Contemporary Mathematics

One Variable Equations in Free Groups via Context Free Languages

Robert H. Gilman and Alexei G. Myasnikov

Abstract. We use context free languages to analyze solution sets to one variable equations over free groups.

Contents

1. Introduction

There are several interesting connections between formal languages and combinatorial group theory. For example virtually free groups can be characterized in terms of context free languages [**11**] as can word hyperbolic groups [**4**]. In this note we see how far context free languages can take us in analyzing solutions to one variable equations over free groups. We do not obtain the exact form of the solution sets, but we do see that consideration of the context free language of all words freely equal to the empty word gives some insight into why large powers occur in these solution sets and suggests an approach which may be fruitful in other situations.

Let F be a free group and Σ a set of free generators and their inverses. An equation over F is a cyclicly reduced word

$$E = u_1 x^{\epsilon_1} \cdots u_d x^{\epsilon_d} \tag{1}$$

in $(\Sigma + x + x^{-1})^*$, the free monoid over $\Sigma \cup \{x, x^{-1}\}$, such that u_i is freely reduced in Σ^*, and each $\epsilon_i = \pm 1$. If substituting a freely reduced word $v \in \Sigma^*$ for x yields $E(v)$ freely equal to the empty word, λ, then v is a solution for E.

2000 *Mathematics Subject Classification.* Primary 20E05; Secondary 20F05 68Q42 68Q45.
Key words and phrases. Free group, formal language.

In 1960 Lyndon proved that one needs only finitely many *parametric words* to describe solutions of one-variable equations over F [**10**]. Further progress in this direction was made by Appel [**1**] and Lorents [**9**], who gave the exact form of the required parametric words. Namely, it turned out that the solution set of $E(x)$ in F is contained in a finite union of sets of the type

$$\{p^n q \mid p, q \in F, n \in \mathbb{Z}\}. \tag{2}$$

Their argument was rather technical; they used direct computations in free groups and the Nielsen cancellation method. Recently, Chiswell and Remeslennikov gave an alternative proof of this result [**3**], which is based on ultrapowers and algebraic geometry over groups. They showed also that the solution set of $E(x)$ is precisely a finite union of sets of the type 2.

Our result is the following.

THEOREM 1. *The solutions to equation (1) are a finite union of sets of the form*

$$\{p_1 p_2^i p_3^j p_4 p_5^k p_6^l p_7 \mid (i, j, k, l) \in S\}$$

where the p_i's are words over Σ^*, and S is a semilinear subset of N^4.

Here N is the set of nonnegative integers; semilinear sets are defined below. As we noted above, Theorem 1 does not give the exact form of the solution sets. The exact form is a consequence of Theorem 1 together with the description of the parametric solutions in a free group from [**6**].

2. Results from Language Theory

For introductions to formal language theory the reader is referred to [**12**] and [**8**]. A survey of language theory and its connections to group theory is given in [**5**].

Let Σ be a finite alphabet and Σ^* the free monoid over Σ. A language is a subset of Σ^*. L^*, $L + L'$, and LL' denote respectively the submonoid generated by a language L, the union of languages L and L' and the product of L and L'. For languages with just one element we may write w instead of $\{w\}$.

We will make use of some results on context–free languages [**2, 8**]. Assume that Σ has formal inverses, and write $\sim$ for free equality.

$$L_1 = \{w \mid w \in \Sigma^*, w \sim \lambda, w \neq \lambda\}$$

is a context–free language and is generated by the context–free grammar with one nonterminal S and productions

$$S \to SS \quad S \to aSa^{-1} \quad S \to aa^{-1} \quad \text{for all } a \in \Sigma.$$

In other words $w \in L_1$ if and only if there is a sequence

$$S = \alpha_0, \alpha_1, \ldots, \alpha_m = w$$

of elements from the free monoid $(\Sigma + S)^*$ such that for $i \geqslant 1$, α_i is obtained by replacing an occurrence of S in α_{i-1} with the right–hand side of one of the rules above. Such sequences are called derivations. Notice that every occurrence of S in a derivation of w is the beginning of a subderivation which derives a subword $w' \sim \lambda$ of w.

