

Some Words about Word Equations

Volker Diekert
University of Stuttgart

MOSCA'19: Meeting on String Constraints and Applications

May 6-9, 2019
Bertinoro international Center for informatics (BiCi)
University Residential Center
Bertinoro (Forlì-Cesena), Italy

May 6, 2019

Part I. A brief history of word equations

Early “Algebraic” undecidability results

Dehn (1912): The word problem of orientable surface groups is decidable (in linear time).

$$G = \langle a_1, b_1, \dots, a_g, b_g \rangle / [a_1, b_1] \cdots [a_g, b_g] = 1.$$

Early “Algebraic” undecidability results

- Post Correspondence Problem.

Given a finite set A and two homomorphisms $f : A^+ \rightarrow \{0, 1\}^+$ and $g : A^+ \rightarrow \{0, 1\}^+$. Is there a word $w \in A^+$ such that $f(w) = g(w)$?

- Word Problem in a finitely presented monoid (Post 1947).

One can construct a finitely presented monoid M (generated by two elements a, b) such that the following problem is undecidable: Given $u, v \in \{0, 1\}^+$, do we have $u = v$ in the monoid M .

The corresponding problem for finitely presented groups was shown to be undecidable by Novitkov and Boone in the late 1950s, only. Proofs are much harder.

Logic: *Gödel versus Tarski: The elementary theory over \mathbb{N} is undecidable (Gödel 1931), but decidable over reals \mathbb{R} (Tarski 1948).*

Word equations in monoids with a decidable word problem

Let M be a finitely generated semigroup (monoid, group) with generating set A and Ω be a set of variables.

A *system of word equations* over M is a set

$$\mathcal{S} = \{ U_i = V_i \mid U_i, V_i \in (A \cup \Omega)^*, i \in S \}.$$

A *solution* is given by a substitution $X \mapsto \sigma(X) \in M$ for variables X such that $\sigma(U_i) = \sigma(V_i)$ becomes an identity in M for all $i \in S$.

WORDEQUATION

On input M and \mathcal{S} decide whether \mathcal{S} has a solution σ .

Special instances:

- A single equation $U=V$.
- Linear Diophantine equations over \mathbb{N}^k or \mathbb{Z}^k .
- Equations over free monoids and free groups.

WORDEQUATION is a special instance of HILBERT10

- Matiyasevich 1970: HILBERT10 is undecidable (based on Davis, Putnam, Robinson)
- Makanin 1977: WORDEQUATION in free monoids is decidable.
- Makanin 1982/84: WORDEQUATION in free groups is decidable.
- Matiyasevich 1996 and D., Matiyasevich, Muscholl 1997: WORDEQUATION in free partially commutative monoids (= trace monoids) is decidable.
- Plandowski 1999: WORDEQUATION is in PSPACE.
- D., Hagenah, Gutiérrez 2001: WORDEQUATION in free groups with rational constraints is PSPACE complete.
- D., Muscholl 2002: WORDEQUATION in free partially commutative groups (= RAAGs) with normalized regular constraints is in PSPACE.
- Lohrey-Sénizergues 2006 and Dahmani-Guirardel 2010: WORDEQUATION in f.g. virtually free (= context-free) groups is decidable. No concrete complexity bound!
- Jež 2013: $\text{WORDEQUATION} \in \text{NSPACE}(n \log n)$ with a proof from THEBOOK!
- D., Elder 2017: WORDEQUATION in virtually free groups is in PSPACE.

Hilbert Tenth Problem

Hilbert's address at the International Congress of Mathematicians 1900 in Paris:

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: Man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen Zahlen lösbar ist.

That is: Hilbert asked whether the following H_{10} set is decidable?

$$\text{HILBERT}_{10} = \{ P(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n] \mid \exists x_1, \dots, x_n \in \mathbb{Z} : P(x_1, \dots, x_n) = 0 \}$$

Word equations and Diophantine problems

$$\mathrm{SL}(2, \mathbb{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{N} \wedge ad - bc = 1 \right\}.$$

Let $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Fact: $\mathrm{SL}(2, \mathbb{N}) = \{U, L\}^*$ is a free monoid with 2 generators¹

¹. Karp-Rabin used this fact 1987 for fast randomized pattern matching.

