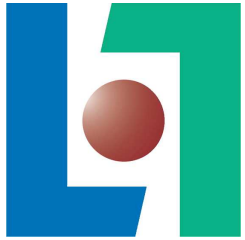

From equations to formal languages

Géraud Sénizergues

LaBRI, Bordeaux University,

Wednesday June 17th 2015

Equations are useful for studying formal languages

INTRODUCTION

Diophantine equations

Equation :

$$(P(X_1, \ldots, X_m), Q(X_1, \ldots, X_m))$$

where P, Q are polynomials with coefficients in $\mathbb{N}$.

Solution :

Integers $x_1, \ldots, x_m \in \mathbb{N}$ such that

$$P(x_1, \ldots, x_m) = Q(x_1, \ldots, x_m)$$

Words as matrices

The monoid homomorphism : $\{a, b\}^* \to \mathbb{R}^{2\times 2}$

$$a \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

is injective (known since the 1920's), with image $\mathrm{SL}_2(\mathbb{N})$.
An equality $u \cdot v = w$ for words reduces to

$$\sum_{j=1}^{2} u_{i,j} \cdot v_{j,k} = w_{i,k}$$

$$u_{1,1}u_{2,2} = u_{2,1}u_{1,2}+1, \quad v_{1,1}v_{2,2} = v_{2,1}v_{1,2}+1, \quad w_{1,1}w_{2,2} = w_{2,1}w_{1,2}+1,$$

for natural integers $u_{i,j}, v_{j,k}, w_{i,k}$.
Hence : word equations reduce to diophantine equations

Word equations

Theorem (Matiyasevich 1970)

The existence of solutions for a diophantine equation is undecidable

1- Bad start for the subject of this talk ...
2- In 1970 : bad news for the project of solving algorithmically word-equations.
Despite this,

Theorem (Makanin 1977)

The existence of solutions for a word equation is decidable

Many works have strengthened this result.
Many contributors in the audience.

Integers, words, trees

The results from

algebraic geometry, invariant theory

might be useful for

integers, words, trees.

contents

TREE-transducers

integers to integers

Definition (Polynomial recurrent sequences)

1- A *system of Linear-Polynomial-recurrent relations* is a system of the form

$$f_i(n+1) = \sum_{i=0}^{m} c_i(n) f_i(n)$$

where m is an integer and c_i are polynomial functions of n, with coefficients in $\mathbb{Q}$.

2- A *system of Polynomial recurrent relations* is a system of the form

$$f_i(n+1) = P_i(f_1(n), f_2(n), \ldots, f_m(n)) \text{ for all } i \in [1, m]$$

where m is an integer and P_i are polynomial with coefficients in $\mathbb{Q}$ over m undeterminates.

integers to integers

Theorem

The equivalence problem is decidable for two sequences defined by polynomial recurrences.

Linear Polynomial recurrences :
[Salvy-Zimmerman Gfun Package, 1994]
Polynomial recurrences :
[G.Sénizergues ICALP'99],[Honkala TCS'00],[G.S. CSR'07]

integers to integers

Sketch of proof.
Question (v1) : $\forall n \in \mathbb{N}, f_1(n) = 0$?
We define polynomials $P_{i,n} \in \mathbb{C}[X_1, \ldots, X_m]$ by :

$$P_{i,0} = X_i, \quad P_{i,n+1} = P_i \circ (P_{1,n}, \ldots, P_{m,n})$$

so that

$$f_i(n) = P_{i,n}(f_1(0), \ldots, f_m(0)).$$

Consider the ideals :

$$I_n := \langle \{P_{1,k} \mid 0 \leq k \leq n\} \rangle$$

integers to integers

The sequence of ideals :

$$I_0 \subseteq I_1 \subseteq \ldots I_n \subseteq I_{n+1} \subseteq \ldots$$

must be ultimately constant :
we note

$$I_\infty = \bigcup_{n \geq 0} I_n$$

Question (v2) :

