INTERNATIONAL GROUP THEORY WEBINAR
November 3 2011

SPEAKER: VITALY ROMAN'KOV

OMSK STATE DOSTOEVSKY UNIVERSITY

ALGORITHMIC THEORY OF SOLVABLE GROUPS

Theory – Complexity – Practicality – Perspective

PART I

THEORY

Friendly definitions

Sol = **solvable groups**

$$Th_{Alg}(Sol) = \text{Information}$$

about $Sol-$groups, their elements, subgroups, subsets, structure ...
that can, in principle at least, be obtained by

machine computation:

Turing machines, automata, computers ...

Presentation of groups

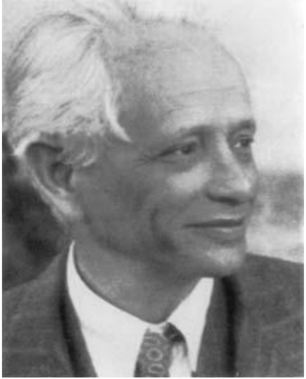
finite or recursive presentation:
$G =< x_1, \ldots, x_n | \{r_\lambda : \lambda \in \Lambda\} >;$

relative presentation in a variety:
$G_{\mathcal{L}} =< x_1, \ldots, x_n | \{r_\lambda : \lambda \in \Lambda\}; \mathcal{L} >$

presentation by generators:
$G = gr(g_1, \ldots, g_n) \leq \bar{G}$

presentation by action: $G = Aut(H)$ or
$G = \pi_1(S)$

Classical decision problems



Max Dehn

Classical decision problems

Word Problem (WP): $w = 1?$

Conjugacy Problem (CP): $\exists x : xgx^{-1} = f?$

Membership Problem (MP): $w \in H \leq G?$

Isomorphism Problem (IP): $G \simeq H?$

Further decision problems

Twisted Conjugacy Problem (TCP): $\exists x : \varphi(x)g = fx$?

Bi-twisted Conjugacy Problem (BTCP):
$\exists x : \varphi(x)g = f\psi(x)$?

where $\varphi, \psi \in Aut(G)$, or more generally, $\varphi, \psi \in End(G)$.

Generation and Presentation Problems:
Find generators or presentation of a subgroup, centralizer, automorphism group and so on

Further decision problems

Let F be a free group of infinite countable rank rank with basis $X_n = \{x_1, ..., x_n, ...\}$ and $G[X] = G * F$ be the free product of any group G with F.

Equation Problem (EqP): for arbitrary $w \in G[X]$ answer if $\exists x_1, ..., \exists x_n | w = 1$?

Endomorphism (Automorphism) Problem (EndoP or AutoP): for arbitrary pair $g, f \in G$ answer if $\exists \varphi \in End(G)\ (Aut(G)) | \varphi(g) = f$?

Epimorphism Problem (EpiP): for arbitrary pair of groups G, H (in a given class of groups) answer if $\exists \varphi \in Hom(G, H) : \varphi(G) = H$?

Polycyclic (in particular, finitely generated nilpotent) groups

Polycyclic (in particular, finitely generated nilpotent) groups

Philip Hall

Philip Hall

Philip Hall at the time of his election to the Royal Society

facing p. 603

Philip Hall's approach

polycyclic groups $\leftrightarrow$ commutative algebra

Ph. Hall established a remarkable connection between the theory of polycyclic groups and commutative algebra.

He noted that, since the class of finitely presented (f.p.) groups is closed under extensions, polycyclic groups are f.p. These groups satisfies *max*, the maximal condition for subgroups, and they admit many other nice properties.

Mal'cev's approach

algorithms $\leftrightarrow$ residuality

A. Mal'cev showed that residual finiteness w.r.t. some recursive enumerable property **P** of a group G implies decidability of **P** in G.

Classical algorithms.