From WORDEQUATION to HILBERT10

Translation of an equation $Z = XY$ with variables X, Y, Z over $\{U, L\}^*$ into a

Diophantine problem: $\begin{pmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{pmatrix} = \begin{pmatrix} X_1 & X_2 \\ X_3 & Y_4 \end{pmatrix} \begin{pmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{pmatrix}$.

$$Z_1 = X_1 Y_1 + X_2 Y_3$$

$$Z_2 = X_1 Y_2 + X_2 Y_4, \quad Z_3 = \dots, \quad Z_4 = \dots$$

$$1 = X_1 X_4 - X_2 X_3, \quad 1 = Y_1 Y_4 - Y_2 Y_3, \quad 1 = Z_1 Z_4 - Z_2 Z_3,$$

$$X_i = A_i^2 + B_i^2 + C_i^2 + D_i^2, \text{ etc by Lagrange}$$

Direct Consequence.

WORDEQUATION in free monoids \leq WORDEQUATION in $SL(2, \mathbb{Z}) \leq$ HILBERT10.

Since $SL(2, \mathbb{Z})$ contains a free subgroup of rank 2, we also see:

WORDEQUATION in free groups \leq WORDEQUATION in $SL(2, \mathbb{Z})$ with constraints.

Existential theory with Constraints

Regular Constraints.

- Atomic formulas: $U=V$ with $U, V \in (A \cup \Omega)^*$.
- Predicates $X \in R$ with $X \in \Omega$ and $R \in \text{REG}(A)$.
- Boolean connectives: \wedge, \vee, \neg etc.

$\{\exists X_1, \dots, \exists X_k : \Phi(X_1, \dots, X_k) = \text{true}\}$

Schulz (1990, LNCS 572)

The existential theory of word equations with regular constraints is decidable.

His proof used Makanin and the fact that $\text{REG}(A) = \text{REC}(A)$.

For any monoid: $L \in M$ is recognizable (that is in $\text{REC}(M)$) if there is a homomorphism $h : M \rightarrow N$ such that $|N| < \infty$ and $h^{-1}(h(L)) = L$.

From word equations with length predicates

Proposition [Durnev (1974), Büchi-Senger (1988)]

Let $A = \{a, b\}$. The existential theory (of equations) in A^* together with length predicates $|X|_a = |Y|_a$ and $|X|_b = |Y|_b$ is undecidable.

Proof

Reduction of HILBERT10.

Open Problem

What about the existential theory (of equations) in A^* together with a single length predicate: $|X| = |Y|$?

String graphs

Concurrency: How to model it algebraically? Trace equations

There are *interleaving models*: $ab = ba$; and Petri nets (they claim for true concurrency) $(a, b) \in I$, then a and b can be executed in parallel.

Algebraic simplification.

Given a finite undirected graph (A, I) , then the *trace monoid* is the free monoid V^* with defining relations $ab = ba$ for all $ab = ba$. The notation I refers to independence.

$$M(A, I) = A^* / \{ ab = ba \mid ab = ba \}.$$

Traces describe runs where the execution of *independent* events can be done in parallel.

Hence: in any order.

Solving trace equations is more demanding than solving word equations, and requires to study equations with regular constraints to express independence.

Solving trace equations turned out be crucial for solving the string graph embedding problem of surfaces.

This is a surprising application as far as possible from concurrency?

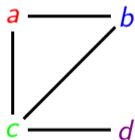
String graphs

Vertices are curves in the plane and edges may cross..

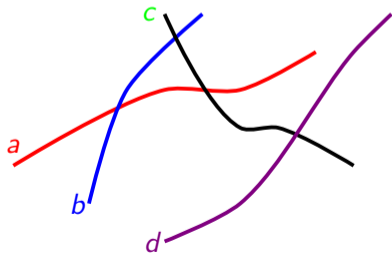
The notion of *string graph* appeared 1966 in a paper by Sinden on circuit layout.

Graham (1976): Given an abstract graph. Can we decide whether it is a string graph.

Graph



Realization as an intersection graph of curves

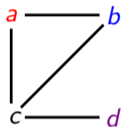


String graph recognition

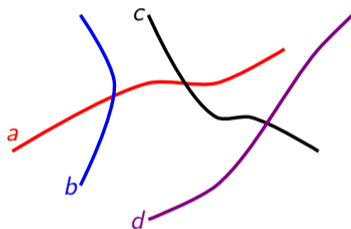
Weak realization of a string graph

The *String Graph Recognition Problem* is reducible to the *Weak Realization Problem*.