$$\forall P \in I_\infty, P(f_1(0), \ldots, f_m(0)) = 0?$$

integers to integers

Step 1 : There exists an integer k such that $I_k = I_{k+1}$.
By Buchberger's theorem it can be computed.
Step 2 : If $I_k = I_{k+1}$, then, for every $r \geq 0$, $I_{k+r} = I_{k+r+1}$:

$$\begin{aligned} P_{1,k+r+1} &= P_{1,k+1} \circ (P_{1,r}, \ldots, P_{m,r}) \\ &= (\sum_{i=0}^{k} U_i \cdot P_{1,i}) \circ \vec{P}_{*,r} \\ &= \sum_{i=0}^{k} (U_i \circ \vec{P}_{*,r}) \cdot (P_{1,i} \circ \vec{P}_{*,r}) \\ &= \sum_{i=0}^{k} (U_i \circ \vec{P}_{*,r}) \cdot P_{1,i+r} \\ &\in I_{k+r}. \end{aligned}$$

words to integers

Definition (Polynomial recurrent sequences)

A system of Polynomial recurrent relations over the alphabet $\mathbb{A}$ is a system of the form

$$f_i(aw) = P_{i,a}(f_1(w), f_2(w), \ldots, f_m(w)) \text{ for } i \in [1, m], a \in \mathbb{A}$$

where m is an integer and $P_{a,i}$ are polynomial with coefficients in $\mathbb{Q}$ over m undeterminates.

Theorem

The equivalence problem is decidable for two maps $\mathbb{A}^* \to \mathbb{Q}$ defined by polynomial recurrences.

Same kind of proof and references.

trees to integers

Definition (Polynomial trees-to-integers recurrent maps)

A system of polynomial recurrent relations over the graded alphabet $\mathbb{A}$ is a system of the form

$$f_i(a(t_1, t_2)) = P_{i,a}(f_1(t_1), \ldots, f_m(t_1), f_1(t_2), \ldots, f_m(t_2))$$

$$\text{for } i \in [1, m], a \in \mathbb{A}$$

where m is an integer and $P_{i,a}$ are polynomial with coefficients in $\mathbb{Q}$ over $2m$ undeterminates.

For simplicity we assume all symbols of $\mathbb{A}$ have arity 2 except a symbol $\perp$ with arity 0.
Example : $\mathbb{A} = \{x, y, z, \perp\}$

$$t = x(y(\perp, x(\perp, \perp)), z(\perp, \perp)).$$

trees to integers

Theorem

The equivalence problem is decidable for two trees-to-integers maps $\mathbb{A}^* \to \mathbb{N}$ *defined by polynomial recurrent relations and initial values.*

[H.Seidl,S.Maneth,G.Kemper arxiv 2015]

trees to integers : the proof

$$\mathbb{I} := \{P \in \mathbb{Q}[X_1, \ldots, X_m] \mid \forall t \in T(\mathbb{A}), P(\vec{f}(t)) = 0\}$$

(the ideal of polynomials that vanish on $\mathrm{Im}(f)$).

Proposition

If $f_1 = 0$ *then*

1- $X_1 \in \mathbb{I}$.

2- $\forall P \in \mathbb{I}, P(\vec{f}(\perp)) = 0$

3- $\forall P \in \mathbb{I}, \forall a \in \mathbb{A}, P \circ \vec{P}_{*,a} \in \left\langle \mathbb{I}[\vec{X}] \cup \mathbb{I}[\vec{Y}] \right\rangle$.

Note $\mathbb{I} \subseteq \mathbb{Q}[X_1, \ldots, X_m]$.
$\mathbb{I}[\vec{Y}]$ means : $\{P[Y_1/X_1, \ldots, Y_m/X_m] \mid P \in \mathbb{I}\}$.
If f_1 is really null over all terms, points (1)(2) are true.
Point (3) leans on next lemma.

trees to integers :the proof

$$I(V_1 \times V_2) := \{P \in \mathbb{Q}[\vec{X}, \vec{Y}] \mid \forall \vec{v_1} \in V_1, \vec{v_2} \in V_2, P(\vec{v_1}, \vec{v_2}) = 0\}$$

Lemma

Let $V_1 \subseteq K^m, V_2 \subseteq K^m$. *Then*
$I(V_1 \times V_2) = \left\langle I(V_1)[\vec{X}] \cup I(V_2)[\vec{Y}] \right\rangle$

