Orbit decidability and the conjugacy problem

E. Ventura

(Universitat Politècnica Catalunya &

Centre de Recerca Matemàtica)

August 30, 2007

PART I: A positive solution to the conjugacy problem for free-by-cyclic groups.

(joint work with O. Bogopolski, A. Martino and O. Maslakova, published in Bull. London Math. Soc. **38**(5) (2006) 787-794)

PART II: Extension of the techniques to a bigger class of groups.

(joint work with O. Bogopolski and A. Martino)

PART I: A positive solution to the conjugacy problem for free-by-cyclic groups.

(joint work with O. Bogopolski, A. Martino and O. Maslakova, published in Bull. London Math. Soc. **38**(5) (2006) 787-794)

PART II: Extension of the techniques to a bigger class of groups.

(joint work with O. Bogopolski and A. Martino)

PART 0: The twisted conjugacy problem.

PART 0: The twisted conjugacy problem.

Let G be a f.p. group and $\phi\colon G \to G$ an automorphism (all given by gen's and rel's.)

Notation. - *morphisms act on the right*, $g \mapsto g\phi$
- *conjugations:* $\gamma_x\colon G \to G$, $g \mapsto x^{-1}gx$.

PART 0: The twisted conjugacy problem.

Let G be a f.p. group and $\phi\colon G \to G$ an automorphism (all given by gen's and rel's.)

Notation. - *morphisms act on the right*, $g \mapsto g\phi$
- *conjugations:* $\gamma_x\colon G \to G$, $g \mapsto x^{-1}gx$.

Definition. *Two elements $u, v \in G$ are said to be ϕ-twisted conjugated, denoted $u \sim_\phi v$, if $v = (g\phi)^{-1}ug$ for some $g \in G$.*

PART 0: The twisted conjugacy problem.

Let G be a f.p. group and $\phi\colon G \to G$ an automorphism (all given by gen's and rel's.)

Notation. - *morphisms act on the right*, $g \mapsto g\phi$
- *conjugations:* $\gamma_x\colon G \to G$, $g \mapsto x^{-1}gx$.

Definition. *Two elements $u, v \in G$ are said to be ϕ-twisted conjugated, denoted $u \sim_\phi v$, if $v = (g\phi)^{-1}ug$ for some $g \in G$.*

Definition. *The ϕ-twisted conjugacy problem for G, $\phi{-}TCP(G)$, and the twisted conjugacy problem for G, $TCP(G)$, are defined in the natural ways.*

PART 0: The twisted conjugacy problem.

Let G be a f.p. group and $\phi\colon G \to G$ an automorphism (all given by gen's and rel's.)

Notation. - *morphisms act on the right*, $g \mapsto g\phi$
- *conjugations:* $\gamma_x\colon G \to G$, $g \mapsto x^{-1}gx$.

Definition. *Two elements $u, v \in G$ are said to be ϕ-twisted conjugated, denoted $u \sim_\phi v$, if $v = (g\phi)^{-1}ug$ for some $g \in G$.*

Definition. *The ϕ-twisted conjugacy problem for G, ϕ–$TCP(G)$, and the twisted conjugacy problem for G, $TCP(G)$, are defined in the natural ways.*

$TCP(G)$ solvable $\Longrightarrow$ $CP(G)$ solvable $\overset{\Longrightarrow}{\not\Longleftarrow}$ $WP(G)$ solvable

Proposition. *Let $H \leq G$ be a characteristic, finite index subgroup of G. If $TCP(H)$ is solvable then $TCP(G)$ is solvable.*

Proposition. *Let $H \leq G$ be a characteristic, finite index subgroup of G. If $TCP(H)$ is solvable then $TCP(G)$ is solvable.*

Proof. Let $\phi \colon G \to G$ and $u, v \in G$ be given. Then,

• Compute $x_1, \ldots, x_r \in G$ such that $G = x_1 H \sqcup \cdots \sqcup x_r H$, and consider the restriction $\phi_H \colon H \to H$ (all in terms of gen's).

Proposition. *Let $H \leq G$ be a characteristic, finite index subgroup of G. If $TCP(H)$ is solvable then $TCP(G)$ is solvable.*

Proof. Let $\phi \colon G \to G$ and $u, v \in G$ be given. Then,

• Compute $x_1, \ldots, x_r \in G$ such that $G = x_1 H \sqcup \cdots \sqcup x_r H$, and consider the restriction $\phi_H \colon H \to H$ (all in terms of gen's).