Classical Decision Problems. Positive Solutions:

- **WP** - Hirsch [1952] (every polycyclic group is residually finite)
- **MP** - Mal'cev [1958] (every polycyclic group is separable)

K.Hirsch 

Classical algorithms.

Classical Decision Problems. Positive Solutions:

- **CP** - Newman [1960] (nilpotent case), Blackburn [1965] (every f.g. nilpotent group is conjugacy separable), Remeslennikov [1969] and Formanek [1976] (every polycyclic group is conjugacy separable)

Classical algorithms.

V.R.  **E.F.** 

Classical algorithms.

IP w.r.t. a given group

Pickel proved that the genus (i.e. the set of all finite homomorphic images) of every f.g. nilpotent group N is finite. Consequently, IP to a fixed f.g. nilpotent group N is decidable.

Classical Decision Problems. Positive Solutions:

- **IP** - Sarkisjan [1979-1980](nilpotent case module the Hasse principle, established (except E_8) by Harder [1969], and for E_8 by Chernousov [1989], Grunewald and Segal [1979-83] (nilpotent case) and Segal [1990] (virtually polycyclic case).

Classical algorithms.

R.S.  **F.G.**  **D.S.** 

Diophantine Problem

Yu. Matijasevich [1970], based on some ideas by J. Robinson, M. Davis and H. Putnam, established negative solution of the well-known Diophantine Problem (Hilbert's Tenth Problem)

M. D., J. R., Yu. M.

Interpretation of Diophantine Problem

V. Roman'kov based on this result to derive undecidability of EqP and EndoP in the classes of free nilpotent and free metabelian groups.

Let $G = N_{r,c}$ be the free nilpotent group of rank r sufficiently large and class $c \geq 6$, or $G = M_r$ be the free metabelian group of rank r sufficiently large.

Then for every Diophantine polynomial

$$D(z_1, ..., z_n) \in \mathbb{Z}[z_1, ..., z_n],$$

we can effectively find two elements $g, f \in G$ such that there is an endomorphism $\varphi \in End(G)$ that $\varphi(g) = f$ if and only if equation

$$D(z_1, ..., z_n) = 0$$

has a solution in $\mathbb{Z}$.

Interpretation of Diophantine Problem

Moreover, we can fix the left side of equation $D(z_1, ..., z_n) = c$, where $c \in \mathbb{Z}$, to obtain non-decidable class of Diophantine equations. Hence, we can fix the element g to obtain non-decidability of the EqP and EndoP in N. The second element f we choose in a cyclic subgroup.

Further algorithms

All the following results were obtained with interpretation of the Diophantine Problem.

Further Decision Problems. **Positive** and **Negative** Solutions:

- **BTCP** - Roman'kov [2010]
- **EqP, EndoP** - Roman'kov [1979]
- **EpiP** - Remeslennikov [1979]
- **Identity Problem** - Kleiman [1979]. There is a solvable variety defined by finitely many laws in which the non-cyclic groups have unsolvable WP.

Further algorithms.

Further Decision Problems. Positive and **Negative** Solutions:

- Eq_1 - Repin [1984]. There exists a f.g. nilpotent group of class 3 in which the EqP for 1−variable equations is undecidable.
- Eq_1P **for free nilpotent groups** - Repin [1984]. In every free nilpotent group N_{rc} of class $c \geq 5 \cdot 10^{10}$ the EqP for 1−variable equations is undecidable.
- EqP **for free nilpotent groups** - Repin [1984]. In every free nilpotent group N_{rc} of rank $r \geq 600$ and class $c \geq 3$ the EqP is undecidable.
- Eq_1 - Repin [1983]. Eq_1P is decidable in every f.g. nilpotent group of class $c \leq 2$.

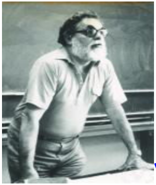
Further algorithms.