Graph



Weak realization as an intersection graph of curves.



Let S be a compact orientable surface with boundary, for example $S = [0, 1] \times [0, 1] \subseteq \mathbb{R}^2$ where the position of the vertices are fixed: $V \subseteq S$.

- ▶ Given a graph $G = (V, E)$ and a relation $R \subseteq E \times E$.
- ▶ Can we embed G such that if e, f cross, then $(e, f) \in R$?

In the picture: $(b, c) \in E$ but b and c do not intersect.

String graphs and word equations

Theorem (Schaefer, Sedgwick, Štefankovič, STOC 2002)

Recognizing string graphs in the plane is NP-complete.

Proof uses a reduction to word equations with given lengths for the solution.

Theorem (Schaefer, Sedgwick, Štefankovič, JCSS 2004)

Recognizing string graphs on any compact surface is in PSPACE.

The proof uses a reduction to quadratic trace equations with involution. Quadratic trace equations with involution are easy to solve in PSPACE by D., Kufleitner (DLT 2002).

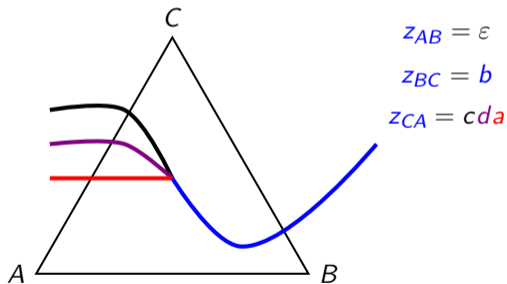
Trace equations are word equations modulo some partial commutation. We need an *involution*, which corresponds to the orientation of faces and edges.

$$\overline{a_1 \cdots a_n} = \overline{a_n \cdots a_1}$$

This means: Read words (or traces) from right-to-left

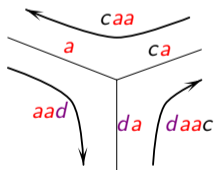
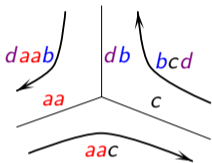
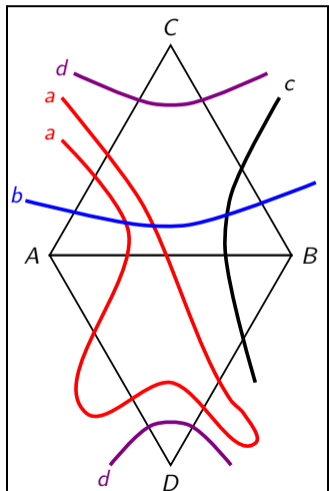
From string graphs to trace equations: Proof ingredients

1. Triangulate a big triangle, such that vertices are inside distinguished small triangles.
2. At most one vertex is present in this triangle.
3. The strings are leaving in some order via some edge.
4. All crossings between strings are inside triangles without vertices.



String graph recognition

Equations modulo partial commutation



$$aac = aa\bar{c}$$
$$bcd = c\bar{d}\bar{b}$$
$$daab = db\bar{a}\bar{a}$$

$$aac = \bar{c}aa$$

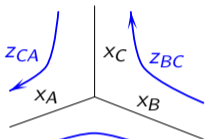
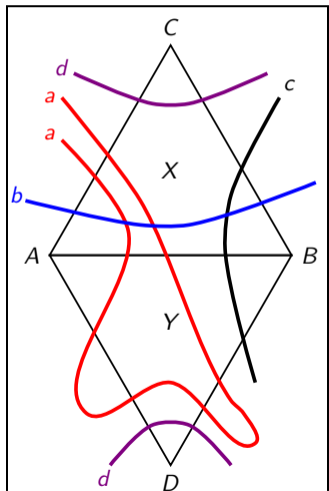
$$caa = ca\bar{a}$$
$$aad = a\bar{d}\bar{a}$$
$$daac = da\bar{c}\bar{a}$$

$$(a, b) \in I$$

$$(b, c) \in I$$

String graph recognition

From string graphs to trace equations

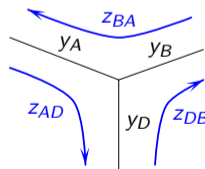


$$z_{AB} = x_A \overline{x_B}$$

$$z_{BC} = x_B \overline{x_C}$$

$$z_{CA} = x_C \overline{x_A}$$

$$z_{AB} = \overline{z_{BA}}$$



$$z_{BA} = y_B \overline{y_A}$$

$$z_{AD} = y_A \overline{y_D}$$

$$z_{DB} = y_D \overline{y_B}$$

Part III. Solving quadratic equations

Matiyasevich 1968: QuadraticWordEquation is NSPACE(n).

