RATIONAL SUBSETS OF UNITRIANGULAR GROUPS

Markus Lohrey
Department für Elektrotechnik und Informatik, Universität Siegen, Germany
lohrey@eti.uni-siegen.de

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by [editor]

It is shown that there exist $d, \ell \geq 3$ and a sequence $C_1, \ldots, C_\ell$ of cyclic subgroups of the d-dimensional unitriangluar matrix group over $\mathbb{Z}$ (which is finitely generated nilpotent) such that membership in the product $C_1 C_2 \cdots C_\ell$ is undecidable.

Keywords: unitriangluar matrix groups; undecidability; rational subets of groups.

Mathematics Subject Classification 2010: 20F10; 20F18; 20H25

1. Introduction

Since the seminal work of Dehn from 1911, algorithmic decision problems are a classical topic in combinatorial group theory. Dehn [5] introduced the word problem (Does a given word over the generators represent the identity?), the conjugacy problem (Are two given group elements conjugate?) and the isomorphism problem (Are two given finitely presented groups isomorphic?), see [15] for general references in combinatorial group theory. Starting with the work of Novikov and Boone from the 1950's, all three problems were shown to be undecidable for finitely presented groups in general. A generalization of the word problem is the *subgroup membership problem* (also known as the *generalized word problem*) for finitely generated groups: Given group elements $g, g_1, \ldots, g_n$, does g belong to the subgroup generated by $g_1, \ldots, g_n$? Explicitly, this problem was introduced by Mihailova in 1959 [17], although Nielsen had already presented an algorithm for the subgroup membership problem for free groups in his paper from 1921 [18].

Motivated partly by automata theory, the subgroup membership problem was further generalized to the *rational subset membership problem*. Assume that the group G is finitely generated by the set X (we always assume X to be symmetric in the sense that $a \in X$ if and only if $a^{-1} \in X$). A finite automaton A with transitions labeled by elements of X defines a subset $L(A) \subseteq G$ in the natural way; such subsets are the rational subsets of G. The set of rational subsets of G can be also defined as the smallest set that contains all finite subsets of G and that is closed under union, product, and the Kleene star operator (which constructs from a subset $A \subseteq G$ the submonoid A^* generated by A). The rational subset membership problem asks whether a given group element belongs to $L(A)$ for a given finite automaton (in fact, this problem makes sense for any finitely generated monoid). The notion of a rational subset of a monoid can be traced back to the work of Eilenberg and Schützenberger from 1969 [6]. In the same year, Benois [3] proved that every finitely generated free group has a decidable rational subset membership problem. Further results on the rational subset membership problem can be found in [7,8,12,13,14,20], see [11] for a survey.

In this paper, we deal with rational subsets of nilpotent groups, more precisely unitriangular matrix groups. Let $N_{r,c}$ be the free nilpotent group of class c generated by r elements. In 1999, Roman'kov [20] presented at a conference a proof, showing that there exists an r such that $N_{r,2}$ has an undecidable rational subset membership problem. The proof consists of a highly technical reduction from Hilbert's 10th problem (the question whether a polynomial equation $p(x_1, \dots, x_n) = 0$, where $p(x_1, \dots, x_n)$ is a multivariate polynomial with integer coefficients, has a solution). Unfortunately, a full version of [20] has never appeared.