Theorem

(G. Baumslag, Cannonito, Robinson, Segal [1991]). Let $G =< x_1, ..., x_n | r_1, ..., r_m >$ be a presentation of a polycyclic group. Then there is a uniform algorithm which, when given a finite subset U of G, produces a f. p. of $gr(U)$.

Hence we can efficiently find a polycyclic presentation of G, the Hirsch number $h(G)$, the Fitting ($Fitt(G)$) and Frattini ($Fratt(G)$) subgroups, the center ($C(G)$), decide if G is torsion-free, and so on.

Further algorithms.

F.C.  **V.R. & D. R.** 

Open questions.

Open questions:

- Is the property of being directly indecomposable decidable for finitely generated nilpotent groups? – Baumslag
- How to compute minimal number of generators of a given polycyclic group? – Kassabov, Nikolov

Finitely generated metabelian groups.

Finitely generated metabelian groups

Finitely generated metabelian groups.

Ph. Hall [1954] proved that every f.g. metabelian group G satisfies max_n (the maximal property for normal subgroups). Hence G is f.p. in $\mathcal{A}^2$ (the variety of metabelian groups).
W. Magnus invented his famous Magnus embedding, which became a very efficient instrument in the theory of solvable groups.

W. Magnus 

Finitely generated metabelian groups.

M.I. Kargapolov

Finitely presented metabelian groups.

Finitely presented metabelian groups. Bieri-Strebel's invariant. Positive Solutions:

- \- Remeslennikov and independently Baumslag [1972] proved that every finitely generated metabelian group is embeddable into finitely presented metabelian group.
- \- Bieri and Strebel [1980] The Bieri-Strebel introduced a geometrical invariant which allowed decide effectively if a given finitely generated metabelian group M is finitely presented, or not.

Finitely presented metabelian groups.

R. Bieri and R. Strebel

Classical algorithms.

Classical Decision Problems. Positive Solutions:

- **WP** - Ph. Hall [1959] (every f.g. metabelian group is residually finite). Timoshenko [1973] - effective algorithm.
- **CP** - Noskov [1982], but is not in general conjugacy separable - Kargapolov and Timoshenko [1973]
- **MP** - Romanovskii [1980], but is not in general finitely separable - Kargapolov and Timoshenko [1973]
- **IP w.r.t.** M_r - Groves and Miller [1986], Noskov [1985]

Classical algorithms.

G.N.  **N.R.**  **E.T.** 

Further algorithms.

Further Decision Problems. **Positive** and **Negative** Solutions:

- **TCP** - Roman'kov, Ventura [2009]
- **EqP, EndoP** - Roman'kov [1979]

Finitely generated metabelian groups.

G. Baumslag 

Finitely generated metabelian groups.

(G. Baumslag, Cannonito, Robinson [1994]). Let $G =< x_1, ..., x_n | r_1, ..., r_m; \mathcal{A}^2 >$. Then:

- There is a uniform algorithm which, when given a finite subset U of G, produces a relatively f. p. of $gr(U)$, its centralizer $C_G(U)$ can be find effficiently. In particular, the center $C(G)$ and the members of the lower central series in G can be given efficiently.
- The set of all torsion elements can be efficiently constructed in the form $u_1 X_1^G u_2 X_2^G ... X_k^G$.
- The Frattini $Frat(G)$ and Fitting $Fitt(G)$ subgroups can be found efficiently

Further algorithms.

Theorem

(Lohrey and Steinberg [2008]). Let M_r be a free non abelian metabelian group of rank r. Suppose **TP** *is a combinatorial tiling problem. Then M_r admits a f.g. submonoid M such that the membership problem w.r.t. M is equivalent to the given* **TP**. *Hence the membership problem w.r.t. f.g. submonoids is undecidable in M_r.*

Further algorithms.

M. Lohrey and B. Steinberg

Open questions.