A *quadratic word equation* is a word equation where every variable appears at most twice.

- $aXaaXYbZ = Y$ is quadratic.
- $aXaaXX = YY$ is not quadratic because X appears three times.

Matiyasevich's algorithm for solving quadratic equations makes deterministic choices and nondeterministic guesses which transform the equation without making it longer.

Soundness: The algorithm never transforms any unsolvable equation into a solvable one.

Completeness: If the equation is solvable, then there is a sequence of (non-)deterministic choices to a trivially solvable equation.

Example

$$\begin{array}{cccc} X & X & Y & Z \\ baa & baa & aba & a \end{array} = \begin{array}{cccc} ba & Y & a & Z \\ ba & aba & a & a \end{array} \begin{array}{c} baa \\ baa \end{array}$$

- 1 $|X| \leq 1$ is impossible. (Why?)
- 2 Rewrite $X = baX$ and obtain $baXbaXYZ = baYaZbaa$. Length increases by 4.
- 3 Cancel ba on the left and obtain $XbaXYZ = YaZbaa$.
Length decreases by 4. Thus, we are back at the original length!
- 4 Guess $X \leq Y$ and rewrite $Y = XY$.
- 5 Obtain $XbaXXYZ = XYaZbaa$. Length increases by 2.
- 6 Cancel X on the left and obtain $baXXYZ = YaZbaa$.
Length decreases by 2. Thus, we are back at the original length!
- 7 Guess $Y = ba$. Obtain $baXXbaZ = baaZbaa$.
- 8 Cancel ba the left and obtain the shorter equation $XXbaZ = aZbaa$.
- 9 This forces $X = a$ and $Z = a$ which is a solution.

Solving quadratic systems: High level description

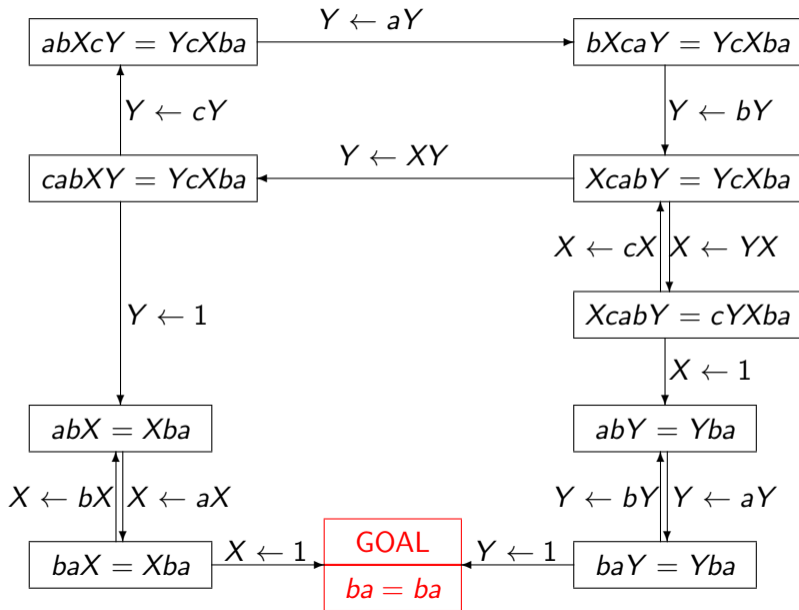
1. Replace some (or none) variables X by the empty word.
2. **Hence:** Search for solution with $X \neq 1$, only.
3. We may assume that the first equation is either of the form

$$\begin{array}{l} X \dots = a \dots \quad \text{with } X \in \Omega, a \in A \\ \text{or } X \dots = Y \dots \quad \text{with } X \in \Omega, Y \in \Omega, X \neq Y. \end{array}$$

Moreover, $|X| \geq \max\{1, |Y|\}$.

