Groups and Algorithms
Groupes et algorithmes
(Org: **Inna Bumagin** (Carleton))

INNA BUMAGIN, Carleton University
The conjugacy and the search conjugacy problem in relatively hyperbolic groups.

If u and v are two conjugate elements in a hyperbolic group then the bound on the length of a shortest conjugating element is linear in terms of the lengths of u and v; this was shown by Lysenok in 1989. This estimate leads to an obvious algorithm to solve both the conjugacy and the search conjugacy problems in hyperbolic groups; however, the algorithm has exponential time complexity. In the book by Bridson and Haefliger one finds a polynomial time algorithm to solve the conjugacy problem. Their proof shows the following. There is an easy procedure to choose shorter representatives of the conjugacy classes of u and v. If those representatives are conjugate then the length of a shortest conjugating element is bounded by a constant that depends only on the group presentation. I will explain how these results generalize to relatively hyperbolic groups.

DELARAM KAHROBAEI, City University of New York, City Tech and Graduate Center
Public key exchange using extensions by endomorphisms and matrices over a Galois field

I am presenting a joint work with H.T.Lam and V.Shpilrain. We describe a key exchange protocol based on an extension of a semigroup of matrices over a Galois field by automorphisms (more generally, by endomorphisms). One of its special cases is the standard Diffie-Hellman protocol, which is based on a cyclic group. However, when our protocol is used with a non-commutative (semi)group, it acquires several useful features that make it compare favorably to the Diffie-Hellman protocol. Here we suggest a particular non-commutative semigroup of matrices over a Galois field as the plat- form and show that security of the relevant protocol is based on a quite different assumption compared to that of the standard Diffie-Hellman protocol. Our key exchange protocol with this platform is quite efficient, too: with private keys of size 127 bits and public key of size 1016 bits, the run time is 0.2 s on a typical desktop computer.

JEREMY MACDONALD, Stevens Institute of Technology
Effective coherence in discriminated groups

Subgroups are usually specified by a generating set, but many group-theoretic algorithms require a presentation as (part of) their input. In applying such algorithms to subgroups it is therefore essential that the ambient group be *effectively coherent*, meaning that a finite presentation can always be computed for a finitely generated subgroup. This property fails in hyperbolic groups, but holds with the additional assumption that the group Γ be locally quasi-convex. We show that effective coherence extends to groups G discriminated by Γ. Such groups G are characterized by being embeddable as subgroups of iterated centralizer extensions of Γ, and effective coherence allows for an algorithm to compute this embedding. It also provides algorithms to enumerate all finitely generated groups discriminated by Γ, and to decide whether a given group is discriminated by Γ.

This is joint work with I. Bumagin.

EDUARDO MARTINEZ-PEDROZA, Memorial University
Local Quasiconvexity and Negative Sectional Curvature in Complexes of Groups.

A hyperbolic group is locally quasiconvex if finitely generated subgroups are quasiconvex. We examine conditions on simply connected 2-complexes ensuring local quasiconvexity of groups acting geometrically on them. This extends earlier work of D.Wise on 2-complexes with negative sectional curvature in the case of free actions. Our extension of this result involves a generalization of the notion of combinatorial sectional curvature, a version of the combinatorial Gauss-Bonnet theorem to complexes of groups, and requires the use of ℓ_2-Betti numbers. This is joint work with Daniel Wise.

GRETCHEN OSTHEIMER, Hofstra University
Groups with logspace normal forms

We consider the class of finitely generated groups which have a normal form computable in logspace. We prove that the class of such groups is closed under passing to finite index subgroups, direct products, wreath products, and certain free products and infinite extensions, and includes the solvable Baumslag-Solitar groups, as well as non-residually finite (and hence non-linear) examples. We define a group to be logspace embeddable if it embeds in a group with normal forms computable in logspace. We prove that finitely generated nilpotent groups are logspace embeddable. It follows that all groups of polynomial growth are logspace embeddable.

joint work with Murray Elder and Gillian Elston

DENIS SERBIN, Stevens Institute of Technology
Compression techniques in infinite words

It's known (Plandowski's algorithm) that one can decide if the outputs of two straight-line programs ρ_1 and ρ_2 over a finite alphabet are equal in polynomial time with respect to the total size of the programs $|\rho_1| + |\rho_2|$. Our goal was to generalize Plandowski's algorithm to $\mathbb{Z}[t]$-completion of a free group F (so-called Lyndon's free group $F^{\mathbb{Z}[t]}$). In order to do this we introduced the notion of *generalized straight-line program* (GSLP for short) whose output is a reduced infinite word representing an element of $F^{\mathbb{Z}[t]}$. We adapted Plandowski's algorithm to the case of GSLP's and obtained the same complexity bounds as in the case of standard straight-line programs.

This is joint work with Alexander Ushakov.

VLADIMIR SHPILRAIN, The City College of New York
Solving problems privately

The increasing trend of outsourcing computations and, more generally, problem solving gives rise to various privacy issues. Probably the most famous problem of that kind is Yao's 'two millionaires problem': Alice has a private number a and Bob has a private number b, and the goal of the two parties is to solve the inequality $a < b$? without revealing the actual values of a or b or, more stringently, without revealing any information about a or b other than $a < b$ or $a > b$. In this talk, I will address group-theoretic problems that are similar in spirit.

BENJAMIN STEINBERG, City College of New York
On a conjecture of Karass and Solitar

Karass and Solitar proved in the late 60s that a finitely generated subgroup of a free group has finite index if and only if it intersections non-trivially each non-trivial normal subgroup. They conjectured that the analogous result would hold for free products of non-trivial groups.

We prove the stronger statement that if A, B are non-trivial groups and H is a subgroup of $A * B$ of finite Kurosh rank, then H is finite index if and only if it intersects non-trivially every non-trivial normal subgroup of $A * B$.

The proof is based on the small cancellation theory/Stallings graph proof of the Karass and Solitar theorem for free groups found by Arzhantseva and by Ivanov/Schupp. Here we replace Stallings graphs by an appropriate notion of the core of a covering space in the setting of subgroups of free products.

SVETLA VASSILEVA, McGill University/Stevens Institute
The conjugacy problem in groups and its space complexity

Space complexity has long been the focus of interest in computer science. With the prevalence of vast amounts of data, it has become a major consideration in computations. Every problem which can be decided in logarithmic space can be decided

in polynomial time, but the converse is not known to hold. We consider the complexity of the conjugacy problem in several classes of groups. In particular, we show that the conjugacy problem in free solvable groups, wreath products of groups and Grigorchuk groups is log-space decidable. (Joint work with A. G. Miasnikov)

MING MING ZHANG, Carleton University

On residually toral relatively hyperbolic groups

B. Baumslag proved that a group being fully residually free is equivalent to being residually free and commutative transitive. In this talk, we generalize Baumslag's theorem to the class $\mathcal{R}$ of finitely generated toral relatively hyperbolic groups. Let Γ be a group from $\mathcal{R}$. We also talk about that a finitely generated fully residually-Γ group (or equivalently, Γ-limit group) can be embedded into a group from $\mathcal{R}$; and moreover, examine that every subgroup of Γ is fully residually-$\mathcal{R}$ by constructing an epimorphism.