Open questions:

- Does the **IP** decidable in the class $\mathcal{A}^2$ of all metabelian groups? – well known question.
- Does the **IP** decidable in the class $\mathcal{N}_2 A$? In the class $\mathcal{A}_p\mathcal{A}, p - -$prime? – Kharlampovich.

Finitely generated solvable groups of class ≥ 3.

Finitely generated solvable groups of class ≥ 3

Classical algorithms.

Classical Decision Problems. Negative Solutions:

- **WP, CP, MP, IP** - Remeslennikov [1973] (there is a f.p. in $\mathcal{A}^5$ group G in which the WP is undecidable. IP w.r.t. fixed group is undecidable for f.p. in $\mathcal{A}^7$ groups - Kirkinskii, Remeslennikov [1975].

Classical algorithms.

Classical Decision Problems. Negative Solutions:

- **WP, CP, MP, IP** - Kharlampovich [1981] (there is a f.p. solvable group G of class 3 in which the WP is undecidable. G can be chosen in the variety $\mathcal{Z}\mathcal{N}_2\mathcal{A}$ defined by identity $((x_1, x_2), (x_3, x_4), (x_5, x_6), y) = 1$. The IP in this variety is undecidable too.

O.G. Kharlampovich

Classical algorithms.

Subsequently, this was proved in a different way by G. Baumslag, Gildenhuys, and Strebel [1985, 1986]. They constructed a f.p. solvable of class 3 group G and a recursive set of words $w_1, \dots, w_n, \dots,$ in generators of G such that $w_i^p = 1$ with p a prime and $w_i \in C(G)$ for which there is no algorithm to decide if a given w_i equals the identity in G. This group can also be used to show that the **IP** is undecidable in the f.p. solvable groups of class 3.

Classical algorithms.

Classical Decision Problems. Positive Solutions:

- **WP** - Kharlampovich [1987] The WP is decidable in any subvariety of $\mathcal{N}_2\mathcal{A}$.
- **WP** - Bieri and Strebel [1980] Every f.p. group $G \in \mathcal{N}_2\mathcal{A}$ is residually finite.

Free solvable groups of finite ranks.

Free solvable groups of finite ranks

Classical algorithms.

Classical Decision Problems. Positive and Negative Solutions:

- **WP, CP** - Kargapolov, Remeslennikov [1966], a free solvable group is conjugacy separable - Remeslennikov, Sokolov [1970].
- **MP** - Umirbaev [1995] (when class $d \geq 3$).There are a f.g. not finitely separated subgroups in each non-abelian free solvable group of class $d \geq 3$ - Agalakov [1983].

Classical algorithms.

V.R. & U^3

Elementary theories.

Elementary theories

Finitely generated nilpotent) groups.

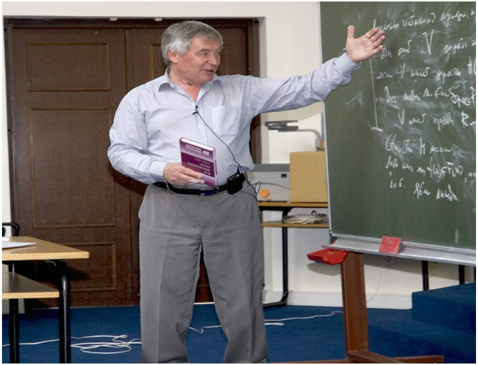
Finitely generated nilpotent groups

Classical decidability problems.

Classical Decidability Problems. Positive and Negative Solutions:

- **Th** - Mal'cev [1960], a free nilpotent group N_{rc} of rank $r \geq 2$ and class $c \geq 2$, a free solvable group S_{rc} of rank $r \geq 2$ and class $d \geq 2$ have undecidable theories.
- **Th** & Th - Ershov [1972] A finitely generated nilpotent group N has decidable theory iff N is virtually abelian.

Classical decidability problems.



Yu.L. Ershov

Finitely generated solvable (in particular polycyclic) groups.

