata (or p-uniform substitutions).

Theorem D. Let $a(n)$ be a linear recurrence over a field of characteristic p. Then the set $\mathcal{Z}(a)$ is a p-automatic set.

H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristic and finite automata*, Invent. Math., 2007.

Linear recurrences over fields of positive characteristic

If $\mathbb{K}$ denotes an infinite field of positive characteristic, then the situation is much more subtle.

Lech's example. Let

$$a(n) := (1+t)^n - t^n - 1 \in \mathbb{F}_p(t)\,.$$

One can show that the sequence a satisfies a linear recurrence while

$$\mathcal{Z}(\mathbf{a}) = \{1, p, p^2, p^3, \ldots\}\,.$$

In fact, Derksen produced more pathological examples and proved the remarkable result that the zero set of a linearly recurrent sequence can always be described in terms of automata (or p-uniform substitutions).

Theorem D. Let $a(n)$ be a linear recurrence over a field of characteristic p. Then the set $\mathcal{Z}(a)$ is a p-automatic set.

H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristic and finite automata*, Invent. Math., 2007.

- Each step in Derksen's proof can be made effective !

Set of vanishing coefficients in characteristic p

Remarkably, in positive characteristic an analogue of Derksen's result holds for multivariate algebraic power series.

Theorem. Let $\mathbb{K}$ be a field of characteristic $p > 0$ and let $f(t_1, \ldots, t_d) = \sum_{n_1,\ldots,n_d} a(n_1, \ldots, n_d) t_1^{n_1} \cdots t_d^{n_d} \in \mathbb{K}[[t_1, \ldots, t_d]]$ be the power series expansion of an algebraic function over $\mathbb{K}(t_1, \ldots, t_d)$. Then

$$\mathcal{Z}(f) := \{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a(n_1, \ldots, n_d) = 0\}$$

is a p-automatic subset of $\mathbb{N}^d$.

B. Adamczewski and J. Bell, *On vanishing coefficients of algebraic power series over fields of positive characteristic*, in progress.

Set of vanishing coefficients in characteristic p

Remarkably, in positive characteristic an analogue of Derksen's result holds for multivariate algebraic power series.

Theorem. Let $\mathbb{K}$ be a field of characteristic $p > 0$ and let $f(t_1, \ldots, t_d) = \sum_{n_1,\ldots,n_d} a(n_1, \ldots, n_d) t_1^{n_1} \cdots t_d^{n_d} \in \mathbb{K}[[t_1, \ldots, t_d]]$ be the power series expansion of an algebraic function over $\mathbb{K}(t_1, \ldots, t_d)$. Then

$$\mathcal{Z}(f) := \{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a(n_1, \ldots, n_d) = 0\}$$

is a p-automatic subset of $\mathbb{N}^d$.

B. Adamczewski and J. Bell, *On vanishing coefficients of algebraic power series over fields of positive characteristic*, in progress.

• We note that this immediately implies Derksen's theorem by taking $d = 1$ and taking $f(t)$ to be a rational function.

Set of vanishing coefficients in characteristic p

Remarkably, in positive characteristic an analogue of Derksen's result holds for multivariate algebraic power series.

Theorem. Let $\mathbb{K}$ be a field of characteristic $p > 0$ and let $f(t_1, \ldots, t_d) = \sum_{n_1,\ldots,n_d} a(n_1, \ldots, n_d) t_1^{n_1} \cdots t_d^{n_d} \in \mathbb{K}[[t_1, \ldots, t_d]]$ be the power series expansion of an algebraic function over $\mathbb{K}(t_1, \ldots, t_d)$. Then

$$\mathcal{Z}(f) := \{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a(n_1, \ldots, n_d) = 0\}$$

is a p-automatic subset of $\mathbb{N}^d$.

B. Adamczewski and J. Bell, *On vanishing coefficients of algebraic power series over fields of positive characteristic*, in progress.

• We note that this immediately implies Derksen's theorem by taking $d = 1$ and taking $f(t)$ to be a rational function.

• As with Derksen's proof, our result is effective.