Proof : use Gröbner bases G_1 (resp. G_2) for V_1 (resp. V_2) in order to show that

$$I(V_1 \times V_2) \subseteq \left\langle I(V_1)[\vec{X}] \cup I(V_2)[\vec{Y}] \right\rangle.$$

This lemma proves point (3).

trees to integers :the proof

Proposition

If there exists some ideal $I \subseteq \mathbb{Q}[X_1, \ldots, X_m]$ *such that*
1- $X_1 \in I$.
2- $\forall P \in I, P(\vec{f}(\perp)) = 0$
3- $\forall P \in I, \forall a \in \mathbb{A}, P \circ \vec{P}_{*,a} \in \left\langle I(\vec{X}) \cup I(\vec{Y}) \right\rangle$.
then $f_1 = 0$

Proof : structural induction over terms.

trees to integers :the proof

The problem $f_1 = 0?$ is thus :
- co-semi-decidable : just find a tree $t \in T(\mathbb{A})$ such that $f_1(t) \neq 0$
- semi-decidable : find an ideal I fulfilling points (1)(2)(3) of Lemma 6.

Hence this problem is decidable

trees to words

Definition (trees-to-words top-down deterministic transductions)

A tree-to-words top-down deterministic transduction, over the graded alphabet $\mathbb{A}$ into the alphabet $\mathbb{B}$, is a map $f_1 : T(\mathbb{A}) \to \mathbb{B}^*$ fulfilling a system of the form

$$f_i(a(t_1, t_2)) = \prod_{j=1}^{\ell(i,a)} f_{\alpha(i,a,j)}(t_{\beta(i,j)}) \text{ for all } i \in [1, m], a \in \mathbb{A}$$

where m is an integer, $\ell(i, a)$ is an integer, $\alpha(i, a, j) \in [1, m]$ and $\beta(i, j) \in \{1, 2\}$.

trees to words

Theorem

The equivalence problem is decidable for two trees-to-words maps $T(\mathbb{A}) \to \mathbb{B}^*$ defined by top-down deterministic transductions.

Proof : Use the faithful representation from slide 4 : reduces the problem to trees-to-integers maps defined by polynomial recurrent relations and initial values.

trees to trees

Definition (trees-to-trees top-down deterministic transductions)

A trees-to-trees top-down deterministic transduction, over the graded alphabet $\mathbb{A}$, is a map $f_1 : T(\mathbb{A}) \to T(\mathbb{A})$ fulfilling a system of the form

$$f_i(a(t_1, t_2)) = T_{i,a}[f_*(\vec{t}_1)/\vec{u}, f_*(\vec{t}_2)/\vec{v}]) \text{ for all } i \in [1, m]$$

where m is an integer, $u_1, \ldots, u_m, v_1, \ldots, v_m$ are variables and $T_{i,a} \in T(\mathbb{A}, u_1, \ldots, u_m, v_1, \ldots, v_m)$.

trees to trees

Theorem

The equivalence problem is decidable for two trees-to-trees maps $T(\mathbb{A}) \to T(\mathbb{A})$ defined by top-down deterministic transductions.

Proof : use the representation of trees by words (prefix polish notation).

Quantum WORD-automata

finite Q-automata

Let d be an integer, $d \geq 1$.
Let $\mathbb{H} := \mathbb{C}^d$ be the hilbert space of dimension d (over $\mathbb{C}$).
A Finite Quantum Automaton $\mathbb{A}$ is given by :
- an homomorphism $\mu : \mathbb{A}^* \to U(d)$
- an initial vector $I \in \mathbb{H}$ with norm 1
- a terminal vector $T \in \mathbb{H}$ with norm 1

Given a number $\lambda \in \mathbb{R}$ (called the threshold), we set :

$$\mathrm{L}(\mathbb{A}, \lambda) := \{w \in \mathbb{A}^* \mid |\langle I|\mu(w)T\rangle| > \lambda\}$$

Physically : after the evolution of the system controlled by w, the *probability* that some observable has the value t corresponding to the eigenvector I is $> \lambda^2$.

languages

N.B.1 Such languages are, in general, not rational.
N.B.2 If the threshold is *isolated*, then $\mathrm{L}(\mathbb{A}, \lambda)$ is rational
[Bertoni DLT 2003]

Theorem

The emptiness problem is decidable for Quantum Finite Automata.