Finitely generated solvable (in particular polycyclic) groups.

Classical decidability problems.

Classical Decidability Problems. Positive and Negative Solutions:

- **Th** & Th - Romanovskii [1972] A virtually polycyclic group P has decidable theory iff P is virtually abelian.
- **Th** & Th - Noskov [1983] A finitely generated virtually solvable group S has decidable theory iff S is virtually abelian.

Universal theories.

Universal theories

Finitely generated nilpotent and metabelian groups.

Finitely generated nilpotent and metabelian groups

Classical decidability problems.

Classical Decidability Problems. Positive and Negative Solutions:

- $Th_{\forall}$ - Roman'kov [1979]. There exists a finitely generated nilpotent metabelian torsion free group with undecidable universal theory. The universal theory of any finitely generated free nilpotent non-abelian group is decidable iff the Diophantine problem for $\mathbf{Q}$ is decidable.
- $Th_{\forall}$ - Chapuis [1995, 1997]. $Th_{\forall}M_r$ of any free metabelian group M_r of a finite rank r is decidable. $Th_{\forall}M_r = Th_{\forall}(\mathbf{Z}wr\mathbf{Z})$.

Free solvable groups of class ≥ 3.

Free solvable groups of class ≥ 3.

Classical decidability problems

Classical Decidability Problems. Positive or Negative Solutions:

- - Chapuis [1998]. If Hilbert's 10th problem has a negative answer for $\mathbf{Q}$, then $Th_{\forall} S_{rd}$ for every free solvable group S_{rd} of rank $r \geq 2$ and class $d > 3$ is undecidable.

O. Chapuis

Finitely generated nilpotent and some other solvable groups.

Have you attended the Remeslennikov's talk?

Algorithmic dimension, constructive models etc.

N. Khisamiev - attend next talk!

PART II

COMPLEXITY

Free solvable groups of finite ranks.

We study the computational complexity of the **WP** in free solvable groups $S_{r,d}$, where $r \geq 2$ is the rank and $d \geq 2$ is the solvability class of the group. Let n be a length of a word (input) $w \in S_{r,d}$. It is known that the Magnus embedding of $S_{r,d}$ into matrices provides a polynomial time decision algorithm for **WP** in a fixed group $S_{r,d}$. Unfortunately, the degree of the polynomial grows together with d, so the uniform algorithm is not polynomial in d.

Free solvable groups of finite ranks: WP.

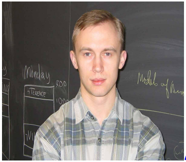
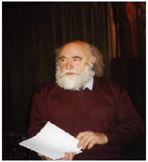
Theorem

(Myasnikov, Roman'kov, Ushakov, Vershik [2010]).

- *The Fox derivatives of elements from $S_{r,d}$ with values in the group ring $\mathbb{Z}S_{r,d-1}$ can be computed in time $O(n^3rd)$.*
- *The* **WP** *has time complexity $O(rn\log_2 n)$ in $S_{r,2}$, and $O(n^3rd)$ in $S_{r,d}$ for $d \geq 3$.*

Free solvable groups of finite ranks: WP.

A.M. 

A.U.  **A.V.** 

Geodesic Problems.

The **Geodesic Problem (GP):** Given a word $w \in F(X)$ find a word $u \in F(X)$ which is geodesic in G such that $w =_G u$.

The **Geodesic Length Problem (GLP):** Given a word $w \in F(X)$ find $|w|_G$.

Bounded Geodesic Length Problem.

As customary in complexity theory one can modify the search problem **GLP** to get the corresponding bounded *decision* problem (that requires only answers "yes" or "no"):

The **Bounded Geodesic Length Problem (BGLP):** Given a word $w \in F(X)$ and $k \in \mathbb{N}$ determine if $|w|_G \leq k$.