• Write $u = x_i h_u$ and $v = x_j h_v$ (with $h_u, h_v \in H$).

Proposition. *Let $H \leq G$ be a characteristic, finite index subgroup of G. If $TCP(H)$ is solvable then $TCP(G)$ is solvable.*

Proof. Let $\phi\colon G \to G$ and $u, v \in G$ be given. Then,

• Compute $x_1, \ldots, x_r \in G$ such that $G = x_1 H \sqcup \cdots \sqcup x_r H$, and consider the restriction $\phi_H\colon H \to H$ (all in terms of gen's).

• Write $u = x_i h_u$ and $v = x_j h_v$ (with $h_u, h_v \in H$).

• ϕ-conjugate u by each x_k, and check whether it belongs to same coset as v, say $(x_k\phi)^{-1} u x_k \in x_j H = H x_j H$.

Proposition. *Let $H \leq G$ be a characteristic, finite index subgroup of G. If $TCP(H)$ is solvable then $TCP(G)$ is solvable.*

Proof. Let $\phi\colon G \to G$ and $u, v \in G$ be given. Then,

• Compute $x_1, \ldots, x_r \in G$ such that $G = x_1 H \sqcup \cdots \sqcup x_r H$, and consider the restriction $\phi_H\colon H \to H$ (all in terms of gen's).

• Write $u = x_i h_u$ and $v = x_j h_v$ (with $h_u, h_v \in H$).

• ϕ-conjugate u by each x_k, and check whether it belongs to same coset as v, say $(x_k \phi)^{-1} u x_k \in x_j H = H x_j H$.

• If there is no such k, then $u \not\sim_\phi v$.

- For each such k, want to know whether $\exists\ h \in H$ such that

$$(h\phi)^{-1}(x_k\phi)^{-1}ux_kh = v \in x_jH,$$

- For each such k, want to know whether $\exists\ h \in H$ such that

$$(h\phi)^{-1}(x_k\phi)^{-1}ux_kh = v \in x_jH,$$

$$x_j^{-1}(h\phi)^{-1}x_j\left[x_j^{-1}(x_k\phi)^{-1}ux_k\right]h = x_j^{-1}v \in H,$$

- For each such k, want to know whether $\exists\ h \in H$ such that

$$(h\phi)^{-1}(x_k\phi)^{-1}ux_kh = v \in x_jH,$$

$$x_j^{-1}(h\phi)^{-1}x_j\left[x_j^{-1}(x_k\phi)^{-1}ux_k\right]h = x_j^{-1}v \in H,$$

$$(h\phi_H\gamma_{x_j})^{-1}\left[x_j^{-1}(x_k\phi)^{-1}ux_k)\right]h = x_j^{-1}v \in H.$$

• For each such k, want to know whether $\exists\ h \in H$ such that

$$(h\phi)^{-1}(x_k\phi)^{-1}ux_kh = v \in x_jH,$$

$$x_j^{-1}(h\phi)^{-1}x_j\left[x_j^{-1}(x_k\phi)^{-1}ux_k\right]h = x_j^{-1}v \in H,$$

$$(h\phi_H\gamma_{x_j})^{-1}\left[x_j^{-1}(x_k\phi)^{-1}ux_k)\right]h = x_j^{-1}v \in H.$$

•This is decidable by using the $\phi_H\gamma_{x_j} - TCP(H)$ applied to elements $x_j^{-1}(x_k\phi)^{-1}ux_k)$, $x_j^{-1}v \in H$. $\square$

• For each such k, want to know whether $\exists\ h \in H$ such that

$$(h\phi)^{-1}(x_k\phi)^{-1}ux_kh = v \in x_jH,$$

$$x_j^{-1}(h\phi)^{-1}x_j\left[x_j^{-1}(x_k\phi)^{-1}ux_k\right]h = x_j^{-1}v \in H,$$

$$(h\phi_H\gamma_{x_j})^{-1}\left[x_j^{-1}(x_k\phi)^{-1}ux_k)\right]h = x_j^{-1}v \in H.$$

•This is decidable by using the $\phi_H\gamma_{x_j} - TCP(H)$ applied to elements $x_j^{-1}(x_k\phi)^{-1}ux_k)$, $x_j^{-1}v \in H$. □

However, Collins-Miller (1977) gave an example $H \leq_2 G$ (so, H characteristic in G) with $CP(H)$ solvable and $CP(G)$ unsolvable.

