Computing solutions to systems of equations over free and hyperbolic groups

Daniel Groves and Henry Wilton

28th March 2008

1. Elementary Theory

If Γ is a group, Theory(Γ) is defined to be the set of first-order logical sentences that are true in Γ, using only the group elements and operations.

Example 1 *The group Γ is abelian if and only if the sentence*

$$\forall\ x, y\ ([x, y] = 1)$$

is in Theory(Γ).

Example 2

$$\forall\ x\ \exists\ n\ (x^n = 1)$$

is not a valid sentence.

Exercise 3 *If $m \neq n$ then*

$$\text{Theory}(\mathbb{Z}^m) \neq \text{Theory}(\mathbb{Z}^n).$$

What about non-abelian free groups F_n?

Theorem 4 (Kharlampovich–Miasnikov, Sela) *Whenever* $m, n > 1$,

$$\text{Theory}(F_m) = \text{Theory}(F_n).$$

Kharlampovich and Miasnikov go on to prove that the elementary theory of free groups is *decidable*—that is, there is an algorithm that determines if a given sentence is true or false.

Sela's techniques extend to cover torsion-free (word-)hyperbolic groups.

Question 5 *Is the elementary theory of a torsion-free hyperbolic group decidable?*

2. Equations over groups

The simple sort of sentence is an equation, so the first step is to study the solutions to systems of equations over groups. Consider a finite set Φ of equations

$$w_i(x_1, \ldots, x_n) = 1$$

in n unknowns over a group Γ. Let G_Φ be the group with presentation

$$\langle x_1, \ldots, x_n | w_i(x_1, \ldots, x_n) \rangle.$$

Exercise 6 *The set of solutions to Φ is in bijection with*

$$\mathrm{Hom}(G_\Phi, \Gamma).$$

So finitely presented groups correspond naturally to varieties over Γ.

Let's fix attention on $\Gamma = F$ a non-abelian free group.

Definition 7 *A finitely generated group L is* fully residually free *or a* limit group *if, whenever $g_1, \ldots, g_n \in L \setminus 1$ there exists a homomorphism $f : L \to F$ such that*

$$f(g_i) \neq 1$$

for each i.

Note that the choice of F does not matter.

Theorem 8 (K–M,S) *For every finitely generated group G there is a finite set of limit group quotients*

$$\{q_i : G \to L_i\}$$

such that any homomorphism $f : G \to F$ factors as

$$G \xrightarrow{q_i} L_i \to F.$$

This can be rephrased as the assertion

$$\mathsf{Hom}(G, F) = \bigcup_i q_i^* \mathsf{Hom}(L_i, F).$$

Limit groups correspond to irreducible varieties.

3. Enumeration

Theorem 9 (Groves–W) *The set of limit groups is recursively enumerable.*

That is, there is a Turing machine that outputs a list of presentations of limit groups. A presentation of every limit group appears on this list.

This answers a question of Delzant.

The most interesting corollaries of this come when we combine our theorem with Makanin's Algorithm.

Theorem 10 (Makanin) *There is an algorithm that takes as input a system of equations and inequations over F and determines if the system has a solution.*

Corollary 11 *There is an algorithm that takes as input a presentation* $\langle X \mid R \rangle$ *for a group* G *and outputs a finite set of limit group quotients*

$$\{q_i : G \to L_i\}$$

with the property that every homomorphism $G \to F$ *factors through some* q_i*.*

Proof: Using our theorem, we can list all finite sets of limit group quotients

$$\{q_i : G = \langle X \mid R \rangle \to L_i = \langle X \mid S_i \rangle\}.$$

The statement that every homomorphism factors through some q_i is equivalent to the system of equations

$$\forall X \subset F \ (R(X) \Rightarrow S_1(X) \vee \ldots \vee S_n(X)).$$

This can be checked by Makanin's Algorithm. **QED**

Of course, there is no algorithm to tell if an arbitrary group presentation represents the trivial group. But with a solution to the word problem, there clearly is. Combining our theorem with Makanin's Algorithm, we get a similar result for limit groups and, perhaps more surprisingly, free groups.

Corollary 12 *There is an algorithm that takes as input a finite presentation for a group* G *and a solution to the word problem in* G*, and determines whether* G *is a limit group.*

Corollary 13 *There is an algorithm that takes as input a finite presentation for a group* G *and a solution to the word problem in* G*, and determines whether* G *is a free group.*

4. Hyperbolic groups

Now let Γ be a (torsion-free) hyperbolic group. The work of Rips, Sela and Dahmani has made inroads into an algorithmic understanding of equations and inequations over Γ.

Theorem 14 (Dahmani, Sela) *There is an algorithm that takes as input a finite set of equations and inequations over Γ and determines whether the system has a solution.*

If the system does not use constants then Γ acts naturally by conjugation on the set of solutions, so if there is one then there are infinitely many. But how many conjugacy classes are there?

Theorem 15 (Groves-W) *There is an algorithm that takes as input a finite set of equations and inequations (without constants) over Γ and determines whether the system has infinitely many conjugacy classes of solutions.*

We can define Γ-limit groups to be 'fully residually Γ' groups. This includes all fg subgroups of Γ! So there are considerable technical difficulties. Many fundamental problems are unsolvable, and Γ-limit groups can be badly behaved: they may not be finitely presented, or admit a nice geometry, for instance.

Definition 16 *A subgroup H of Γ is called* immutable *if there are only finitely many conjugacy classes of embeddings $H \hookrightarrow \Gamma$.*

For instance, if Γ is the fundamental group of a closed hyperbolic 3-manifold then it follows from Mostow Rigidity that Γ is an immutable subgroup of itself.

Theorem 15 enables us to get some sort of algorithmic purchase on immutable subgroups.

Corollary 17 *There is a Turing machine that outputs a list of all finite subsets of* Γ *that generate immutable subgroups.*