APPLYING GROEBNER BASIS TECHNIQUES TO GROUP THEORY

LANDON RABERN

Abstract. We apply the machinery of Groebner bases to finitely presented groups. This allows for computational methods to be developed which prove that a given finitely presented group is not n-linear over a field k assuming some mild conditions. We also present an algorithm which determines whether or not a finitely presented group G is trivial given that an oracle has told us that G is n-linear over an algebraically closed field k.

Lemma 1. *Given a group presentation $G = \langle g_1, \ldots, g_m | r_1, \ldots, r_t \rangle$ there is an algorithm to determine if a word in $\{g_1, \ldots, g_m, g_1^{-1}, \ldots, g_m^{-1}\}$ is trivial under all n-dimensional linear representations of G over an algebraically closed field K. Moreover, the result does not depend on the specific field K, but only on its characteristic.*

Proof. To each g_k we assign an $n \times n$ matrix (x_{ij}^k) of variables. Similarly to each g_k^{-1} assign a matrix of variables (d_{ij}^k). We will work over the polynomial ring $K[x_{ij}^k, d_{ij}^k \mid 1 \leq k \leq m, 1 \leq i, j \leq n]$ in $2mn^2$ variables. Substituting our variable matrices into the relations $\{g_1 g_1^{-1}, g_1^{-1} g_1, \ldots, g_k g_k^{-1}, g_k^{-1} g_k, r_1, \ldots, r_t\}$ and setting them equal to the identity matrix yields $(2k + t)n^2$ equations in $K[x_{ij}^k, d_{ij}^k \mid 1 \leq k \leq m, 1 \leq i, j \leq n]$. Let I be the ideal generated by these equations, then $V(I)$ is precisely the set of all n-dimensional linear representations of G over K. Now let w be a word in $\{g_1, \ldots, g_m, g_1^{-1}, \ldots, g_m^{-1}\}$. Substituting our variable matrices into w and setting the result equal to the identity matrix yields n^2 equations $\{f_1, \ldots, f_{n^2}\}$ which are all in $I(V(I))$ if and only if w is trivial in every n-dimensional representation of G over K. Since K is algebraically closed, the Nullstellensatz (see [1], [2] or [3]) gives $I(V(I)) = \sqrt{I}$ and we have reduced the problem to testing for radical membership. Now Gröbner basis techniques allow for testing radical membership and we are done (see [2] or [1]). All the coefficients in the equations being worked with lie in the prime subfield of K and the radical membership test requires no calculations to leave the prime subfield. Hence the result depends only on the characteristic of K. $\square$

We note that this algorithm can be quite inefficient since it requires the computation of a Gröbner basis. The common method of computation (Buchberger's algorithm or some variant) has been shown to have worst case complexity which is a double exponential in the number of variables (see [2]). The same note applies to the other algorithms (and "computational methods" – algorithms minus the guarantee of termination) presented here as they require computation of Gröbner bases as well.

Definition 2. Let K be an algebraically closed field of characteristic p. For a finitely presented group G, we define

$$N_n^p(G) = \bigcap\{N \trianglelefteq G \mid G/N \hookrightarrow GL_n(K)$$

Lemma 1 says that membership in $N_n^p(G)$ is decidable and also that we are justified in not including the field in our notation.

Corollary 3. *The word problem is decidable for f.p. residually linear groups.*

Proof. Assume we are given a word w in G. Note that if w is non-trivial, then there is some (n, p) for which $w \notin N_n^p(G)$ (since G is residually linear). Run through pairs (n, p) using the diagonal ordering, testing whether or not $w \in N_n^p(G)$. If w is non-trivial, we will hit upon a pair (n, p) demonstrating this in finite time. Now interlace this with the disc diagram algorithm for enumerating trivial words and we have a complete algorithm for solving the word problem. □

Since residually finite groups are residually linear, this gives a new method for solving the word problem in f.p. residually finite groups. Also, f.p. residually linear groups are residually finite since f.g. linear groups are residually finite by a result of Malcev (see [4]). That is, we have not solved the word problem for any new groups.

We will now specialize to characteristic zero to avoid unnecessary notation. The same results hold with identical proofs for positive characteristic. We may as well work over $\mathbb{C}$ for now.