A language is bounded if it is a subset of $w_1^* \cdots w_n^*$ for some $w_i \in \Sigma^*$. Lemma 2 shows that bounded context–free languages are related to semi–linear subsets of

N^n, the set of n–tuples of non–negative integers. A semi–linear set is a finite union of linear sets, and a linear set is one of the form $\vec{m}+M$ for $\vec{m} \in N^n$ and M a finitely generated submonoid of N^n. Semi–linear sets are closed under intersection, monoid homomorphism from N^n to N^m, and Cartesian product [**7**, Section 6]. The last part means that if $T \subset N^n$ and $T' \subset N^m$ are semi–linear, so is $T \times T' \subset N^{n+m}$.

LEMMA 2. *If $L \subset \Sigma^*$ is context–free and $\{u_i, v_i \mid 1 \leqslant i \leqslant n\} \subset \Sigma^*$, then*

$$\mathcal{J} = \{(j_1, \ldots, j_n) \mid u_1 v_1^{j_1} \cdots u_n v_n^{j_n} \in L\}$$

is semi–linear.

PROOF. $L' = L \cap u_1^* v_1^* \cdots u_n^* v_n^*$ is the intersection of a context–free language with a regular one and so is context–free. Define

$$\mathcal{I} = \{(i_1, j_1, \ldots, i_n, j_n) \mid u_1^{i_1} v_1^{j_1} \cdots u_n^{i_n} v_n^{j_n} \in L''\}.$$

It suffices to show that $\mathcal{I}$ is semi–linear as $\mathcal{J}$ can be recovered from $\mathcal{I}$ by operations which preserve semi–linearity.

Let

$$\Delta = \{b_i, c_i \mid 1 \leqslant i \leqslant n\}$$

be a new alphabet. By [**7**, Lemma 2.6]

$$L'' = \{\, b_1^{i_1} c_1^{i_1} \cdots b_n^{i_n} c_n^{j_n} \mid (i_1, j_1, \ldots, i_n, j_n) \in \mathcal{I} \,\}$$

is context–free, and Parikh's Theorem [**2**, Section 2.4] applied to L'' says that $\mathcal{I}$ is semi–linear. □

3. Proof of Theorem 1

Fix a free group F, a set of Σ of free generators and their inverses, and an equation E over F.

PROPOSITION 3. *Suppose $d \geqslant 3$. For each solution v of E there is a cyclic subword*

$$z = v^{\epsilon_{i-1}} u_i v^{\epsilon_i} u_{i+1} v^{\epsilon_{i+1}}$$

of $E(v)$ such that v^{ϵ_i} lies in a subword of z freely equal to λ. Cyclic means that indices are read modulo d. We say that i is an index associated with the solution v.

PROOF. Fix a derivation $S \xrightarrow{*} E(v)$. Choose an S which derives a subword z_1 of $E(v)$ containing some v^{ϵ_i} but such that no other S occurring in that subderivation derives such a subword. By considering the first step in the subderivation we see that $z_1 = z_2 z_3$, $a z_2 a^{-1}$, or $a a^{-1}$ where z_2 and z_3 are subwords which do not contain a complete occurrence of any v^{ϵ}. In all cases we may extend z_1 to the right and left as necessary to obtain z. □

LEMMA 4. *Suppose $d \geqslant 3$, and let*

$$C = \max\{|u_k| \mid 1 \leqslant k \leqslant d\}.$$

If i is an index associated with the solution v and if the exponents ϵ_{i-1}, ϵ_i, ϵ_{i+1} alternate in sign, then v lies in a language $p_1 p_2^* p_3^* p_4$ for words $p_j \in \Sigma^*$ of length at most C.

PROOF. By inverting x and cyclicly permuting E as necessary we reduce to the case $z = v^{-1}u_1vu_2v^{-1}$. Proposition 3 implies that $v = v_1v_2$ with v_1 extending to a suffix of $v^{-1}u_1v_1$ freely equal to λ and v_2 extending to a prefix of $v_2u_2v^{-1}$ freely equal to λ. It suffices to show that under these conditions $v_1 \in p_1p_2^*$ and $v_2 \in p_3^*p_4$. The former result follows from the latter by taking inverses.