4. Either write $X = aZ$ or $X = YZ$, where Z is a new variable.
5. Replace all X by aZ or YZ respectively.
6. New system where X does not occur any more and Z occurs at most twice.
7. Cancel either a or Y on the left of the first equation.

Search Graph for $abXcY = YcXba$



Rational subsets are everywhere

A *nondeterministic finite automaton* (NFA) over a monoid M is a finite directed graph \mathcal{A} with initial and final states where the arcs are labeled with elements of M . Reading the labels of paths from initial to final states defines the *accepted language* $L(\mathcal{A}) \subseteq M$.

Definition

$L \subseteq M$ is *rational* if $L = L(\mathcal{A})$ for some NFA.

- Rational = regular for f.g. free monoids.
- In general, rational sets are **not closed under intersection**.

All solutions are given by an NFA over the endomorphisms over $(A \cup \Omega)^*$

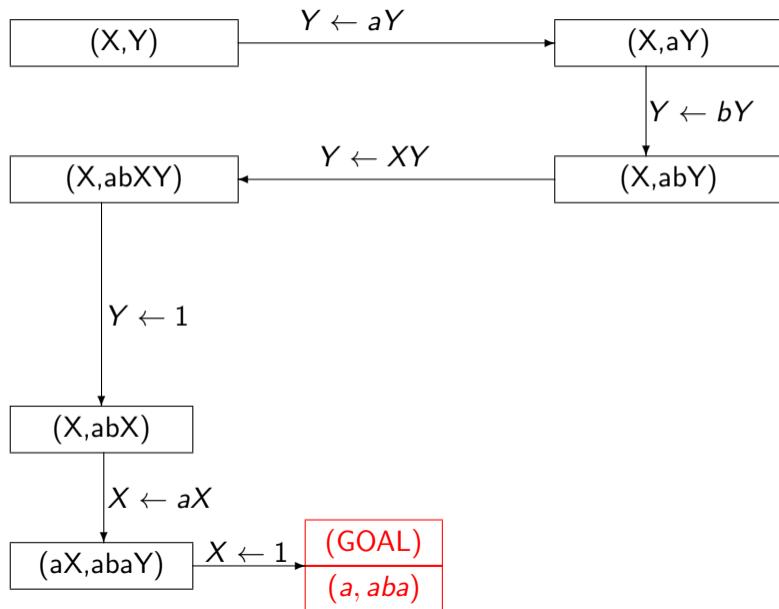
More precisely:

- 1 Let $\text{End}_A((A \cup \Omega)^*)$ denote the monoid of endomorphisms over $(A \cup \Omega)^*$ which leave the letters of A invariant. Thus, an endomorphism $h \in \text{End}_A((A \cup \Omega)^*)$ is the same as a mapping $h : \Omega \rightarrow A \cup \Omega^*$. This in turn is the same as a *deterministic table*: for each $X \in \Omega$ there is exactly one table entry which is the word $h(X)$.
- 2 Let $X \leftarrow w$ denote the endomorphism $h \in \text{End}_A((A \cup \Omega)^*)$ such that $h(X) = w$ and $h(y) = y$ for all $X \neq y \in A \cup \Omega$.
- 3 Read the search graph as an NFA \mathcal{A} where the initial state is the initial equation and the *Goal* is the final state. That is the state without variables.
- 4 We obtain $L(\mathcal{A}) \subseteq \text{End}_A((A \cup \Omega)^*)$.

If we apply endomorphisms on the right, then we write $(X)hg$. Thus, $(X)hg = hg(X)$ in traditional notation. We obtain:

$$\{ (\sigma(X), \sigma(Y) \mid \sigma \text{ solves the quadratic equation} \} = \{ ((X)h, (Y)h \mid h \in L(\mathcal{A}) \}.$$

An accepting path for the equation $abXcY = YcXba$



EDT0L languages

EDT0L refers to **E**xtended, **D**eterministic, **T**able, **0** interaction, and **L**indenmayer system.

See: The Book of **L** (Springer, 1986).

EDT0L languages via a “rational control” due to Asveld (1977).