Every torsion-free finitely generated nilpotent group embeds into a group of unitriangular integer matrices [9, Theorem 17.2.5], see Section 3 for precise definitions. We denote with UT_d the group of all $(d \times d)$-unitriangular matrices over $\mathbb{Z}$. Hence, from Roman'kov's result it follows that for some $d \geq 2$ the group UT_d has an undecidable rational subset membership problem. In fact, we must have $d \geq 3$, since $\mathsf{UT}_2 \cong \mathbb{Z}$. In this paper, we show that undecidability occurs already for a very specific class of rational subsets: We show that there exist $d, \ell \geq 3$ and a sequence $C_1, \dots, C_\ell$ of cyclic subgroups of UT_d such that the membership problem for the product $C_1 C_2 \cdots C_\ell$ (a rational subset of UT_d) is undecidable (Theorem 5.1). We emphasize that the cyclic subgroups $C_1, \dots, C_\ell$ are fixed in the sense that in principle one could explicitly write down a list of generators for these subgroups. The input of the undecidable problem only consists of a matrix $M \in \mathsf{UT}_d$ and it is asked whether $M \in C_1 C_2 \cdots C_l$. As Roman'kov's proof, our undecidability proof is based on Hilbert's 10th problem. We split the proof into two steps. In the first step, we use Hilbert's 10th problem to show that solvability of certain matrix equations is undecidable (Proposition 4.1). For this we use a construction by Ben-Or and Cleve [2] that, roughly speaking, allows to reduce the evaluation of a polynomial to a sequence of matrix multiplications. In the second step, we reduce the solvability of the matrix equations from Proposition 4.1 to the membership problem for a sequence of cyclic subgroups of UT_d (for a fixed d). Let us also mention that one can replace in our undecidability result every cyclic subgroup $C_i = \langle G_i \rangle$ by the one-generator submonoid $G_i^* = \{G_i^n \mid n \geq 0\}$ and retain undecidability, see Theorem 5.2.

To obtain undecidability we must have $l \geq 3$, i.e., we need products of at least 3 cyclic subgroups. This follows from a result of Lennox and Wilson [10], according to which products of two subgroups H, K of a polycyclic group G are closed in the profinite topology, i.e., for every $g \notin HK$ there exists a homomorphism φ

from G into a finite group such that $\varphi(g) \notin \varphi(HK)$. Since every finitely generated polycyclic group is finitely presented it follows that the membership problem for a product of two finitely generated subgroups of a finitely generated polycyclic group is decidable. In this context, one should also mention that [10] contains an example of a product of 3 subgroups of UT_3 (the Heisenberg group), which is not closed in the profinite topology.

2. Related work

There exist a large number of papers dealing with (variants of) the matrix mortality problem. In this problem, it is asked, whether for given integer matrices $M_1, \dots, M_k$, the submonoid $\{M_1, \dots, M_k\}^*$ contains the zero matrix. Paterson [19] proved that the matrix mortality problem is undecidable in dimension 3, whereas the decidability status for dimension 2 is open.

Theorem 5.1 and 5.2 can be also interpreted by saying that solvability of matrix equations of the form $M = M_1^{x_1} M_2^{x_2} \cdots M_l^{x_l}$, where $M, M_1, \dots, M_l$ are unitriangluar matrices and $x_1, \dots, x_l$ are variables that either range over the integers or the natural numbers, is undecidable. Similar matrix equations were studied in [1], but there the matrices $M, M_1, \dots, M_l$ are not assumed to be unitriangluar (not even invertible).

3. Unitriangular groups

A $(d \times d)$-matrix A over $\mathbb{Z}$ is *unitriangluar* if $A[i,i] = 1$ for all $1 \leq i \leq d$ and $A[i,j] = 0$ for all $1 \leq j < i \leq d$. This means that all diagonal entries are 1 and all entries below the diagonal are zero. With UT_d we denote the set of all $(d \times d)$-unitriangular matrices over $\mathbb{Z}$. It forms a nilpotent group.