Though **GLP** seems easier than **GP** , in practice, to solve **GLP** one usually solves **GP** first, and only then computes the geodesic length. M. Elder proved that these problems are equivalent.

Turing reducibility of the Geodesic Problems

The algorithmic "hardness" of the problems **WP, BGLP, GLP**, and **GP** in a given group G each one is Turing reducible in polynomial time to the next one in the list:

$$WP \preceq_{T,p} BGLP \preceq_{T,p} GLP \preceq_{T,p} GP,$$

and **GP** is Turing reducible to **WP** in exponential time:

$$GP \preceq_{T,exp} WP$$

Complexity of the Geodesic Problems

.

If G has polynomial *growth*, i.e., there is a polynomial $p(n)$ such that for each n cardinality of the ball B_n of radius n in the Cayley graph $\Gamma(G, X)$ is at most $p(n)$, then one can easily construct this ball B_n in polynomial time with an oracle for the **WP** in G. It follows that if a group with polynomial growth has **WP** decidable in polynomial time then all the problems above have polynomial time complexity. Observe now, that by Gromov's theorem [1981] f.g. groups of polynomial growth are virtually nilpotent. It is also known that the latter have **WP** decidable in polynomial time (nilpotent f.g. groups are linear). These two facts together imply that the **GP** is polynomial time decidable in f.g. virtually nilpotent groups.

Complexity of the Geodesic Problems

On the other hand, there are many groups of exponential growth where **GP** is decidable in polynomial time:

- hyperbolic groups - Epstein and al.
- the Baumslag-Solitar group (metabelian, non polycyclic of exponential growth)

$$BS(1,2) = \langle a, t \mid t^{-1}at = a^2 \rangle$$

- Elder [2010].

Complexity of the Geodesic Problems

In general, if **WP** in G is polynomially decidable then **BGLP** is in the class NP, i.e., it is decidable in polynomial time by a non-deterministic Turing machine. In this case **GLP** is Turing reducible in polynomial time to an NP problem, but we cannot claim the same for **GP**. Observe, that **BGLP** is in NP for any f.g. metabelian group, since they have **WP** decidable in polynomial time.

It might happen though, that **WP** in a group G is polynomial time decidable, but **BGLP** in G is NP-complete.

Parry [1992] showed that **BGLP** is NP-complete in the metabelian group

$$\mathbb{Z}_2 wr(\mathbb{Z} \times \mathbb{Z})$$

the wreath product of $\mathbb{Z}_2$ and $\mathbb{Z} \times \mathbb{Z}$.

Complexity of the Geodesic Problems

It was claimed Droms, Lewin and Servatius [1993] that in $S_{r,d}$ **GLP** is decidable in polynomial time. Unfortunately, in this particular case their argument is fallacious.

Theorem

(Myasnikov, Roman'kov, Ushakov, Vershik [2010]).
Let M_r be a free metabelian group of finite rank $r \geq 2$.
Then **BGLP** *(relative to the standard basis in M_r) is NP-complete.*

Corollary

The search problems **GP** *and* **GLP** *are NP-hard in non-abelian M_r.*

To see the NP-completeness we construct a polynomial reduction of the Rectilinear Steiner Tree Problem to **BGLP** in M_r.

Free solvable groups of finite ranks: CP.

The CP in S_r, d reduces via the Magnus embedding to the CP in $A_r wr S_{r,d-1}$ in time $O(n^3 rd)$
The Power Problem (PP) in a group G:

$$\exists ? n \in \mathbb{Z} : g^n = f.$$

Theorem

(Vassileva [2011]).

- *The Power Problem (PP) in $S_{r,d}$ is decidable in time $O(n^6 rd)$.*
- *The* **CP** *has time complexity $O(n^8 rd)$ in $S_{r,d}$.*

APPROACHES: OLD AND NEW

APPROACHES: OLD AND NEW

APPROACHES: OLD AND NEW

- Philip Hall established a great connection between the theory of solvable groups and commutative algebra. A lot of results on f.g. nilpotent and polycyclic groups have been obtained with efficient use of this tool.
- Anatolii Ivanovich Mal'cev invented efficient connection between residual properties and decidability. This is one of the most important tools in the theory of groups.

