Equations in free groups and EDT0L languages

Volker Diekert[1]

Universität Stuttgart

Group Theory International Webinar, Thursday, April 16, 2015

[1] Joint work with: Laura Ciobanu and Murray Elder
The paper is on arXiv and it will appear at ICALP 2015, Kyoto, 2015 July 6 -10

The main result

Let $W = 1$ with $W \in F(A \cup \Omega)$ be an equation over a free group $F(A)$ in variables $\Omega = \{X_1, \ldots, X_k\}$. There is a simple algorithm which yields a finite NFA $\mathcal{A}$ such that:

- $\mathcal{A}$ accepts a rational language R of endomorphisms over C^*.
- $A \subseteq C$.
- The alphabet C is of linear size in the input.
- The set of all solutions σ in reduced words for $W =$ is

$$\begin{aligned}\{\, (\sigma(X_1), \ldots, \sigma(X_k)) \in A^* \times \cdots \times A^* \;\mid \sigma(W) = 1 \,\}\\ = \{\, (h(\$_1), \ldots, h(\$_k)) \in C^* \times \cdots \times C^* \;\mid h \in R \,\}\end{aligned}$$

where $\$_1, \ldots, \$_k \in C$ are special symbols.

Remarks

- Our result relies on the (re-)compression technique due to Artur Jeż for solving word equations (STACS 2013).
- The set of all solutions is finite if and only if R is a finite.
- As a byproduct we obtain the following new complexity results:
  - The existential theory of free groups is in NSPACE$(n \log n)$.
  - Deciding whether an equation in free groups has only finitely many solutions is in NSPACE$(n \log n)$.

Commercial break

We believe that NSPACE$(n \log n)$ is space optimal.
The compression technique is powerful.
It provides the simplest method to solve equations in free groups.

Unfortunately, it is somewhat difficult to explain why it is easy. Sorry.

NFAs and rational subsets

Let M be any monoid, eg. either $M = F(A)$ or $M = C^*$ or $M = \mathrm{End}(C^*)$.

A nondeterministic finite automaton (NFA) over 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.
- Benois (1969): Rational sets in free groups form a Boolean algebra.

EDT0L languages

EDT0L refers to **E**xtended, **D**eterministic, **T**able, **0** interaction, and **L**indenmayer system. See: The Book of **L** (Springer, 1986).

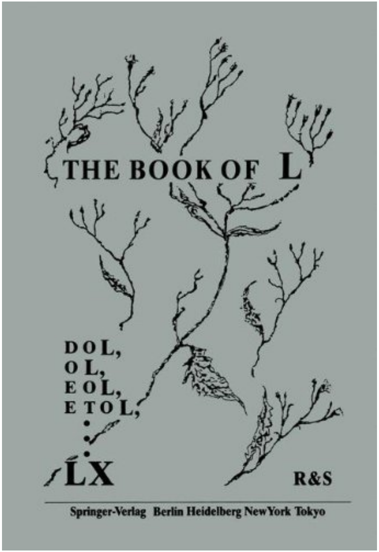
EDT0L languages via a “rational control” due to Asveld (1977).

Definition

$L \subseteq A^*$ is an EDT0L language if there is an extended alphabet C with $A \subseteq C$, a symbol $\# \in C$, and a rational set of endomorphisms $R \subseteq \mathrm{End}(C^*)$ such that

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

The picture of **L**



The main result as a statement about EDT0L

Theorem

Let $W = 1$ with $W \in F(A \cup \Omega)$ be an equation (with rational constraints) over a free group $F(A)$ in variables $\Omega = \{X_1, \ldots, X_k\}$. Then the set of all solutions of W in reduced words is an EDT0L language.

- EDT0L languages form a proper subset of indexed languages.
- Solution sets are not context-free, in general.
- The context-free language of words over $\{a, a^{-1}, b, b^{-1}\}$ which reduce to the empty word is not in EDT0L. Thus, the word problem of $F(a, b)$ is not in EDT0L. (This is a well-known fact in formal language theory.)
- It is open whether the word problem of $\mathbb{Z}$ is in EDT0L.