[Blondel,Jeandel,Koiran,Portier SIAM J. on Comput. 2005]
N.B.3 :
- rationality for isolated threshold is true for *stochastic* automata
- decidability of emptiness fails for *stochastic* automata

Q-languages : emptiness problem

Reformulation 1 :

$$\forall w \in \mathbb{A}^*, \mu(w) \in S?$$

where S is the set :

$$\{M \in \mathbb{C}^{d^2}, |\langle I|MT\rangle|^2 \leq \lambda^2\}$$

Note S is semi-algebraic within $\mathbb{R}^{2d^2}$.

Q-languages :emptiness problem

Note S is closed (for the euclidean topology). Let

$$G := \overline{\langle \{\mu(a) \mid a \in \mathbb{A}\} \rangle}$$

the closed subgroup generated by the matrices $\mu(a)$.
Reformulation 1 :

$$G \subseteq S?$$

Q-languages :emptiness problem

Theorem

Every compact subgroup G of $\mathrm{GL}_n(\mathbb{R})$ is algebraic.

[Mneimné-Testard Introduction à la théorie des groupes de Lie classiques, 1986].

This means : there exists finitely many polynomials $P_1, \ldots, P_n$ over the undeterminates $X_{i,j}$,$(i,j) \in [1,n] \times [1,n])$ such that, for every matrix $M = (m_{i,j})$

$$M \in G \Leftrightarrow P_k(\ldots, m_{i,j}, \ldots) = 0 \quad \text{for all } k \in [1,n].$$

Remark 1 : $U(d) \subseteq \mathrm{GL}_{2d}(\mathbb{R})$.

Remark 2 : can be rephrased as : every compact subgroup G of $\mathrm{GL}_n(\mathbb{R})$ is Zariski-closed in $\mathbb{R}^{n^2}$.

Q-languages :emptiness problem

Theorem

Given a finite set $M_1, \ldots, M_m$ of invertible matrices of dimension n over a field $\mathbb{K}$, one can compute a finite set of polynomials P_k over $\mathbb{K}$ such that,

$$I(\langle\{M_1, \ldots, M_m\}\rangle) = \langle P_1, \ldots, P_r\rangle$$

[Derksen,Jeandel,Koiran J. Symbolic Comput. 2005].
i.e. the Zariski-closure of a finitely generated group of matrices can be computed.
Reformulation 2 :

$$\forall m_{i,j} \in \mathbb{R}, \vec{m} \in Z(\langle P_1, \ldots, P_r\rangle) \Rightarrow \vec{m} \in S?$$

By Tarski's theorem (on $\mathrm{FOL}(\mathbb{R}, +, \times)$) this is decidable.

Q-gates :universality problem

Let $\mathcal{G} = \{g_1, \ldots, g_m\}$ be a set of " quantum -gates" i.e. unitary matrices.
It is called universal if, there exists some integer $k \geq 1$ such that, for every $n \geq k$, every unitary matrix $U \in \mathrm{U}(n)$ is the limit of "circuits over the set $\mathcal{G}$".
This means : the closed subgroup generated by all the matrices $\mathrm{Id}_p \otimes g \otimes \mathrm{Id}_q$ (with $p \cdot d(g) \cdot q = n$) equals $\mathrm{U}(n)$.

Theorem

Universality of a finite set of Q-gates with rational (or algebraic) coefficients is decidable.

[Blondel,Jeandel,Koiran,Portier SIAM J. on Comput. 2005].
Above method for a given k (now $S = \mathrm{U}(k)$).
Since there is a universal set with $k = 8$ [Kitaev and alii 1997], it suffices to test the property for this dimension only.