APPROACHES: OLD AND NEW

- William Magnus introduced the *Magnus embedding* that allows to apply induction on solvability class of a group. J. Birman, S. Bachmuth, H. Mochizuki, V. Remeslennikov, A. Smelkin, Yu. Kuz'min extended and improved this instrument.

S. Bachmuth  **A. Smelkin** 

APPROACHES: OLD AND NEW

- Ralph Fox introduced and developed the free derivatives, S. Bachmuth and other (H. Mochizuki, N. and C. Gupta's, V. Remeslennikov, N. Romanovskii, E. Timoshenko, V. Shpilrain, U. Umirbaev, V. Roman'kov ...) succeded in using this tool in solvable setting.

R. Fox  **A.M. and** R^3 

APPROACHES: OLD AND NEW

- Olga Kharlampovich demonstrated how results of M. Minsky from recursion theory works in constructing counter examples in the solvable group theory. G. Baumslag, D. Gildenhuys and R. Strebel apllied this tool differently.

APPROACHES: OLD AND NEW

Almost all negative results in the algorithmic theory of nilpotent groups based on the well-known negative solution to Hilbert's Tenth Problem found by Yu. Matijasevich [1970].

- Vitaly Roman'kov established interpretation of Diophantine Problem in the theory of solvable groups to prove undecidability of the **EqP and EndoP**. D. Segal, Yu. Kleyman and N. Repin applied this tool for a number of other algorithmic problems.

NEW TIMES – NEW SONGS

We just mention the following tools:

- Geometrical approach - circulation, flows (A.M. Vershik, A. Myasnikov, V.A. Roman'kov, A. Ushakov),
- Combinatorial tiling (L. Levin, B. Steinberg, M. Lohrey).
- Compression (M. Lohrey, S. Schlimer).

NEW TIMES – NEW DANCES

- Algebraic geometry over groups (B. Plotkin, V. Remeslennikov, A. Myasnikov, G. Baumslag, M. Amaglobeli, N. Romanovskii, E. Timoshenko ...).

M.A., E.T., V.R., and A. Olshanskii

PRACTICALITY

PART III

PRACTICALITY

PRACTICALITY

We assume that practical algorithms work with random dates. In numerous of cases “random” exclude “the worst” case.
The Simplex Method is a very good sample of such algorithm.
Hence, the *generic set* of dates when algorithm works well became a very important notion.

Charles Sims 

COMPUTING IN PERMUTATION GROUPS

Permutation groups is the most developed subdomain in the Computational Group Theory.
Fundamental is a technique first proposed by C. Sims in the 1960's.
Let $G \leq Sym(\Omega)$, where $\Omega = \{\omega_1, ..., \omega_n\}$. The tower

$$G = G^{(1)} \geq ... \geq G^{(n+1)} = 1,$$

where $G^{(i)}$ is a pointwise stabilizer of $\{\omega_1, ..., \omega_{i-1}\}$, underlines almost all practical algorithms.
Furst, Hopcroft and Lucks [1980] have showed that a variant of Sims's method runs in polynomial time.
Now there is the non-substancional polynomial-time library for permutation groups.

POLYNOMIAL-TIME THEORY (PTTh) of matrix groups

Polynomial-time theory of linear groups started with matrix groups over finite fields. Such group is specified by finite list of generators. The two most basic questions are:

- membership in $gr(U)$
- the order of the group $gr(U)$

Even in the case of abelian groups it is not known how to answer these questions without solving hard number theoretic problems (factoring and discrete logarithm). So the reasonable question is whether these problems are decidable in randomized polynomial time using number theory oracles.