• For each such k, want to know whether $\exists\ h \in H$ such that

$$(h\phi)^{-1}(x_k\phi)^{-1}ux_kh = v \in x_jH,$$

$$x_j^{-1}(h\phi)^{-1}x_j\left[x_j^{-1}(x_k\phi)^{-1}ux_k\right]h = x_j^{-1}v \in H,$$

$$(h\phi_H\gamma_{x_j})^{-1}\left[x_j^{-1}(x_k\phi)^{-1}ux_k)\right]h = x_j^{-1}v \in H.$$

•This is decidable by using the $\phi_H\gamma_{x_j} - TCP(H)$ applied to elements $x_j^{-1}(x_k\phi)^{-1}ux_k)$, $x_j^{-1}v \in H$. $\square$

However, Collins-Miller (1977) gave an example $H \leq_2 G$ (so, H characteristic in G) with $CP(H)$ solvable and $CP(G)$ unsolvable.

Corollary. *There exists a f.p. group H with $CP(H)$ solvable but $TCP(H)$ unsolvable.*

Theorem. *Every finitely generated*

(i) abelian

(ii)

(iii)

(iv)

group has solvable twisted conjugacy problem.

Theorem. *Every finitely generated*

(i) abelian

(ii) free

(iii)

(iv)

group has solvable twisted conjugacy problem.

Theorem. *Every finitely generated*

(i) abelian

(ii) free

(iii) surface

(iv)

group has solvable twisted conjugacy problem.

Theorem. *Every finitely generated*

(i) abelian

(ii) free

(iii) surface

(iv) polycyclic

group has solvable twisted conjugacy problem.

Theorem. *Every finitely generated, virtual*

(i) abelian

(ii) free

(iii) surface

(iv) polycyclic

group has solvable twisted conjugacy problem.

PART I: a positive solution to the conjugacy problem for free-by-cyclic groups.

The motivation to study this concept was that allowed us to solve the conjugacy problem for free-by-cyclic groups.

• Let $F_n = \langle x_1, \ldots, x_n \rangle$ be the free group on $\{x_1, \ldots, x_n\}$ ($n \geq 2$).

• Let $M_\phi = \langle x_1, \ldots, x_n, \, t \mid wt = t(w\phi) \rangle$ be the free-by-cyclic group defined by ϕ.

PART I: a positive solution to the conjugacy problem for free-by-cyclic groups.

The motivation to study this concept was that allowed us to solve the conjugacy problem for free-by-cyclic groups.

• Let $F_n = \langle x_1, \ldots, x_n \rangle$ be the free group on $\{x_1, \ldots, x_n\}$ $(n \geq 2)$.

• Let $M_\phi = \langle x_1, \ldots, x_n, t \mid wt = t(w\phi) \rangle$ be the free-by-cyclic group defined by ϕ.

• Collecting t's to the left, we have usual normal forms $t^r w$, with $r \in \mathbb{Z}$, $w \in F_n$.

PART I: A positive solution to the conjugacy problem for free-by-cyclic groups.

The motivation to study this concept was that allowed us to solve the conjugacy problem for free-by-cyclic groups.

- Let $F_n = \langle x_1, \ldots, x_n \rangle$ be the free group on $\{x_1, \ldots, x_n\}$ $(n \geq 2)$.

- Let $M_\phi = \langle x_1, \ldots, x_n, t \mid wt = t(w\phi) \rangle$ be the free-by-cyclic group defined by ϕ.

- Collecting t's to the left, we have usual normal forms $t^r w$, with $r \in \mathbb{Z}$, $w \in F_n$.

Proposition. *(Bogopolski, Martino, Maslakova, V.)*
If $TCP(F_n)$ solvable, then $CP(M_\phi)$ solvable.

Proposition. *(Bogopolski, Martino, Maslakova, V.)*
If $TCP(F_n)$ solvable, then $CP(M_\phi)$ solvable.