Definition

A relation $R \subseteq A^* \times \dots \times A^*$ is a *EDT0L* if there is an extended alphabet C with $A \subseteq C$, symbols $c_1, \dots, c_k \in C$, and a rational set of endomorphisms $R \subseteq \text{End}(C^*)$ such that

$$L = \{ (h(c_1), \dots, h(c_k)) \mid h \in R \} \subseteq A^*.$$

We have just seen.

Proposition

The set of all solutions of a quadratic word equation is EDT0L.

But the result is the same for all equations.

EDTOL

All solutions for word equations in free monoids with rational constraints

Equations with rational constraints are better!

Theorem [Ciobanu, D., Elder (ICALP 2015)]

Let $U=V$ with be an equation in variables X_i and $R_i \subseteq A^*$ regular languages for $i = 1, \dots, k$. Then the set of all solutions of the equation with regular constraints is EDT0L. That is

$$\begin{aligned} & \{ (\sigma(X_1), \dots, \sigma(X_k)) \mid \sigma \text{ solves the equation } U=V \text{ with } \sigma(X_i) \in R_i \} \\ & = \{ (h(X_1), \dots, h(X_k)) \mid h \in L(\mathcal{A}) \}. \end{aligned}$$

The result became possible due to the *recompression technique* of Artur Jež for solving word equations (STACS 2013, JACM 2016) mentioned earlier in the talk.

More about solving equations by recompression by Artur himself later the week.

More EDT0L results. We can consider other structures than words. For example.

- Free groups with solutions in reduced words. Ciobanu, D., Elder (ICALP 2015)
- Partially commutative monoids and groups with solutions in normal forms. D., Jež, Kufleitner (ICALP 2016)
- Twisted word equations with solutions in normal forms. D., Elder (ICALP 2017)
Special case: $SL(2, \mathbb{Z})$.
- Solutions sets to systems of equations in hyperbolic groups are EDT0L in PSPACE. Ciobanu, Elder (ICALP 2019)

Related results about context free groups G . (That is, given a presentation $\varphi : A^* \rightarrow G$, then $\varphi^{-1}(1)$ is context-free language.)

- G is context-free $\iff G$ is a finitely generated subgroup in a semidirect product of a free group by a finite group. (D., Weiß (2017) The Isomorphism Problem for Finite Extensions of Free Groups Is In PSPACE. Sénizergues, Weiß (ICALP 2018)

Some future work

- Prove the **main conjecture in the field**: **WordEquations** is NP-complete
- Prove the weaker form **QuadraticWordEquations** is NP-complete
- Fix the number of variables by k , say $k = 4$. Prove that solvability of word equations with at most k variables can be tested in polynomial time.
- **Büchi's Problem**: **WordEquation with the equal-length predicate**.
- Given a word equation with regular constraints and the not regular palindrome-predicate ($X = \overline{X}$), then we can still decide solvability. What else can be done?
- Equations with rational constraints in $SL(2, \mathbb{Z})$ are decidable. What about equations for the monoid of matrices $\mathbb{Z}^{2 \times 2}$? The special case of the membership problem in $\mathbb{Z}^{2 \times 2}$ is decidable. Potapov and Semukhin (MFCS 2017).

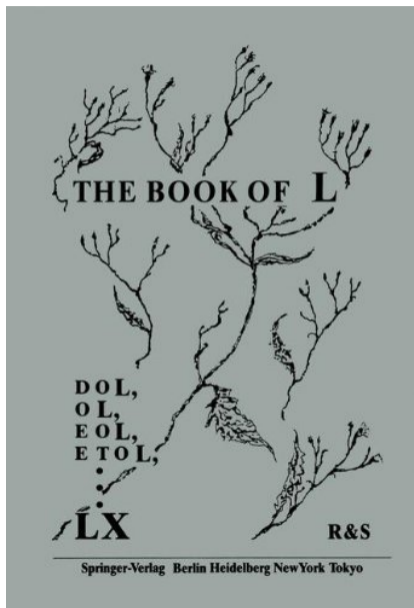
This is the end

Thank you


This is the end,
Beautiful friend,
This is the end,
My only friend, the end.


Jim Morrison, 08.12.1943–03.07.1971


The Book of L by Rozenberg and Salomaa in 1985




Related Literature.