Suppose then that v_2 extends to a prefix of $v_2u_2v^{-1}$ freely equal to λ. If the prefix ends in u_2, we are done. Assume that this is not the case, and let $u_2 = rsr^{-1}$ with s cyclicly reduced. Note $s \neq \lambda$ because E is cyclicly reduced. We have $v_2u_2v^{-1} = v_2(rsr^{-1})(v_2^{-1}v_1^{-1})$ where we are using parentheses to indicate freely reduced subwords. From our assumption and the fact that cancellation can occur only on either side of rsr^{-1} we see that $v_2 = v_3r^{-1}$ and $v_2u_2v^{-1} = v_3s(v_3^{-1}v_1^{-1})$. Since s is cyclicly reduced, further cancellation can occur only on one side or the other of s if $v_3 \neq \lambda$. It follows that $s = s_1s_2$ with $v_3 = s_1^{-1}s^{-k}$ or s_2s^k, $k \geq 0$. Consequently

$$v_2 = s_1^{-1}s^{-k}r^{-1} = (s_2s_1)^{-k}(rs_1)^{-1}$$

or

$$v_2 = s_2s^kr^{-1} = (s_2s_1)^ks_2r^{-1}$$

as desired. □

LEMMA 5. *If $d \leqslant 2$, then all freely reduced solutions v of E are contained in a finite union sets of the form $p_1p_2^*p_3$ with $|p_j| \leqslant C$. In general all freely reduced solutions are contained a finite union of sets $p_1p_2^*p_3^*p_4p_5^*p_6^*p_7$ with $|p_j| \leqslant 9dC$.*

PROOF. The first assertion can be verified directly, so assume $d \geqslant 3$. By Proposition 3 and Lemma 4 we may restrict our attention to solutions v with an associated index i for which the exponents ϵ_{i-1}, ϵ_i, ϵ_{i+1} do not alternate. By inverting x and inverting and cyclicly permuting E reduce to $z = v^{\epsilon}u_1vu_2v$. As before $v = v_1v_2$ with v_1 extending to a suffix of $v^{\epsilon}u_1v_1$ freely equal to λ and v_2 extending to a prefix of v_2u_2v freely equal to λ.

Suppose either $|v_2| \geqslant |v|/2$ or $\epsilon = 1$ and $|v_1| \geqslant |v|/2$. We will show that $|v| \leqslant 2C$ or v is a solution to an equation to which Lemma 4 applies. We treat the case $|v_2| \geqslant |v|/2$; the argument is similar in the other case.

If v_2 cancels completely in u_2, then we are done. Otherwise there is a prefix v_3 of v with $v_2u_2v_3 \sim \lambda$. Hence $u_2 = rs$ with $v_2 = v_4r^{-1}$, $v_3 = s^{-1}v_5$, and $v_4v_5 \sim \lambda$. We have $v = s^{-1}v_4^{-1}\ldots = \ldots v_4r^{-1}$. The subwords v_4^{-1} and v_4 must be disjoint in v because if they overlapped, it would be in a word equal to its own inverse. If v_4 is a subword of s, then $|v_2| \leqslant |u_2|$, and again we are done. Thus we may assume $v = s^{-1}v_4^{-1}tv_4r^{-1}$ for some $t \neq \lambda$. The condition $t \neq \lambda$ follows from the fact that v is freely reduced. As $|v_4r^{-1}| = |v_2| \geqslant |v|/2$, it follows that $|s^{-1}v_4| \geqslant |v|/2 - C$ and $|t| \leqslant C$.

Observe that v_4 is a solution to the equation obtained by choosing a new letter y, substituting $\alpha = s^{-1}y^{-1}tyr^{-1}$ for x in E and reducing the result. To describe the reduction of $E(\alpha)$ write $t = t_1t_2t_1^{-1}$ with t_2 freely reduced. For any $u \in \Sigma^*$ free reduction of $\alpha^{\pm 1}u\alpha^{\pm 1}$ leaves the subwords $t_2^{\pm 1}$ untouched except when $u = \lambda$ and the exponents of the two α's differ. But this case cannot occur because E has no subwords xx^{-1} or $x^{-1}x$. Thus each $t_2^{\pm 1}$ survives free reduction of $E(\alpha)$. The same argument together with the fact that E is cyclicly reduced shows that each $t_2^{\pm 1}$ survives cyclic reduction of $E(\alpha)$.

By the preceding argument the cyclic reduction, E', of $E(\alpha)$ has length at least d. Since $E(\alpha)$ reduces to λ when v_4 is substituted for y, y or y^{-1} must occur in E'. In fact there must be an even number of occurrences of y^ϵ, and they must alternate in sign. With one more conjugation if necessary so that E' begins with $y^{\pm 1}$, E' becomes an equation in y with solution v_4.