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in M_ϕ.

- $(g^{-1}t^{-k})(t^r u)(t^k g) = t^r (g\phi^r)^{-1} t^{-k} u t^k g = t^r (g\phi^r)^{-1} (u\phi^k) g.$

Proposition. *(Bogopolski, Martino, Maslakova, V.)*
If $TCP(F_n)$ solvable, then $CP(M_\phi)$ solvable.

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in M_ϕ.

- $(g^{-1}t^{-k})(t^r u)(t^k g) = t^r (g\phi^r)^{-1} t^{-k} u t^k g = t^r (g\phi^r)^{-1}(u\phi^k)g.$

- $t^r u$ and $t^s v$ conj. in M_ϕ $\iff$ $r = s$, $v \sim_{\phi^r} (u\phi^k)$ for some $k \in \mathbb{Z}$.

Proposition. *(Bogopolski, Martino, Maslakova, V.)*
If $TCP(F_n)$ solvable, then $CP(M_\phi)$ solvable.

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in M_ϕ.

- $(g^{-1}t^{-k})(t^r u)(t^k g) = t^r (g\phi^r)^{-1} t^{-k} u t^k g = t^r (g\phi^r)^{-1}(u\phi^k) g.$

- $t^r u$ and $t^s v$ conj. in M_ϕ $\iff$ $r = s$, $v \sim_{\phi^r} (u\phi^k)$ for some $k \in \mathbb{Z}$.

- To reduce to finitely many k's, note that $u \sim_\phi u\phi$ (because $u = (u\phi)^{-1}(u\phi)u$) and so,

  $t^r u$ and $t^s v$ conj. in M_ϕ $\iff$ $r = s$, $v \sim_{\phi^r} (u\phi^k)$ for some $k = 0, \ldots, r-1$.

- Hence, $CP(M_\phi)$ reduces to finitely many checks of $TCP(F_n)$.

• ... except that this is wrong for $r = 0$, where there still is a parameter with infinitely many values:

$$\begin{array}{c} u \text{ and } v \\ \text{conj. in } M_\phi \end{array} \quad \Longleftrightarrow \quad v \sim u\phi^k \text{ for some } k \in \mathbb{Z}.$$

• ... except that this is wrong for $r = 0$, where there still is a parameter with infinitely many values:

$$\begin{matrix} u \text{ and } v \\ \text{conj. in } M_\phi \end{matrix} \quad \Longleftrightarrow \quad v \sim u\phi^k \text{ for some } k \in \mathbb{Z}.$$

• This is precisely Brinkmann's result:

Theorem. *Given $\phi\colon F_n \to F_n$ and $u, v \in F_n$, it is decidable whether $v \sim u\phi^k$ for some $k \in \mathbb{Z}$.*

proved using train tracks, and providing a complicated algorithm. This completes the proof.□

Theorem. *(Bogopolski, Martino, Maslakova, V.)*
$TCP(F_n)$ *is solvable.*

Theorem. *(Bogopolski, Martino, Maslakova, V.)*
$TCP(F_n)$ is solvable.

Proof. Let $\phi \colon F_n \to F_n$, and $u, v \in F_n$ be given.

Theorem. *(Bogopolski, Martino, Maslakova, V.)*
$TCP(F_n)$ *is solvable.*

Proof. Let $\phi\colon F_n \to F_n$, and $u, v \in F_n$ be given.

- Extend ϕ to ϕ' as follows: $\begin{array}{rccc} \phi'\colon & F_n * \langle z\rangle & \longrightarrow & F_n * \langle z\rangle \\ & z & \mapsto & uzu^{-1} \end{array}$.

Theorem. *(Bogopolski, Martino, Maslakova, V.)*
$TCP(F_n)$ is solvable.

Proof. Let $\phi\colon F_n \to F_n$, and $u, v \in F_n$ be given.

• Extend ϕ to ϕ' as follows: $\begin{array}{rcl} \phi'\colon F_n * \langle z \rangle & \longrightarrow & F_n * \langle z \rangle \\ z & \mapsto & uzu^{-1} \end{array}$.

• **Claim:** $u \sim_\phi v \Leftrightarrow Fix(\phi'\gamma_v)$ contains an element of the form $g^{-1}zg$ with $g \in F_n$. In this case, g is a valid twisted conjugator.