We repeat the construction of the variety of representations as in Lemma 1, giving names to things along the way. Given a group presentation $G = \langle g_1, \ldots, g_m | r_1, \ldots, r_t \rangle$, we construct a variety in $\mathbb{C}^n$ for each $n \geq 1$. Fix $n \geq 1$. To each g_k assign an $n \times n$ matrix $X_k = (x_{ij}^k)$ of variables. Similarly to each g_k^{-1} assign a matrix of variables $D_k = (d_{ij}^k)$. Substitute these variable matrices into the relations $\{g_1 g_1^{-1}, g_1^{-1} g_1, \ldots, g_k g_k^{-1}, g_k^{-1} g_k, r_1, \ldots, r_t\}$ and set them equal to the identity matrix to get $(2k+t)n^2$ equations in $R_n = \mathbb{C}[x_{ij}^k, d_{ij}^k \mid 1 \leq k \leq m, 1 \leq i,j \leq n]$. Now our variety V is the zero set of these equations. We call V the *n-dimensional representation variety* of G over $\mathbb{C}$ and denote it by V_n. The corresponding ideal $I(V_n)$ will be denoted I_n.

Lemma 4. *We have homomorphisms $\phi_n : G \to GL_n(R_n/I_n)$ given by mapping g_i to the equivalence class of X_i and g_i^{-1} to the equivalence class of D_i. Moreover,* $\ker(\phi_n) = N_n^0$.

Proof. First note that the equivalence class of each of $\{X_1, \ldots, X_k, D_1, \ldots, D_k\}$ lies in $GL_n(R_n/I_n)$ since the equations forcing invertibility are in I_n. Also, the equations forcing the relations in the presentation of G are I_n. Hence $\{X_1, \ldots, X_k, D_1, \ldots, D_k\}$ generates a quotient of G as a subgroup of $GL_n(R_n/I_n)$, and ϕ_n is precisely the quotient map. By construction, the kernel is everything which maps to the identity matrix under every n-dimensional representation; namely, N_n^0. □

Note that this need not be a proper linear representation since R_n/I_n need not be an integral domain. However, since $\mathbb{C}$ is algebraically closed, we have a minimal decomposition $I_n = P_1 \cap \ldots \cap P_f$ into prime ideals which we can use to decompose ϕ_n into a direct sum of proper linear representations.

Lemma 5. *We have a decomposition of $\phi_n : G \to GL_n(R_n/I_n)$ as $\phi_n = \phi_n^1 \oplus \ldots \oplus \phi_n^f$, where each $\phi_n^i : G \to GL_n(R_n/P_i)$ is a proper linear representation.*

Proof. From the canonical embedding of $R_n/P_1 \cap \ldots \cap P_f$ into $R_n/P_1 \times \ldots \times R_n/P_f$, we get an embedding of $GL_n(R_n/P_1 \cap \ldots \cap P_f)$ into $GL_n(R_n/P_1) \times \ldots \times GL_n(R_n/P_f)$. Take ϕ_n^i to be the i-th coordinate of this map composed with ϕ_n. □

Theorem 6. *G/N_n^0 is linear over some field F of characteristic zero.*

Proof. Since $R_n/P_1, \ldots, R_n/P_f$ are all integral domains of the same characteristic, there is some field F into which they all embed (e.g. an extension of the algebraic closure of the prime subfield having trancendence degree at least that of any of the R_n/P_i) . Hence we may embed $GL_n(R_n/P_1) \times \ldots \times GL_n(R_n/P_f)$ into $GL_{nf}(F)$. Composing this embedding, the one in the previous lemma, and ϕ_n gives the desired faithful linear representation. □

Corollary 7. *G is linear over some field F of characteristic zero if and only if $N_n^0 = \{1\}$ for some n.*

Proof. Immediate. □

We can do a bit better by finding the smallest possible f in Lemma 5.

Definition 8. Let G be a f.p. group. For any algebraically closed field k of characteristic zero, we may compute the ideal I_n and determine a minimal decomposition $I_n = P_1 \cap \ldots \cap P_{f(k)}$. Let $Irr(G, n) = \min\{f(k) \mid k$ an algebraically closed field of characteristic zero $\}$.

With this definition, Theorem 6 can be improved to the following.

Theorem 9. *G/N_n^0 is $Irr(G,n)n$-linear over some field F of characteristic zero.*

Theorem 10. *There is a computational method which has as input:*

1. *A f.p. group G.*
2. *An algorithm to solve the word problem in G.*
3. *An integer $n \geq 1$.*

and terminates outputting "G is not n-linear over any field of characteristic zero" as long as G is not $Irr(G,n)n$-linear over some field F of characteristic zero.