From groups to monoids with involution

Starting point: Replace $F(A)$ by A^*, where A^* is a free monoid with involution. Transform the group equation $W = 1$ into a word equation $U = V$ over A^*. Add special constants $\$_1, \ldots, \$_k$ and $\#$ with $\overline{\#} = \#$ to A. Replace $U = V$ by a single word:

$$W_{\text{init}} = \$_1 X_1 \cdots \$_k X_k \# U \# V \# \overline{U} \# \overline{V} \# \overline{X_k}\, \overline{\$_k} \cdots \overline{X_1}\, \overline{\$_1}.$$

Introduce a rational constraint $\sigma(X) \notin \bigcup_{a \in A} A^* a \overline{a} A^*$ via a morphism $\mu : A^* \to N$ where N is a finite monoid with zero 0. This ensures that solutions are in reduced words.

Definition

A solution of a word $W \in (A \cup \Omega)^*$ is a morphism $\sigma : \Omega \to A^*$ such that

- $\sigma(W) = \sigma(\overline{W})$.
- $\mu\sigma(X) \neq 0$ for all $X \in \Omega$, ie. $\sigma(X)$ has no nontrivial factor $a\overline{a}$.

The finite monoid N keeping the words reduced

Define $N = \{1, 0\} \cup A \times A$ to "remember first and last letters" with $1 \cdot x = x \cdot 1 = x$, $0 \cdot x = x \cdot 0 = 0$, and

$$(a, b) \cdot (c, d) = \begin{cases} 0 & \text{if} \quad b = \overline{c} \\ (a, d) & \phantom{\text{if}} \quad b \neq \overline{c}. \end{cases}$$

The monoid N has an involution by $\overline{1} = 1$, $\overline{0} = 0$, and $\overline{(a, b)} = (\overline{b}, \overline{a})$.

Fix the morphism $\mu_0 : A^* \to N$ given by $\mu_0(\$_i) = \mu_0(\#) = 0$ and $\mu_0(a) = (a, a)$ otherwise.

μ_0 respects the involution.

$\mu_0(w) = 0$ if and only if either w is not reduced or contains a symbol from $\$_1, \ldots, \$_k, \#$.

Specify an equation together with a set of constants and variables, a morphism μ (which controls the rational constraints) and a partial commutation which allows some symbols to commute.

Specification: $(W, B, \mathcal{X}, \mu, \theta)$

W	$=$ equation, the solution is a palindrome.
B	$=$ constants with $A \subseteq B = \overline{B} \subseteq C$.
$\mathcal{X}$	$=$ variables in W.
μ	$=$morphism to control constraints.
θ	$=$ partial commutation

During the process of finding a solution we change these parameters and we describe the process in terms of a diagram of states and arcs between them.

Arcs changing variables: substitution arcs

Arcs $(W, B, \mathcal{X}, \mu, \theta) \xrightarrow{\varepsilon} (\tau(W), B, \mathcal{X}', \mu', \theta')$ manipulate variables via a morphism $\tau : \mathcal{X} \to M(B, \mathcal{X}', \mu', \theta')$. The label is $\varepsilon = \mathrm{id}_{C^*}$.

1. $\tau(X) = 1$: remove X (and $\overline{X}$) from W. Potentially removes partial commutation.
2. $\tau(X) = aX$: substitute X by aX, where a is a constant.
3. $\tau(X) = YX$: split X as YX and define a type $\theta(Y) = a$, where a is a constant. After that Y commutes with a. This commuting relation is used for compressing blocks a^ℓ into a single fresh letter a_ℓ.

Arcs changing constants: compression arcs

Arcs $(h(W'), B, \mathcal{X}, \mu, \theta) \xrightarrow{h} (W', B', \mathcal{X}, \mu', \theta')$ change the constants. The label $h \in \mathrm{End}(C^*)$ induces a morphism $h : M(B') \to M(B)$ in the opposite direction of the arc.