Set of vanishing coefficients in characteristic p

Remarkably, in positive characteristic an analogue of Derksen's result holds for multivariate algebraic power series.

Theorem. Let $\mathbb{K}$ be a field of characteristic $p > 0$ and let $f(t_1, \ldots, t_d) = \sum_{n_1,\ldots,n_d} a(n_1, \ldots, n_d) t_1^{n_1} \cdots t_d^{n_d} \in \mathbb{K}[[t_1, \ldots, t_d]]$ be the power series expansion of an algebraic function over $\mathbb{K}(t_1, \ldots, t_d)$. Then

$$\mathcal{Z}(f) := \{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a(n_1, \ldots, n_d) = 0\}$$

is a p-automatic subset of $\mathbb{N}^d$.

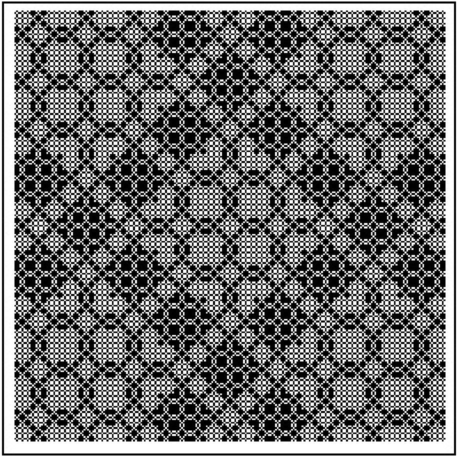
B. Adamczewski and J. Bell, *On vanishing coefficients of algebraic power series over fields of positive characteristic*, in progress.

• We note that this immediately implies Derksen's theorem by taking $d = 1$ and taking $f(t)$ to be a rational function.

• As with Derksen's proof, our result is effective.

• This result has many interesting consequences related to Diophantine equations (S-unit equations, Mordell–Lang theorem).

An example of an automatic subset of $\mathbb{N}^2$



An application : linear recurrence and decidability

As already mentioned, we do not know wether one can decide if the zero set of a given linear recurrence with rational coefficients is empty or not.

An application : linear recurrence and decidability

As already mentioned, we do not know wether one can decide if the zero set of a given linear recurrence with rational coefficients is empty or not.

Given linear recurrences $a_1(n), a_2(n), \ldots, a_d(n)$ over a field K. A general question is related to the description of the set

$$\mathcal{Z}(a_1, \ldots, a_d) := \left\{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid a_1(n_1) + a_2(n_2) + \cdots + a_d(n_d) = 0\right\} .$$

An application : linear recurrence and decidability

As already mentioned, we do not know wether one can decide if the zero set of a given linear recurrence with rational coefficients is empty or not.

Given linear recurrences $a_1(n), a_2(n), \ldots, a_d(n)$ over a field K. A general question is related to the description of the set

$$\mathcal{Z}(a_1, \ldots, a_d) := \left\{ (n_1, \ldots, n_d) \in \mathbb{N}^d \mid a_1(n_1) + a_2(n_2) + \cdots + a_d(n_d) = 0 \right\} .$$

Conjecture. If $K = \mathbb{Q}$, there exists a positive integer d such that the property

$$\mathcal{Z}(a_1, \ldots, a_d) \neq \emptyset$$

is indecidable.

An application : linear recurrence and decidability

As already mentioned, we do not know wether one can decide if the zero set of a given linear recurrence with rational coefficients is empty or not.

Given linear recurrences $a_1(n), a_2(n), \ldots, a_d(n)$ over a field K. A general question is related to the description of the set

$$\mathcal{Z}(a_1, \ldots, a_d) := \left\{ (n_1, \ldots, n_d) \in \mathbb{N}^d \mid a_1(n_1) + a_2(n_2) + \cdots + a_d(n_d) = 0 \right\} .$$

Conjecture. If $K = \mathbb{Q}$, there exists a positive integer d such that the property

$$\mathcal{Z}(a_1, \ldots, a_d) \neq \emptyset$$

is indecidable.

In contrast, we deduce from our result that this question is decidable for fields of characteristic p.