The Word and Conjugacy Problem in Amalgamated Products

Jonathan Siegel

July 29, 2011

A General Overview

Our work here has concerned the word and particularly the conjugacy problem in various different groups, especially the braid groups. This is due to the fact that such problems, if computationally intensive to solve, could form the basis of a non-commutative cyptosystem. During this study, one particular topic of interest is when and how we can solve the word and conjugacy problems in amalgamated products.

The Free Product of Groups

Definition

Let G and H be groups. Then the free product of G and H, denoted by $G * H$ is the group of reduced strings whose characters are elements of $G \cup H$. A string is reduced using multiplication in either of the groups G or H, that is $g_1 g_2$ is replaced by the single element $g_1 * g_2$ if both $g_1 \in G$ and $g_2 \in G$. The group operation is concatenation.

Remarks

It is clear that a string in the free product is reduced iff its characters come alternatingly from G and H. So $s = g_1 h_1 g_2 h_2 \ldots$.

If $G =< V_G | R_G >$ and $H =< V_H | R_H >$, then $G * H =< V_G \cup V_H | R_G \cup R_H >$.

Amalgamated Products

Amalgamated products are similar to free products except that we can now identify a subgroup of G with a subgroup of H.

Definition

Let G, H, and K be groups and let $\phi : K \to G$ and $\nu : K \to H$ be homomorphisms. Then the amalgamated product of G and H is $G * H / << \phi(k)(\nu(k))^{-1} >>$. So the amalgamated product is the free product factored over the relations $\phi(k) = \nu(k)$ for all $k \in K$.

The Word Problem in Amalgamated Products

Theorem

Let H and K be groups and let G be their amalgamated product over some subgroup L. If the word problem is algorithmically solvable in both H and K and the membership problem is solvable for L, then the word problem in solvable for G.

One solves the word problem by reducing a given word in each of the factor groups as much as possible and then checking whether or not a factor can be reduced using the relations resulting from the amalgamation.

The Conjugacy Problem in Amalgamated Products

The conjugacy problem is not in general solvable in amalgamated products. Nonetheless the following lemma has allowed us to obtain several positive results.

Lemma

Let H and K be groups and let G be their amalgamated product over some subgroup L. So we have $\phi : L \to H$ and $\nu : L \to K$ where both ϕ and ν are injective and we are amalgamating over the image of ϕ and ν. Then G contains a subgroup L^* isomorphic to L and if x and y are two cyclically reduced words which are conjugate, then $l(x) = l(y)$ and there exists a cyclic permutation of y say y^* such that x and y^* are conjuagate by an element c such that $l(c) = 1$. Moreover, if $l(x) = l(y) > 1$, then $c \in L^*$.

Solution for the Conjugacy Problem in certain Amalgamated Products

Theorem

Let G be the amalgamated product of H and K over a subgroup of H and K isomorphic to L. Thus we have maps $\pi : L \to H$ and $\nu : L \to K$. Assume that H and K have solvable conjugacy problem. Also assume that the subgroup L^* of G isomorphic to L has solvable membership problem. Then if L^* is in the center of G, the conjugacy problem in G is solvable.

In particular since the Braid group B_3 satisfies the assumptions of the theorem, we can solve the conjugacy problem in B_3 using this approach.

Conjugacy Problem in Amalgamated Products of Free Groups

Jonathan Siegel

Definition

A cyclic subgroup of a free group F is called maximal if it is not contained in any other cyclic subgroup of F.

Theorem

Let H and K be two free groups on any number of generators. Let G be their amalgamated product over a maximal cyclic subgroup generated by g. Then the conjugacy problem is solvable in G.