 P. R. Asveld.
Controlled iteration grammars and full hyper-AFL's.
Information and Control, 34(3):248 – 269, 1977.

 J. R. Büchi and S. Senger.
Definability in the existential theory of concatenation and undecidable extensions of this theory.
Zeitschr. f. math. Logik und Grundlagen d. Math., 34:337–342, 1988.

 L. Ciobanu, V. Diekert, and M. Elder.
Solution sets for equations over free groups are EDT0L languages.
International Journal of Algebra and Computation, 26:843–886, 2016.
Conference abstract in ICALP 2015, LNCS 9135 with full version on ArXiv e-prints:
[abs/1502.03426](https://arxiv.org/abs/1502.03426).

 L. Ciobanu and M. Elder.
Solutions sets to systems of equations in hyperbolic groups are EDT0L in PSPACE.
ArXiv e-prints, [abs/1902.07349](https://arxiv.org/abs/1902.07349), 2015.



F. Dahmani and V. Guirardel.

Foliations for solving equations in groups: free, virtually free and hyperbolic groups.

J. of Topology, 3:343–404, 2010.



V. Diekert.

Makanin's Algorithm.

In M. Lothaire, editor, *Algebraic Combinatorics on Words*, volume 90 of *Encyclopedia of Mathematics and Its Applications*, chapter 12, pages 387–442. Cambridge University Press, 2002.



V. Diekert and M. Elder.

Solutions of twisted word equations, EDT0L languages, and context-free groups.

In I. Chatzigiannakis, P. Indyk, F. Kuhn, and A. Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, volume 80 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 96:1–96:14, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.



V. Diekert, C. Gutiérrez, and Ch. Hagenah.

The existential theory of equations with rational constraints in free groups is PSPACE-complete.

Information and Computation, 202:105–140, 2005.

Conference version in STACS 2001, LNCS 2010, 170–182, 2001.



V. Diekert, Yu. Matiyasevich, and A. Muscholl.

Solving word equations modulo partial commutations.

Theoretical Computer Science, 224:215–235, 1999.

Special issue of LFCS'97.



V. Diekert and A. Muscholl.

Solvability of equations in free partially commutative groups is decidable.

International Journal of Algebra and Computation, 16:1047–1070, 2006.

Conference version in Proc. ICALP 2001, 543–554, LNCS 2076.



V. G. Durnev.

On equations in free semigroups and groups.

Matematicheskie Zametki, 16:717–724, 1974.

In Russian; English translation: *Math. Notes of the Acad. of Sci. of the USSR* 16 (1975) 1024–1028.



M. Lohrey and G. Sénizergues.

Theories of HNN-extensions and amalgamated products.

In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, *ICALP*, volume 4052 of *Lecture Notes in Computer Science*, pages 504–515. Springer, 2006.



G. S. Makanin.

The problem of solvability of equations in a free semigroup.

Math. Sbornik, 103:147–236, 1977.

English transl. in *Math. USSR Sbornik* 32 (1977).



G. S. Makanin.

Equations in a free group.

Izv. Akad. Nauk SSR, Ser. Math. 46:1199–1273, 1983.

English transl. in *Math. USSR Izv.* 21 (1983).



J. V. Matijasevič.

A connection between systems of word and length equations and Hilbert's tenth problem.

Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), 8:132–144, 1968.



Yu. Matiyasevich.

Reduction of trace equations to word equations.

Talk given at the “Colloquium on Computability, Complexity, and Logic”, Institut für Informatik, Universität Stuttgart, Germany, Dec. 5–6, 1996.



Yu. V. Matiyasevich.

Hilbert's Tenth Problem.

MIT Press, Cambridge, Massachusetts, 1993.



W. Plandowski.

Satisfiability of word equations with constants is in PSPACE.

J. ACM, 51:483–496, 2004.

Conference version in Proc. FOCS'99.



G. Rozenberg and A. Salomaa.

The Book of L.

Springer, 1986.



M. Schaefer, E. Sedgwick, and D. Štefankovič.

Recognizing string graphs in NP.

Journal of Computer and System Sciences, 67:365–380, 2003.



K. U. Schulz.

Makanin's algorithm for word equations — Two improvements and a generalization.

In K. U. Schulz, editor, *Word Equations and Related Topics*, volume 572 of *Lecture Notes in Computer Science*, pages 85–150, Heidelberg, 1990. Springer-Verlag.