Let $1 \leq i < j \leq d$. With $A_{i,j}^{(d)}$ we denote the $(d \times d)$-matrix with $A_{i,j}^{(d)}[i,j] = 1$ and $A_{i,j}^{(d)}[k,l] = 0$ for $(k,l) \neq (i,j)$. We omit the superscript (d) in $A_{i,j}^{(d)}$, if the dimension d is clear from the context. In particular, we assume that $d \geq j$ when using the notation $A_{i,j}$. Note that

$$A_{i,j} A_{k,l} = \begin{cases} A_{i,l} & \text{if } j = k \\ 0 & \text{if } j \neq k. \end{cases} \tag{3.1}$$

For an integer a define $T_{i,j}^{(d)}(a) = \mathsf{Id} + a \cdot A_{i,j}^{(d)}$, where Id is the $(d \times d)$-identity matrix. Moreover, let $T_{i,j}^{(d)} = T_{i,j}^{(d)}(1)$. Again, we just write $T_{i,j}(a)$ and $T_{i,j}$ if the dimension d is clear from the context. The group UT_d is generated by the matrices $T_{i,i+1}$ for $1 \leq i < d$, see e.g. [4]. Note that $T_{i,j}(a) = T_{i,j}^a$ for all $a \in \mathbb{Z}$.

As usual we denote with $[x,y] = x^{-1}y^{-1}xy$ the commutator of x and y.

Lemma 3.1. *For all $a, b \in \mathbb{Z}$ and $1 \leq i < j < k \leq d$ we have $[T_{i,j}^a, T_{j,k}^b] = T_{i,k}^{ab}$.*

Proof. Using (3.1) we get

$$\begin{aligned}[T_{i,j}^a, T_{j,k}^b] &= (\mathsf{Id} - a \cdot A_{i,j}) \cdot (\mathsf{Id} - b \cdot A_{j,k}) \cdot T_{i,j}(a) \cdot T_{j,k}(b) \\ &= (\mathsf{Id} + ab \cdot A_{i,k} - a \cdot A_{i,j} - b \cdot A_{j,k}) \cdot (\mathsf{Id} + a \cdot A_{i,j}) \cdot T_{j,k}(b) \\ &= (\mathsf{Id} + ab \cdot A_{i,k} - b \cdot A_{j,k}) \cdot (\mathsf{Id} + b \cdot A_{j,k}) \\ &= (\mathsf{Id} + ab \cdot A_{i,k}) \\ &= T_{i,k}^{ab},\end{aligned}$$

which proves the lemma. □

Lemma 3.2. *For all $1 \leq i < j \leq d$, $1 \leq k < l \leq d$ with $j \neq k$, $i \neq l$ we have $[T_{i,j}, T_{k,l}] = \mathsf{Id}$, i.e., $T_{i,j}$ and $T_{k,l}$ commute.*

Proof. Using (3.1) we get

$$\begin{aligned}[T_{i,j}, T_{k,l}] &= (\mathsf{Id} - A_{i,j}) \cdot (\mathsf{Id} - A_{k,l}) \cdot (\mathsf{Id} + A_{i,j}) \cdot (\mathsf{Id} + A_{k,l}) \\ &= (\mathsf{Id} - A_{i,j} - A_{k,l}) \cdot (\mathsf{Id} + A_{i,j} + A_{k,l}) \\ &= \mathsf{Id},\end{aligned}$$

which proves the lemma. □

4. Exponential expressions

An *exponential expression E of dimension d over the variables $x_1, \ldots, x_k$* is a product of the form

$$E = M_1^{e_1} M_2^{e_2} \cdots M_l^{e_l}$$

with $e_1, \ldots, e_l \in \mathbb{Z} \cup \{x_1, \ldots, x_k\}$ and $M_1, \ldots, M_l \in \mathsf{UT}_d$. A valuation for E is a mapping $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$. We extend v to $v : \{x_1, \ldots, x_k\} \cup \mathbb{Z} \to \mathbb{Z}$ by $v(z) = z$ for all $z \in \mathbb{Z}$ and define the matrix

$$v(E) = M_1^{v(e_1)} M_2^{v(e_2)} \cdots M_l^{v(e_l)}.$$

For the exponential expression $E = M_1^{e_1} M_2^{e_2} \cdots M_l^{e_l}$ we define

$$E^{-1} = (M_l^{-1})^{e_l} (M_{l-1}^{-1})^{e_{l-1}} \cdots (M_1^{-1})^{e_1}.$$

Clearly, for every valuation v we have $v(E^{-1}) = v(E)^{-1}$.