Context-free WORD-grammars

generating series

For every $L \subseteq \mathbb{A}^*$, the generating series of L is :

$$S_L := \sum_{n \geq 0} a_n X^n$$

where $a_n := \text{Card}(\{w \in \mathbb{A}^* \mid w \in L \text{ and } |w| = n\})$.
Let us consider a c.f. grammar G over the terminal alphabet $\mathbb{A}$, and v_1 a non-terminal of G.

Theorem

1- If the grammar G is non-ambiguous, then the generating series $S(G, v_1)$ of the language $L(G, v_1)$ is algebraic over $\mathbb{Q}(X)$.
2- From the grammar G, one can compute the minimal polynomial P of the generating series of $L(G, v_1)$

Point 1 : [Chomsky-Schutzenberger 1963]
Point 2 : [Kuich-Salomaa Semi-rings,Automata,Languages,1986].

generating series is holonomic

Theorem

If S is an algebraic power series (over $\mathbb{K}(X)$), then S is holonomic.

[Comtet R.E.M. 1964]
Constructive proof : from the minimal polynomial of S one can compute a differential equation with polynomial coefficients, that S satisfies.

Corollary

If $S = \sum a_n X^n$ is an algebraic power series, then $(a_n)_{n\in\mathbb{N}}$ fulfills a LP-recurrence (linear recurrence with polynomial coefficients).

N.B. From the minimal polynomial of S
–> differential equation
– >LP-recurrence.

equivalence problem

Theorem

Let G be a non-ambiguous cf grammars and v_1, v_2 two non-terminals. Let us assume that $L(G, v_1) \subseteq L(G, v_2)$. Then one can decide whether

$$L(G, v_1) = L(G, v_2)?$$

equivalence problem

Algorithm :

Compute the min. pols P_1 (resp. P_2) of S_{L_1} (resp. S_{L_2})
IF $P_1 \neq P_2$
    RETURN NO
ELSE
  FOR $n = 0 \rightarrow \deg(P_1) - 1$
    $a_n := \mathrm{Card}(\{w \in \mathbb{A}^* \mid w \in L(G, v_1) \text{ and } |w| = n\})$
    $b_n := \mathrm{Card}(\{w \in \mathbb{A}^* \mid w \in L(G, v_2) \text{ and } |w| = n\})$
  IF $\exists n \in [0, deg(P_1) - 1], a_n \neq b_n$
    RETURN NO
  ELSE
    RETURN YES

equivalence problem

Corollary

Let G be a non-ambiguous cf grammar, v a non-terminal and R a right-linear grammar. One can decide whether

$$L(R) \subseteq L(G)?$$

[Salomaa-Soittola Theoretic Aspects of Formal Power Series, sec IV.5 1983]

Algorithm :

0- Make R non-ambiguous (or even deterministic).

1- Compute a non-ambiguous grammar for $L(G) \cap L(R)$

2- Test whether $S_{L(G)\cap L(R)} = S_{L(G)}$?

inherently ambiguous languages

Application : generate examples of context-free inherently ambiguous languages.

Principle : build a c.f. language L where the following problem is undecidable
INPUT : a right-linear grammar R
QUESTION : $\mathrm{L}(R) \subseteq L$?

inherently ambiguous languages

Construction :

- start from a Turing machine T that enumerates a non-recursive set S
- encode T into a g.s.m. g such that the word

$$g^{\omega}(a) = \#u_0\#u_1\#\ldots\#u_n\ldots$$

  is the sequence of all configurations of T starting on u_0
- by [Berstel IPL, 1986], $L := \mathbb{A}^* - Pref(w)$ is co-context-free
- $R \subseteq (\mathbb{A}^* - Pref(w))$ is undecidable
  argument : you can formulate $u \in S$ as the inclusion

$$\mathbb{A}^*\#uq_F\# \subseteq (\mathbb{A}^* - Pref(w))?$$

- hence L is context-free, inherently ambiguous.

inherently ambiguous languages

N.B.1 the generating series $S(L)$ is rational over $\mathbb{Q}(X)$.
Our argument is based on undecidability
N.B.2 transcendence of the commutative, multivariate generating series $S(L)(a_1, \ldots, a_m)$ is proved in [Autebert,Flajolet,Gabarro IPL 1987]