PTTh: MATRIX GROUPS OVER FINITE FIELDS

The first algorithms for computing with finite solvable matrix groups were designed by E. Luks [1992].

(Luks, Babai, Beals, Seress et al. - last 25-30 years).Let $G \leq GL(n, \mathbb{F}_q)$ be a f.g. matrix group over a finite field $\mathbb{F}_q$.

- One can test in polynomial time whether G is solvable and, if so, whether G is nilpotent.
- If G is solvable, one can also find, for each prime p, the $p-$part of G. In the nilpotent case it is its (unique) Sylow $p-$subgroup.
- Also, given a solvable $G \leq GL(n, \mathbb{F}_q)$ the following problems can be solved: find $|G|$, decide the MP w.r.t. G, find a presentation of G via generators and defining relators, find a composition series of G, et cetera.

PTTh: POLYCYCLIC GROUPS

pc-presentation approach

Eick, Nickel, Kahrobaei, Ostheimer ... .

Pc-presentation of a polycyclic group exhibits its polycyclic structure.

Pc-presentations allows efficient computations with the groups they define. In particular the WP is efficiently decidable in a group given by a pc-presentation.

GAP 4 package polycyclic designed for computations with polycyclic groups which are given by a pc-presentations.

PTTh: POLYCYCLIC GROUPS

nilpotent-by-abelian-by finite presentation approach

$$G \in \mathcal{NAF}$$

The bi-twisted conjugacy problem:

$$\varphi, \psi \in End(G), g, f \in G$$

$$\exists ? x : \varphi(x) g = f \psi(x)$$

PTTh: MATRIX GROUPS OVER INFINITE FIELDS

Theorem

(Kopytov [1968]). Let $G \leq GL(n, \bar{Q})$ be a f.g. matrix group over an algebraic number field $\bar{Q}$. Then the following problems are decidable:

- *determine finiteness of G*
- *determine solvability of G*
- *MP_{sol} the membership problem w.r.t. solvable G*

PTTh: MATRIX GROUPS OVER INFINITE FIELDS

V. Kopytov (second) with N.R., N. Medvedev and A. Glass

PTTh: POLYCYCLIC MATRIX GROUPS OVER INFINITE FIELDS

Most computational problems are known to be decidable for polycyclic matrix groups over number fields. Algorithmically useful finite presentation can be computed for them (Assman, Eick [2005], Ostheimer [1999]).
The WP and MP can be solved (Assmann, Eick [2005]), and using the f.p., many further structural problems have a practical solution (Holt, Eick, O'Brien [2005]).

PTTh: MATRIX GROUPS OVER INFINITE FIELDS

Some methods are developed for computing with matrix groups defined over a range of infinite domains.

Let G be a f.g. matrix group over an infinite field $\mathbb{F}$.

- (Detinko, Flannery [2007]). A practical nilpotent testing algorithm is provided for matrix groups over $\mathbb{F}$.

The main algorithms have been implemented in GAP, for groups over $\mathbb{Q}$.

PTTh: MATRIX GROUPS OVER INFINITE FIELDS

Let $\mathbb{F} = \bar{\mathbb{Q}}$ be an algebraic number field. By the celebrated Tits's theorem a f.g. subgroup $G \leq GL(n, \bar{\mathbb{Q}})$ either contains a nonabelian free subgroup F or has a solvable subgroup H of finite index (Tits Alternative).

(Beals [2002]).

- There is a polynomial time algorithm for deciding which of two conditions of the Tits's Alternative holds for a given G.
- Let G has a solvable subgroup H of finite index. Then one is able in polynomial time to compute a homomorphism φ such that $\varphi(G)$ is a finite matrix group, and $ker(\varphi)$ is solvable. If in addition, H is nilpotent, then there is effective method to compute an encoding of elements of G.

PART IV

PERSPECTIVE

TO BE PRESENTED LATER

The end

THANK YOU! BYE!

Th