1. Make B larger via morphisms $c \mapsto h(c) \neq 1$ where $c \in B'$. This provides us with enough fresh letters which can be used for compression.
2. Consider morphisms $c \mapsto h(c) \in B^*$ with $1 \leq |h(c)| \leq 2$; and move from an equation $h(W')$ to W'. We compress the word $h(c)$ into a (fresh) letter c. As a consequence $|W'| \leq |h(W)|$. The equation gets shorter.
3. Replace B by a smaller alphabet B' if W does not use a letter in $B \setminus B'$. We have $h = \mathrm{id}_{C^*}$. This keeps the alphabet of constants small.
4. Introduce partial commutation between constants by making θ larger: $h = \mathrm{id}_{C^*}$. Used inside block compression. If a^ℓ is compressed into a_ℓ, then a and a_ℓ must commute, hence define $\theta(a_\ell) = a$.

Notation

Let C be a fixed extended alphabet with $A \subseteq C$ and $|C| \leq 100\,|W_{\text{init}}|$.

$A \subseteq B = \overline{B} \subseteq C$ and $\mathcal{X} = \overline{\mathcal{X}} \subseteq \Omega$ with morphism $\mu : B \cup \mathcal{X} \to N$ such that $\mu(a) = \mu_0(a)$ for all $a \in A$.

A type is a partial mapping $\theta : (B \cup \mathcal{X}) \setminus A \to B$ respecting the involution such that $\mu(\theta(x)x) = \mu(x\theta(x)) \in N$.

We define

$$M(B \cup \mathcal{X}, \mu, \theta) = (B \cup \mathcal{X})^* / \{\, \theta(x)x = x\theta(x) \;\mid\; x \in B \cup \mathcal{X} \,\} \xrightarrow{\mu} N$$

$M(B)$ denotes the submonoid of $M(B \cup \mathcal{X}, \mu, \theta)$ generated by B. We have $A^* \subseteq M(B)$ since $\theta(a)$ is not defined for $a \in A$.

The monoids $M(B)$ and $M(B \cup \mathcal{X}, \mu, \theta)$ are free partially commutative.

We need only free products of free commutative monoids.

The states of the NFA $\mathcal{A}$ of endomorphisms

Definition

A state of $\mathcal{A}$ is a tuple $P = (W, B, \mathcal{X}, \mu, \theta)$ such that:

- $W \in M(B \cup \mathcal{X}, \mu, \theta)$.
- $|W| \leq 100\,|W_{\text{init}}|$.
- W is called the equation at P.

Initial states

$(W_{\text{init}}, A, \Omega, \mu, \emptyset)$

Final states

$(W, B, \emptyset, \mu, \emptyset)$ with $\overline{W} = W \in B^*$ and $\$_1 \cdots \$_k$ is a prefix of W.

Solutions at states

Definition

Let $P = (W, B, \mathcal{X}, \mu, \theta)$ be a state.

- A B-solution at P is given by a morphism $\sigma : \mathcal{X} \to B^*$ inducing a B-morphism $\sigma : M(B \cup \mathcal{X}, \mu, \theta) \to M(B)$ such that $\sigma(W) = \sigma(\overline{W})$.
- A solution at P is a pair (α, σ) such that σ is a B-solution and $\alpha : M(B) \to A^*$ is an A-morphism.

Remark

- If $(W_{\mathrm{init}}, A, \Omega, \mu, \emptyset)$ has a solution (α, σ), then it has the form $(\mathrm{id}_{A^*}, \sigma)$
- Final states $(W, B, \emptyset, \mu, \emptyset)$ have a unique B-solution id_{B^*}.

$\mathcal{A}$ obtains the substitution and compression arcs

Let $P = (W, B, \mathcal{X}, \mu, \theta) \xrightarrow{h} (W', B', \mathcal{X}', \mu', \theta') = P'$, where $h : M(B') \to M(B)$ is an A-morphism with the restrictions above.

Lemma

- If σ' is a B'-solution at P' and if $\alpha : M(B) \to A^*$ is an A-morphism, then $(\alpha h, \sigma')$ is a solution at P' and there exists a solution (α, σ) at P with $\alpha\sigma W = \alpha h \sigma' W'$.
- If (α, σ) at P, then there exists a solution $(\alpha h, \sigma')$ at P' with $\alpha\sigma W = \alpha h \sigma' W'$.

