Quadratic equations in hyperbolic groups are NP-complete

Alina Vdovina (joint results with O.Kharlampovich, A. Mohajeri, A. Taam)

9 March 2016

History

- Malcev (1962), Wicks (1962): one commutator equations
- Comerford, Edmunds (1981) : notion of canonical forms
- Lyndon, Schupp (1977): quadratic systems of words
- Schupp (1997): quadratic equations in small cancellation groups
- Stallings, Culler (1980) : using surfaces to solve equations in groups
- Olshanskii, Grigorchuk, Kurachanov (1989): if the number of variables is fixed there is a polynomial time algorithm for free groups
- Grigorchuk, Lysenok (1992): hyperbolic groups

- Kharlampovich, Lysenok, Myasnikov, Toikan (2009): deciding if a quadratic equation over a free group is satisfiable is NP-complete
- Kharlampovich, Vdovina and Lysenok, Myasnikov (2011): Quadratic estimates for the length of minimal solutions of orientable quadratic equations in free groups, degree 4 for non-orientable.
- In this talk: the work for hyperbolic and toral relatively hyperbolic groups.

Theorem

Let Γ be a torsion-free hyperbolic group given by a generating set A and a finite number of relations. It is possible to compute a constant N with the property that if a quadratic equation $Q(X, A) = 1$ is solvable in Γ, then there exists a solution ϕ such that for any variable x, $|\phi(x)| \leq N|Q|^3$ if Q is orientable, $|\phi(x)| \leq N|Q|^4$, if Q is non-orientable.

Definition

A group G that is hyperbolic relative to a collection $\{H_1, \ldots, H_k\}$ of subgroups (see Section 4 for a definition) is called *toral* if $H_1, \ldots, H_k$ are all abelian and G is torsion-free.

Theorem

Let Γ be a toral relatively hyperbolic group with generating set A. It is possible to compute a constant N with the property that if a quadratic equation $Q(X, A) = 1$ is solvable in Γ, then there exists a solution ϕ such that for any variable x, $|\phi(x)| \leq N|Q|^5$ if Q is orientable, $|\phi(x)| \leq N|Q|^{12}$, if Q is non-orientable.

Complexity Theory

Definition

Problem P is Polynomial-time reducible to problem Q if whenever P has a solution, such a solution can be obtained from a solution of Q in polynomial time.

Definition

Class NP is the class of all decision problems for which the ”yes”-instances are recognizable in polynomial time by a non-deterministic Turing machine. (Easy to verify a given solution.)

Complexity Theory

Definition

A problem P is NP-complete if it is in class NP and any other problem in class NP is reducible to P in polynomial-time. In other words, P is at least as hard as any other problem in class NP.

Definition

A problem P is NP-hard if any NP-complete problem is polynomial time Turing reducible to P.

Theorem

Let $E(X) = 1$ be a quadratic equation in a non-elementary hyperbolic group Γ with the set of variables X. Then the problem of deciding if a quadratic equation over Γ is satisfiable, is NP-complete.

Main ingredients of the proofs

- Wicks forms in free groups
- Quadratic sets of words
- Products of commutators and squares in free products
- Multi-forms in free products
- Estimates for minimal solutions in free groups
- Estimates for minimal solutions in hyperbolic groups
- Bin packing problem

Definition

Let G be a group and w be an element of its commutator subgroup. We define the *orientable genus* $g(w)$ of w as the least positive integer g such that w is a product of g commutators in G.

Definition

We define the *non-orientable genus* $g(w)$ of w as the least positive integer n such that w is a product of g squares in G.

Definition

An *orientable Wicks form* is a cyclic word $w = w_1 w_2 \dots w_{2l}$ (a cyclic word is the orbit of a linear word under cyclic permutations) in some alphabet $a_1^{\pm 1}, a_2^{\pm 1}, \dots$ of letters $a_1, a_2, \dots$ and their inverses $a_1^{-1}, a_2^{-1}, \dots$ such that

(i) if a_i^{ϵ} appears in w (for $\epsilon \in \{\pm 1\}$) then $a_i^{-\epsilon}$ appears exactly once in w,

(ii) the word w contains no cyclic factor (subword of cyclically consecutive letters in w) of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ (no cancellation),

(iii) if $a_i^{\epsilon} a_j^{\delta}$ is a cyclic factor of w then $a_j^{-\delta} a_i^{-\epsilon}$ is not a cyclic factor of w (substitutions of the form $a_i^{\epsilon} a_j^{\delta} \longmapsto x, \quad a_j^{-\delta} a_i^{-\epsilon} \longmapsto x^{-1}$ are impossible).