Proposition 4.1. *There are constants $d, k \geq 1$ and a fixed exponential expression E of dimension d over k variables such that the following problem is undecidable:*

input: *A matrix $M \in \mathsf{UT}_d$.*
question: *Is there a valuation v with $v(E) = M$?*

Proof. By Matiyasevich's theorem [16], every recursively enumerable set of natural numbers can be obtained as the intersection of $\mathbb{N}$ with the range of a multivariate polynomial over $\mathbb{Z}$. By taking an undecidable recursively enumerable set (e.g. the halting problem) one obtains a fixed polynomial $P(x_1 \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ such that the following problem is undecidable:

input: A natural number $a \in \mathbb{N}$.
question: Does the equation $P(x_1, \ldots, x_k) = a$ has a solution in $\mathbb{Z}^k$?

Let us fix the polynomial $P(x_1, \ldots, x_k)$. We can write $P(x_1, \ldots, x_k)$ as

$$P(x_1, \ldots, x_k) = \sum_{i=1}^{m} \prod_{j=1}^{n} Q_{i,j},$$

where $Q_{i,j} \in \mathbb{Z} \cup \{x_1, \ldots, x_k\}$. We can assume that all products $\prod_{j=1}^{n} Q_{i,j}$ have the same length n by simply padding with 1's. For a valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ we also write $v(P)$ for $P(v(x_1), \ldots, v(x_k))$.

Let us set $d = n + 1 \geq 2$. All matrices will have dimension d in the rest of the proof. We construct from P a fixed exponential expression E of dimension d over the variables $x_1, \ldots, x_k$ such that for every valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ we have $v(E) = T_{1,d}^{v(P)}$. The following construction uses ideas from Ben-Or and Cleve [2].

The idea is to construct from the product $Q_i = \prod_{j=1}^{n} Q_{i,j}$ $(1 \leq i \leq m)$ an exponential expression E_i of dimension d over the variables $x_1, \ldots, x_k$ such for every valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ we have $v(E_i) = T_{1,d}^{v(Q_i)}$. Then we can define $E = E_1 E_2 \cdots E_m$ and get for every valuation v:

$$v(E) = \prod_{i=1}^{m} v(E_i) = \prod_{i=1}^{m} T_{1,d}^{v(Q_i)} = T_{1,d}^{\sum_{i=1}^{m} v(Q_i)} = T_{1,d}^{v(P)}.$$

So let us fix $1 \leq i \leq m$. For $1 \leq l \leq n$ let $R_l = \prod_{j=1}^{l} Q_{i,j}$. Hence, $R_n = Q_i$. By induction, we construct for every $1 \leq l \leq n = d-1$ an exponential expression F_l of dimension d over the variables $x_1, \ldots, x_k$ such that for every valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ we have

$$v(F_l) = T_{1,l+1}^{v(R_l)}.$$

Let us start with $l = 1$ and let $Q_{i,1} = Q \in \mathbb{Z} \cup \{x_1, \ldots, x_k\}$. Then we set $F_1 = T_{1,2}^{Q}$. For the induction step, assume that $l \geq 2$ and that the exponential expression F_{l-1} with $v(F_{l-1}) = T_{1,l}^{v(R_{l-1})}$ has been constructed. Let $Q_{i,l} = Q \in \mathbb{Z} \cup \{x_1, \ldots, x_k\}$. Then we set

$$F_l = [F_{l-1}, T_{l,l+1}^{Q}].$$

Let v be a valuation. We get

$$v(F_l) = [v(F_{l-1}), T_{l,l+1}^{v(Q)}] = [T_{1,l}^{v(R_{l-1})}, T_{l,l+1}^{v(Q)}] \overset{\text{Lemma 3.1}}{=} T_{1,l+1}^{v(R_{l-1}) \cdot v(Q)} = T_{1,l+1}^{v(R_l)}.$$