Soundness of $\mathcal{A}$

Let $h_1 \cdots h_t$ be the labels of a path from an initial state $P_0 = (W_{\text{init}}, A, \Omega, \mu, \emptyset)$ to a final state $(W, B, \emptyset, \mu, \emptyset)$. Then $\sigma(X_i) = h_1 \cdots h_t(\$_i)$ defines a solution at P_0.

Complexity

Theorem

The graph $\mathcal{A}$ can be constructed deterministically in singly exponential time via some NSPACE$(n \log n)$ algorithm which outputs states and arcs which appear on paths between initial and final vertices.
The NFA $\mathcal{A}$ satisfies the soundness property, i.e., the corresponding EDT0L language is a subset of solutions in reduced words.

Proof.

The complexity statement is trivial by standard methods.
It is only here where $|h(c)| \leq 2$ is used.
Soundness was stated above.

“Then a miracle occurs” (cf. S. Harris): completenes

By soundness of the NFA $\mathcal{A}$ it remains to prove the following purely existential statement

Theorem

Let $(\mathrm{id}_{A^*}, \sigma)$ *be a solution at an initial vertex* $(W_{\mathrm{init}}, A, \Omega, \mu, \emptyset)$*. Then there exists a path inside* $\mathcal{A}$ *to a some final vertex.*

Proof.

Iterate block compression and pair compression based on the method of Jeż presented at STACS 2013. Details are on arXiv.

"Then a miracle occurs" (cf. S. Harris): completenes

By the soundness of the NFA $\mathcal{A}$ it remains to prove the following purely existential statement:

Theorem

Let $(\mathrm{id}_{A^*}, \sigma)$ *be a solution at an initial vertex* $(W_{\mathrm{init}}, A, \Omega, \mu, \emptyset)$*. Then there exists a path inside* $\mathcal{A}$ *to some final vertex.*

Proof.

Iterate block compression and pair compression based on the method of Jeż presented at STACS 2013. Details are on arXiv.

This is the end. Thank you.

Related Literature.

A. V. Aho.
Indexed grammars—an extension of context-free grammars.
J. Assoc. Comput. Mach., 15:647–671, 1968.

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

M. Benois.
Parties rationelles du groupe libre.
C. R. Acad. Sci. Paris, Sér. A, 269:1188–1190, 1969.

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.

V. Diekert, A. Jeż, and W. Plandowski.
Finding all solutions of equations in free groups and monoids with involution.
Proc. CSR 2014 **LNCS**8476: 1–15, 2014.

A. Ehrenfeucht and G. Rozenberg.
On some context free languages that are not deterministic ET0L languages.
RAIRO Theor. Inform. Appl., 11:273–291, 1977.

S. Eilenberg.
Automata, Languages, and Machines, Vol A.
Acad. Press, 1974.

J. Ferté, N. Marin, and G. Sénizergues.
Word-mappings of level 2.
Theory Comput. Syst., 54:111–148, 2014.

R. H. Gilman.
Personal communication, 2012.

A. Jeż.
Recompression: a simple and powerful technique for word equations.
Proc. STACS. **LIPIcs**, 20:233–244, 2013. Journal version to appear in JACM

O. Kharlampovich and A. Myasnikov.
Elementary theory of free non-abelian groups.
J. of Algebra, 302:451–552, 2006.

A. G. Myasnikov and V. Roman'kov.
On rationality of verbal subsets in a group.
Theory Comput. Syst., 52:587–598, 2013.

W. Plandowski.
An efficient algorithm for solving word equations.
Proc. STOC'06: 467–476. ACM Press, 2006.

W. Plandowski.
personal communication, 2014.

W. Plandowski and W. Rytter.
Application of Lempel-Ziv encodings to the solution of word equations.
Proc. ICALP'98. **LNCS**1443: 731–742, 1998.

A. A. Razborov.
On systems of equations in free groups.
In Combinatorial and Geometric Group Theory, pages 269–283. Cambridge University Press, 1994.

G. Rozenberg and A. Salomaa.
The Book of **L**. Springer, 1986.

G. Rozenberg et al. (Eds.)
Handbook of Formal Languages, Vol 1. Springer, 1997.

Z. Sela.
Diophantine geometry over groups VIII: Stability.
Annals of Math., 177:787–868, 2013.