Theorem. *(Bogopolski, Martino, Maslakova, V.)*
$TCP(F_n)$ is solvable.

Proof. Let $\phi\colon F_n \to F_n$, and $u, v \in F_n$ be given.

- Extend ϕ to ϕ' as follows: $\begin{array}{rcl} \phi'\colon F_n * \langle z \rangle & \longrightarrow & F_n * \langle z \rangle \\ z & \mapsto & uzu^{-1} \end{array}$.

- **Claim:** $u \sim_\phi v \Leftrightarrow Fix(\phi'\gamma_v)$ contains an element of the form $g^{-1}zg$ with $g \in F_n$. In this case, g is a valid twisted conjugator.

In fact, if $v = (g\phi)^{-1}ug$ for some $g \in F_n$, then

$$\begin{array}{rcl} (g^{-1}zg)\phi'\gamma_v & = & v^{-1}(g\phi)^{-1}uzu^{-1}(g\phi)v \\ & = & g^{-1}u^{-1}(g\phi)(g\phi)^{-1}uzu^{-1}(g\phi)(g\phi)^{-1}ug \\ & = & g^{-1}zg. \end{array}$$

- So the algorithm is as follows:
  - compute $\phi'\gamma_v$,
  - compute generators for $Fix(\phi'\gamma_v)$ (Maslakova, using train tracks again),
  - draw Stallings graph for $Fix(\phi'\gamma_v)$,
  - check whether $\exists$ loop labelled z and connected to basepoint with a path not using z's. $\square$

- So the algorithm is as follows:
  - compute $\phi'\gamma_v$,
  - compute generators for $Fix(\phi'\gamma_v)$ (Maslakova, using train tracks again),
  - draw Stallings graph for $Fix(\phi'\gamma_v)$,
  - check whether $\exists$ loop labelled z and connected to basepoint with a path not using z's. $\square$

Remark. *Checking whether $Fix(\phi'\gamma_v)$ contains an element of the form $g^{-1}zg$ seems much easier (!?) than computing the full $Fix(\phi'\gamma_v)$.*

PART II: Extension of the techniques to a bigger class of groups.

Consider an algorithmic short exact sequence of groups:

$$1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

- everything is given by gen's and rel's,
- can compute β-preimages in G,
- can compute α-preimages of elements in G mapping to 1_H.

For every $g \in G$, consider $\psi_g \colon F \to F$, $x \mapsto g^{-1}xg$.

The action subgroup is $A_G = \{\psi_g \mid g \in G\} \leq Aut(F)$.

Theorem. *Let* $1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$ *be an algorithmic short exact sequence of groups such that*

(i) $TCP(F)$ *is solvable,*

(ii) $CP(H)$ *is solvable, and*

(iii) there is an algorithm which, given an input $1 \neq h \in H$, *computes a finite set of elements* $z_{h,1}, \ldots, z_{h,t_h} \in H$ *such that*

$$C_H(h) = \langle h \rangle z_{h,1} \sqcup \cdots \sqcup \langle h \rangle z_{h,t_h}$$

(in particular, $\langle h \rangle$ *has finite index in* $C_H(h)$*).*

Then,

$$CP(G) \text{ is solvable} \iff A_G \leq Aut(F) \text{ is orbit decidable.}$$

Proof. $CP(G)$ splits into two subproblems:
- given $u, v \in F$ decide whether they are conjugate in G: this is orbit decidability of $A_G \leq Aut(F)$.

Proof. $CP(G)$ splits into two subproblems:
- given $u, v \in F$ decide whether they are conjugate in G: this is orbit decidability of $A_G \leq Aut(F)$.
- given $g, g' \in G \setminus F$ decide whether they are conjugate in G. Let us solve this using (i)-(iii):

Proof. $CP(G)$ splits into two subproblems:

- given $u, v \in F$ decide whether they are conjugate in G: this is orbit decidability of $A_G \leq Aut(F)$.

- given $g, g' \in G \setminus F$ decide whether they are conjugate in G. Let us solve this using (i)-(iii):

• check whether $g\beta, g'\beta$ are conjugate in H; if not, g, g' are not conjugate in G either.