This concludes the proof of the proposition. $\square$

5. Membership in products of cyclic subgroups

The main result of this paper is:

Theorem 5.1. *There exists a fixed constant e and a fixed list $(\langle G_i \rangle)_{1 \le i \le \lambda}$ of cyclic subgroups of UT_e such that membership in the product $\prod_{i=1}^{\lambda} \langle G_i \rangle$ is undecidable.*

Proof. We prove the theorem by a reduction from the problem from Proposition 4.1. Let $d, k \ge 1$ be as in Proposition 4.1 and let

$$E = M_1^{e_1} M_2^{e_2} \cdots M_l^{e_l}$$

be the fixed exponential expression of dimension d over the variables $x_1, \ldots, x_k$ from Proposition 4.1. We can assume that $e_i = 1$ whenever e_i is not a variable.

Basically, we construct the list of cyclic subgroups from E by replacing every subexpression $M_i^{e_i}$ by the subgroup $\langle M_i \rangle \le \mathsf{UT}_d$ generated by the matrix M_i. Two problems appear:

- We do not gurantee that for $1 \le i < j \le l$ with $e_i = e_j \in \{x_1, \ldots, x_k\}$ we iterate the matrix M_i the same number of times as the matrix M_j.
- If $e_i = 1$, then we do not gurantee that the generator matrix M_i appears exactly once.

To achieve these two constraints, we work in the group $\mathsf{UT}_d \times \mathsf{UT}_{l+1} \le \mathsf{UT}_{d+l+1}$. Hence, we can set $e = d + l + 1$ in the theorem. For every $1 \le i \le k$ (i.e., for every variable $x_1, \ldots, x_k$) let

$$P_i = \{j \mid 1 \le j \le l, e_j = x_i\}.$$

Moreover, let

$$Z = \{i \mid 1 \le i \le l, e_i = 1\}.$$

Note that the sets Z and P_j $(1 \le j \le k)$ form a partition of $\{1, \ldots, l\}$.

First of all, for every $1 \le i \le l$ we define the cyclic subgroup C_i as follows:

$$C_i = \langle (M_i, T_{1,i+1}^{-1}) \rangle \le \mathsf{UT}_d \times \mathsf{UT}_{l+1}.$$

Moreover, for every $i \in Z$ we define the pair

$$E_i = (\mathsf{Id}, T_{1,i+1}) \in \mathsf{UT}_d \times \mathsf{UT}_{l+1}.$$

Finally, for every $1 \le i \le k$ (i.e., for every variable $x_1, \ldots, x_k$) we define the cyclic subgroup

$$D_i = \langle (\mathsf{Id}, \prod_{j \in P_i} T_{1,j+1}) \rangle \le \mathsf{UT}_d \times \mathsf{UT}_{l+1}.$$

Claim. For every matrix $M \in \mathsf{UT}_d$ the following holds: There is a valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ such that $M = v(E)$ if and only if

$$(M, \mathsf{Id}) \in \prod_{i \in Z} E_i \prod_{i=1}^{k} D_i \prod_{i=1}^{l} C_i. \tag{5.1}$$