Orientable circuits

Let Γ be a connected cubic graph, with multiple edges allowed. Orientation of edges is arbitrary but fixed.

Definition

Orientable circuit is a path in a graph which runs through each edge exactly once in each direction, but never immediately after its inverse.

Does it always exist?

Inductive step to single out a commutator

$$C = u_1 a^{-1} b u_2 c^{-1} a u_3 b^{-1} c u_4 =$$

$$[u_1 a^{-1} c u_2^{-1} u_3^{-1} u_1^{-1}, u_1 u_3 u_2 c^{-1} b u_3^{-1} u_1^{-1}]$$

$$u_1 u_3 u_2 u_4$$

Theorem

Let C be an orientable word of genus g in a free group F. Then C can be presented in the form $[a_1, b_1] \dots [a_g, b_g]$, where $|a_i| < 2|C|, |b_i| < 2|C|, |d_i| < 2|C|$ for $i = 1, ..., g$.
If C is non-orientable then C can be represented as a product of squares $a_1^2 ... a_g^2$ with $|a_i| \leq 3|C|^2$.

Theorem

Let W_1,...,W_k be an orientable quadratic set of words of genus g, and $C_1, \ldots, C_k$ be elements of a free group F such that the system $W_i = C_i,\ i = 1, \ldots, k$ has a solution in F and $\sum_{i=1}^{k} |C_i| = s$ in F. Then some product of conjugates of C_i's in any order can be presented as a product of at most g commutators of elements in F with lengths strictly less then $2s$, and conjugating elements also have length bounded by $2s$.

Theorem

Let $W_1,...,W_k$ be a non-orientable quadratic set of words of genus g, and $C_1, \ldots, C_k$ be elements of a free group F such that the system $W_i = C_i,\ i = 1, \ldots, k$ has a solution in F and $\sum_{i=1}^{k} |C_i| = s$ in F. Then some product of conjugates of C_i's in any order can be presented as a product of at most g squares $a_1^2 ... a_g^2$ with $|a_i| \leq 12s^4$ and conjugating elements have length bounded by $2s^2$.

Definition

A quadratic equation E with variables $\{x_i, y_i, z_j\}$ and non-trivial coefficients $\{C_i, C\} \in F(A)$ is said to be in *standard form* if its coefficients are expressed as freely and cyclically reduced words in A^* and E has either the form:
$\prod_{i=1}^{g}[x_i, y_i]\prod_{j=1}^{m-1} z_j^{-1} C_j z_j C = 1$ where $[x, y] = x^{-1}y^{-1}xy$, in which case we say it is orientable
or it has the form $\prod_{i=1}^{g} x_i^2 \prod_{j=1}^{m-1} z_j^{-1} C_j z_j C = 1$ in which case we say it is non-orientable.

Example

Let a solution of a quadratic equation be obtained from the non-orientable multi-form by a permissible substitution:

$$V_1 = A\xi_1 ED\psi_1 C^{-1} B\xi_3 A^{-1} FB\xi_2 EG_1 G_2 H_1 O_2 O_1^{-1} I_1,$$

$$V_2 = C\psi_2 H_2 O_2 ZG_2 I_2 I_1 F,$$

$$V_3 = D\psi_3 H_2 H_1^{-1} I_2 O_1 ZG_1,$$

where $\xi_1\xi_2^{-1}\xi_3 = U_1, \psi_1\psi_2\psi_3^{-1} = U_2$, (U_1, U_2) has orientable genus 3 in some free factor G_i, and $|V_1| + |V_2| + |V_3| = s$.