Proof. Since we have an algorithm to solve the word problem in G, we can start enumerating non-trivial words and testing if they are in N_n^0. If we find a non-trivial word in N_n^0, then we can conclude that G is not n-linear over any field of characteristic zero since this word is trivial in every n-dimensional representation of G. Now if G is not $Irr(G,n)n$-linear over a field of characteristic zero, then $N_n^0 \neq \{1\}$ by Theorem 9. Hence there is some non-trivial word in there and our enumeration will hit upon it in finite time. □

Lemma 5 says that the representation in Lemma 4 breaks down into f n-dimensional representations over integral domains of characteristic zero. For a fixed algebraically closed field k, we can actually compute Gröbner beses for the prime's in the decomposition $I_n = P_1 \cap \ldots \cap P_f$. Thus we can actually do computations with our representations $\phi_n^i : G \to GL_n(R_n/P_i)$.

Lemma 11. *If a f.p. group G is n-linear over an algebraically closed field k, then ϕ_n^i is faithful for some i.*

Proof. Let $z \in V_n$ be a faithful representation of G. Then $z \in V(P_i)$ for some i. That is, z is a root of every polynomial in P_i. If a word is trivial under ϕ_n^i, then all of the polynomial equations that result upon multiplying the matrices lie in P_i. Hence all of these polynomial equations have z as a root and thus the word was trivial in G since z is faithful. □

Theorem 12. *There is a computational method which has as input:*

1. *A f.p. group G.*
2. *An algorithm to solve the word problem in G.*
3. *An algebraically closed field k of characteristic zero.*
4. *An integer $n \geq 1$.*

and terminates outputting "G is not n-linear over k" as long as G is not n-linear over some field F of characteristic zero.

Proof. First compute the minimal decomposition of I_n into prime ideals. By Lemma 11, all we need to do is show that none of the ϕ_n^i are faithful. Enumerate non-trivial words and test triviality under the ϕ_n^i. If G is not n-linear over some field F of characteristic zero, then none of the ϕ_n^i are faithful, so this process will terminate in finite time. $\square$

We can also get some results about the non-existence of algorithms to test if a group is linear. The following theorem is trivially true if we *have* an n-dimensional representation of G over k; however, we only assume that G *is* n-linear over k – perhaps an oracle told us so.

Theorem 13. *Given a f.p. group G which is n-linear over an algebraically closed field k, there is an algorithm to decide whether or not G is trivial.*

Proof. First note that I_n is maximal if and only if $V_n = \{$ trivial representation $\}$. Since G has a faithful n-dimensional representation, this holds if and only if G is trivial. So we can determine whether or not G is trivial by determining whether or not I_n is maximal. To do this, with some fixed ordering, compute a reduced Gröbner basis for I_n. Then this basis looks like $\{x_1 - a_1, \ldots, x_r - a_r\}$ if and only if I_n is maximal. $\square$

Since being n-linear over k is a Markov property (see [4]), we know that there is no algorithm to decide if a f.p. group G is n-linear over a given algebraically closed field k. We give another proof of this.

Corollary 14. *There is no algorithm to decide if a f.p. group G is n-linear over a given algebraically closed field k.*

Proof. Assume, to get a contradiction, that we had such an algorithm. Then given a f.p. group G, we run the algorithm and if it says G is not n-linear over k, then we know that G is non-trivial. If it says that G is n-linear over k, then by Theorem 13 we can determine whether or not G is trivial. Hence, we have an algorithm to decide whether or not a f.p. group is trivial. There is no such algorithm, so this gives the desired contradiction. $\square$

References

[1] William W. Adams, Philippe Loustaunau. An Introduction to Grobner Bases. Graduate Studies in Mathematics, Volume 3. American Mathematical Society (1994).

[2] David Cox, John Little, Donal O'Shea. Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer-Verlag (1996).

[3] Thomas W. Hungerford. Algebra. Graduate Texts in Mathematics, No. 73. Springer-Verlag (1974).

[4] Charles F. Miller III. Decision problems for groups - a survey and reflections. Algorithms and Classification in Combinatorial Group Theory. MSRI Publications No. 23, Springer-Verlag (1992), 1-59.

Department of Mathematics, UC Santa Barbara
E-mail address: `landonr@math.ucsb.edu`