Proof of the Claim. Fix a matrix $M \in \mathsf{UT}_d$. Let us first assume that there is a valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ such that $M = v(E)$. Thus,

$$M = M_1^{v(e_1)} M_2^{v(e_2)} \cdots M_l^{v(e_l)}. \tag{5.2}$$

Note that by Lemma 3.2 all the matrices $T_{1,i+1} \in \mathsf{UT}_{l+1}$ $(1 \leq i \leq l)$ pairwise commute. Actually, the matrices $T_{1,i+1}$ $(1 \leq i \leq l)$ generate a copy of $\mathbb{Z}^l$ inside UT_{l+1} Together with (5.2), this implies

$$\prod_{i \in Z} \overbrace{(\mathsf{Id}, T_{1,i+1})}^{=E_i} \prod_{i=1}^{k} \overbrace{\big(\mathsf{Id}, \prod_{j \in P_i} T_{1,j+1}\big)^{v(x_i)}}^{\in D_i} \prod_{i=1}^{l} \overbrace{(M_i, T_{1,i+1}^{-1})^{v(e_i)}}^{\in C_i} =$$

$$\Big(M, \prod_{i \in Z} T_{1,i+1} \prod_{i=1}^{k} \big(\prod_{j \in P_i} T_{1,j+1}\big)^{v(x_i)} \prod_{i=1}^{l} T_{1,i+1}^{-v(e_i)}\Big) =$$

$$\Big(M, \prod_{i \in Z} T_{1,i+1} \prod_{i=1}^{k} \prod_{j \in P_i} T_{1,j+1}^{v(x_i)} \prod_{i=1}^{l} T_{1,i+1}^{-v(e_i)}\Big) = (M, \mathsf{Id})$$

and hence (5.1).

For the other direction assume that (5.1) holds. Hence, there exists a valuation $v : \{x_1, \ldots, x_k\} \to \mathbb{Z}$ and numbers $h_i \in \mathbb{Z}$ $(1 \leq i \leq l)$ such that

$$(M, \mathsf{Id}) = \prod_{i \in Z} (\mathsf{Id}, T_{1,i+1}) \prod_{i=1}^{k} \big(\mathsf{Id}, \prod_{j \in P_i} T_{1,j+1}\big)^{v(x_i)} \prod_{i=1}^{l} (M_i, T_{1,i+1}^{-1})^{h_i} \tag{5.3}$$

By projecting onto the first component, this implies

$$M = M_1^{h_1} M_2^{h_2} \cdots M_l^{h_l}.$$

Moreover, by projecting (5.3) onto the second component and using the commutativity of the matrices $T_{1,i+1} \in \mathsf{UT}_{l+1}$ $(1 \leq i \leq l)$, we get

$$\mathsf{Id} = \prod_{i \in Z} T_{1,i+1} \prod_{i=1}^{k} \prod_{j \in P_i} T_{1,j+1}^{v(x_i)} \prod_{i=1}^{l} T_{1,i+1}^{-h_i}. \tag{5.4}$$

Recall that the matrices $T_{1,i+1}$ $(1 \leq i \leq l)$ generate a copy of $\mathbb{Z}^l$ inside UT_{l+1}. Hence, (5.4) implies $h_i = 1 = e_i$ for every $i \in Z$ and $h_j = v(x_i)$ for every $1 \leq i \leq k$ and every $j \in P_i$. Hence, we have $M = M_1^{v(e_1)} M_2^{v(e_2)} \cdots M_l^{v(e_l)}$, i.e., $M = v(E)$. This proves the claim.

Since (5.1) is equivalent to

$$(\mathsf{Id}, M)\big(\prod_{i \in Z} E_i\big)^{-1} \in \prod_{i=1}^{k} D_i \prod_{i=1}^{l} C_i,$$

the above claim proves the theorem. $\square$

Recall that $g^* = \{g^i \mid i \geq 0\}$ denotes the submonoid generated by a group element $g \in G$. Our construction in the proof of Theorem 5.1 also shows the following result. The reason is that Hilbert's 10th problem remains undecidable if one asks for solutions in the natural numbers (an integer variable x can be replaced by the difference $y - z$ for two new variables y and z).