There are at most $4dC$ letters in $E(\alpha)$ besides the y's. Consequently the length of the coefficients in E' is bounded above by $4dC$. Either Lemma 4 or the statement about solutions for $d \leqslant 2$ implies that $v_4 \in q_1 q_2^* q_3^* q_4$ with $|q_j| \leqslant 4dC$. Hence $v = s^{-1} v_4^{-1} t v_4 r^{-1}$ is contained in a set of the required form.

It remains to consider the case $z = v^{-1} u_1 v u_2 v$ and $|v_2| < |v|/2$. The argument used in the proof of Lemma 4 yields $v_1 = p_1 p_2^k$. Hence v_2 extends to a prefix of $v_2 u_2 p_1 p_2^k v_2$ freely equal to λ. As $|v_2| < |v|/2$, we see that v_2 extends to a prefix of $v_2 u_2 p_1 p_2^k$ freely equal to λ. The desired result follows by a straightforward argument. □

The following lemma is the last step in the proof of Theorem 1.

LEMMA 6. *The solutions to E are a finite union of sets of the form*

$$\{p_1 p_2^i p_3^j p_4 p_5^k p_6^l p_7 \mid (i,j,k,l) \in S\}$$

where S is a semilinear subset of N^4.

PROOF. By the preceding results it suffices to show that for any choice of $\{p_i\}$ the set $\{(i,j,k,l) \mid E(p_1 p_2^i p_3^j p_4 p_5^k p_6^l p_7) \sim \lambda\}$ is semilinear. First consider substitutions in which the exponents i, j, k, l are allowed to vary for different occurrences of x^ϵ in E. There will be $4d$ exponents $i_1, j_1, k_1, l_1, \ldots, i_d, j_d, k_d, l_d$. Let T be the set of $4d$–tuples for which

$$u_1 (p_1 p_2^{i_1} p_3^{j_1} p_4 p_5^{k_1} p_6^{l_1} p_7)^{\epsilon_1} \cdots u_d (p_1 p_2^{i_n} p_3^{j_n} p_4 p_5^{k_n} p_6^{l_n} p_7)^{\epsilon_d} \sim \lambda.$$

The set of all words of this type is

$$L_1 \cap w_1 (p_1 p_2^* p_3^* p_4 p_5^* p_6^* p_7)^{\epsilon_1} \cdots w_n (p_1 p_2^* p_3^* p_4 p_5^* p_6^* p_7)^{\epsilon_n}$$

and so T is semi–linear by Lemma 2. Imposing the condition that appropriate indices agree is equivalent to intersecting T with linear subsets of N^{4d}, and S is the projection of that intersection to a subset of coordinates. □

References

[1] K. Appel, *One-variable equations in free groups.* Proc. Amer. Math. Soc., **19** (1968), 912–918.

[2] J.-M. Autebert, J. Bersteland and L. Boasson, *Context-free languages and pushdown automata*, *in* Handbook of Formal Languages, vol. 1, Springer Verlag, 1997.

[3] I. Chiswell and V. N. Remeslennikov, *Equations in free groups with one variable I*, J. Group Theory, **3** no. 4 (2000), 445–466.

[4] R. Gilman, *On the definition of word hyperbolic groups*, Math. Z., **242** (2002), 529–541.

[5] R. Gilman, *Formal Languages and their Application to Combinatorial Group Theory*, Contemp. Math., Amer. Math. Soc., to appear.

[6] R. H. Gilman, A. G. Myasnikov, A. Kvaschuk and V. N. Remeslennikov, *Parametric solutions of one-variable equations*, preprint.

[7] S. Ginsburg and E. Spanier, *Bounded ALGOL-like languages*, Trans. Amer. Math. Soc., **113** (1964), 333–368.

[8] J. Hopcroft and J. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, 1979.

[9] A. Lorenc, *Coefficient-free equations in free groups*, (Russian) Dokl. Akad. Nauk SSSR, **160** (1965), 538–540.

[10] R. Lyndon, *Equations in free groups*, Trans. Amer. Math. Soc., **96** (1960), 445–457.
[11] D. Muller and P. Schupp, *Groups, the theory of ends and context-free languages* J. Computer and System Sci., **26** (1983) 295–310.
[12] G. Rozenberg and A. Salomaa eds., Handbook of Formal Languages, vols. 1–3, Springer Verlag, 1997.

Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken, NJ 07030
E-mail address: rgilman@stevens.edu

Department of Mathematics and Statistics, McGill University, Montreal, QC, Canada, H3A2K6
E-mail address: alexeim@att.net