Example

Now we have to bring the multi-form to a quadratic set in a free group. First of all we perform augmentations, and our multi-form is as follows:

$$V_1' = AE_1DC_1^{-1}B_1U_1A^{-1}FB_1E_1G_1G_2H_1O_2O_1^{-1}I_1,$$

$$V_2' = C_1H_3O_2ZG_2I_2I_1F,$$

$$V_3' = DU_2^{-1}H_3H_1^{-1}I_2O_1ZG_1,$$

where $E_1 = \xi_1 E, B_1 = B\xi_2\xi_1^{-1}, C_1 = C\psi_1^{-1}$, and $H_3 = \psi_1\psi_2 H_2$.

Example

Without loss of generality, we may assume that $U_2 = UU_1^{-1}$, where $U = [b_1, c_1][b_2, c_2][b_3, c_3]$. Substituting U_2 by UU_1^{-1}, we get a quadratic set of non-orientable genus 15 for the free group. The length of every letter in V_1', V_2', V_3' is bounded by s, and every letter in U is bounded by $2|U_1| + 2|U_2| \leq 2s$. Using the results for the free group, we get that the length of the solution is bounded by a polynomial of degree 8 in s.

Theorem

Let h be an orientable word of genus g in a hyperbolic group Γ. Let M be the number of elements in Γ represented by words of length at most 4δ in $F(X)$ (δ is the hyperbolicity constant), $l = \delta(log_2(12g-6)+1)$. Then h can be presented in a form $[a_1, b_1]\dots[a_g, b_g]$, where $|a_i| < 2|h| + 3(12g-6)(12l+M+4)$, $|b_i| < 2|h| + 3(12g-6)(12l+M+4)$ for $i = 1, ..., g$.

Theorem

Let $W_1,...,W_k$ be a quadratic set of words of orientable genus g and and $C_1, \ldots, C_k$ be elements of a hyperbolic group Γ such that the system $W_i = C_i,\ i = 1, \ldots, k$ has a solution in Γ, and $\sum_{i=1}^{k} |C_i| = s$. Let M be the number of elements in Γ represented by words of length at most 4δ in $F(X)$ (δ is the hyperbolicity constant), $l = \delta(log_2(12g - 6) + 1)$. Let $S = (2|h| + 3(12g - 6)(12l + M + 4))^2$ Then some product of conjugates of C_i's can be presented as a product of at most g commutators of elements with lengths strictly less then S, and conjugating elements also have length bounded by S.

Recall that the (exact) bin packing problem is:

Problem

(Exact) Bin Packing

- *INPUT: A s-tuple of positive integers* $(r_1, ...r_s)$ *and positive integers* B, N.
- *QUESTION: Is there a partition of* $\{1, ..., s\}$ *into N subsets* S_i*, with*

$$\{1, ..., s\} = S_1 \sqcup ... \sqcup S_N$$

such that for each i=1,...,N we have

$$\sum_{j \in S_i} r_j = B$$

Let $G = \langle A|R\rangle$ be a non-elementary δ-hyperbolic group. G contains a convex free subgroup $F(b, b_1)$ of rank two. which contains a convex free subgroup $F(b, c, d)$ of rank three. We can assume that b, c, d are cyclically reduced. Given b, c, d, by [Ol93] there are constants λ, C such that any path labeled by b^t, c^t or d^t is (λ, C)-quasigeodesic for all t. There is a constant $R(\delta, \lambda, C)$ such that any (λ, C)-quasigeodesic path is in the R-neighborhood of a geodesic path with the same endpoints. There exists an integer D, such that the normal closure $\mathcal{N} =<< (b^{s_1 D}, c^{s_2 D}, d^{s_3 D} >>$ in G is free for any $s_i > 0$ (also, $G/\mathcal{N}$ is non-elementary hyperbolic). We can choose numbers t_1, t_2 such that t_2 is much larger than t_1 and t_1 is much larger than R. Now let $a = d^D c^{t_1 D} d^D c^{t_2 D} d^D$.

Equation for which problem of finding solution is NP-hard

Now consider the following equation

$$\prod_{j=1}^{s} = x_j^{-1}[a, b^{r_j}]x_j = [a^N, b^B]$$

where r_j, N, B are positive integers, $r_j = r_j' D$ for r_j', N, B from bin packing problem, for all j. Suppose there is a solution to this equation. We will show this implies a bin packing for r_j', N, B.