Theorem 5.2. *There exists a fixed constant e and a fixed list of matrices* $M_1, \ldots,$ $M_\lambda \in \mathsf{UT}_e$ *such that membership in the rational subset* $M_1^* M_2^* \cdots M_\lambda^*$ *is undecidable.*

6. Open problem

One can ask for the minimal dimension e as well as the minimal number λ of cyclic subgroups such that Theorem 5.1 remains true. In particular, are there three cyclic subgroups $C_1, C_2, C_3 \leq \mathsf{UT}_3$ of the Heisenberg group such that membership in the product $C_1 C_2 C_3$ is undecidable? We need at least three subgroups by [10].

Another open problem concerns the submonoid membership problem for nilpotent groups. The submonoid membership problem for a finitely generated group G asks, whether for given group elements $g, g_1, \ldots, g_n \in G$, g belongs to the submonoid $\{g_1, \ldots, g_n\}^*$. It is open, whether there exists a finitely generated nilpotent group with an undecidable submonoid membership problem.

Acknowledgment. The author thanks the anonymous referee for useful comments.

References

[1] P. Bell, V. Halava, T. Harju, J. Karhumäki, and I. Potapov. Matrix equations and hilbert's tenth problem. *IJAC*, 18(8):1231–1241, 2008.
[2] M. Ben-Or and R. Cleve. Computing algebraic formulas using a constant number of registers. *SIAM Journal on Computing*, 21(1):54–58, 1992.
[3] M. Benois. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris*, Sér. A, 269:1188–1190, 1969.
[4] D. K. Biss and S. Dasgupta. A presentation for the unipotent group over rings with identity. *Journal of Algebra*, 237(2):691–707, 2001.
[5] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Mathematische Annalen*, 71:116–144, 1911. In German.
[6] S. Eilenberg and M. P. Schützenberger. Rational sets in commutative monoids. *Journal of Algebra*, 13:173–191, 1969.
[7] Z. Grunschlag. *Algorithms in Geometric Group Theory*. PhD thesis, University of California at Berkley, 1999.
[8] M. Kambites, P. V. Silva, and B. Steinberg. On the rational subset problem for groups. *Journal of Algebra*, 309(2):622–639, 2007.
[9] M. I. Kargapolov and J. I. Merzljakov. *Fundamentals of the theory of groups*, volume 62 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.
[10] J. C. Lennox and J. S. Wilson. On products of subgroups in polycyclic groups. *Archiv der Mathematik*, 33(4):305–309, 1979/80.
[11] M. Lohrey. The rational subset membership problem for groups: A survey. submitted for publication, `http://www.eti.uni-siegen.de/ti/veroeffentlichungen/13-rat-survey.pdf`, 2014.

[12] M. Lohrey and B. Steinberg. The submonoid and rational subset membership problems for graph groups. *Journal of Algebra*, 320(2):728–755, 2008.

[13] M. Lohrey and B. Steinberg. Tilings and submonoids of metabelian groups. *Theory of Computing Systems*, 48(2):411–427, 2011.

[14] M. Lohrey, B. Steinberg, and G. Zetzsche. Rational subsets and submonoids of wreath products. In *Proceedings of the 40th International Colloquium on Automata, Languages, and Programming, Part II, ICALP 2013*, volume 7966 of *Lecture Notes in Computer Science*, pages 361–372. Springer, 2013.

[15] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory.* Springer, 1977.

[16] Y. V. Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachusetts, 1993.

[17] K. A. Mihaĭlova. The occurrence problem for free products of groups. *Doklady Akademii Nauk SSSR*, 127:746–748, 1959.

[18] J. Nielsen. Om regning med ikke kommutative faktoren og dens anvendelse i gruppeteorien. *Matematisk Tidsskrift, B.*, pages 77–94, 1921. In Danish.

[19] M. Paterson. Unsolvability in 3×3 matrices. *Studies appl. Math.*, 49:105–107, 1970.

[20] V. Roman'kov. On the occurence problem for rational subsets of a group. In V. Roman'kov, editor, *International Conference on Combinatorial and Computational Methods in Mathematics*, pages 76–81, 1999.