Proof. $CP(G)$ splits into two subproblems:
- given $u, v \in F$ decide whether they are conjugate in G: this is orbit decidability of $A_G \leq Aut(F)$.
- given $g, g' \in G \setminus F$ decide whether they are conjugate in G. Let us solve this using (i)-(iii):

• check whether $g\beta, g'\beta$ are conjugate in H; if not, g, g' are not conjugate in G either.
• Otherwise, compute $u \in G$ such that $(u\beta)^{-1}(g\beta)(u\beta) = g'\beta$.

Proof. $CP(G)$ splits into two subproblems:
- given $u, v \in F$ decide whether they are conjugate in G: this is orbit decidability of $A_G \leq Aut(F)$.
- given $g, g' \in G \setminus F$ decide whether they are conjugate in G. Let us solve this using (i)-(iii):

• check whether $g\beta, g'\beta$ are conjugate in H; if not, g, g' are not conjugate in G either.
• Otherwise, compute $u \in G$ such that $(u\beta)^{-1}(g\beta)(u\beta) = g'\beta$.
• Changing g to g^u, we can assume $g\beta = g'\beta \neq 1_H$. Compute $f \in F$ such that $g' = gf$.

Proof. $CP(G)$ splits into two subproblems:
- given $u, v \in F$ decide whether they are conjugate in G: this is orbit decidability of $A_G \leq Aut(F)$.
- given $g, g' \in G \setminus F$ decide whether they are conjugate in G. Let us solve this using (i)-(iii):

• check whether $g\beta, g'\beta$ are conjugate in H; if not, g, g' are not conjugate in G either.
• Otherwise, compute $u \in G$ such that $(u\beta)^{-1}(g\beta)(u\beta) = g'\beta$.
• Changing g to g^u, we can assume $g\beta = g'\beta \neq 1_H$. Compute $f \in F$ such that $g' = gf$.
• Compute the centralizer of $g\beta \neq 1$ in H, and preimages $y_1, \ldots, y_t$ in G: $C_H(g\beta) = \langle g\beta \rangle (y_1\beta) \sqcup \cdots \sqcup \langle g\beta \rangle (y_t\beta)$.

- Compute $p_i \in F$ such that $y_i^{-1} g y_i = g p_i$ ($g\beta$ and $y_i\beta$ commute in H).

• Compute $p_i \in F$ such that $y_i^{-1} g y_i = g p_i$ ($g\beta$ and $y_i\beta$ commute in H).

• All possible conjugators from g to g' in G commute with $g\beta = g'\beta$ in H, so they are of the form $g^r y_i x$, for some $r \in \mathbb{Z}$, $i = 1, \ldots, t$ and $x \in F$. Now,

$$(x^{-1} y_i^{-1} g^{-r})\, g\, (g^r y_i x) = x^{-1}(y_i^{-1} g y_i)x = x^{-1} g p_i x$$

• Compute $p_i \in F$ such that $y_i^{-1} g y_i = g p_i$ ($g\beta$ and $y_i\beta$ commute in H).

• All possible conjugators from g to g' in G commute with $g\beta = g'\beta$ in H, so they are of the form $g^r y_i x$, for some $r \in \mathbb{Z}$, $i = 1, \ldots, t$ and $x \in F$. Now,

$$(x^{-1} y_i^{-1} g^{-r})\, g\, (g^r y_i x) = x^{-1}(y_i^{-1} g y_i)x = x^{-1} g p_i x$$

and

$$\begin{aligned} x^{-1} g p_i x = gf \iff\ & g^{-1} x^{-1} g p_i x = f \\ & (x\varphi_g)^{-1} p_i x = f \\ & f \sim_{\varphi_g} p_i, \end{aligned}$$

which is finitely many checks of $TCP(F)$. □

This applies, for example, to algorithmic short exact sequences

$$1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

where

- F is virt. abelian, virt. free, virt. surface, virt. polycyclic

  and

- H is hyperbolic + torsion elements having finite centralizers.

The free-by-free case

Take $F = \langle x_1, \ldots, x_n \mid \rangle$, $H = \langle t_1, \ldots, t_m \mid \rangle$, $\varphi_1, \ldots, \varphi_m \in Aut(F_n)$, and consider

$$1 \longrightarrow F \longrightarrow G = \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid x_i t_j = t_j (x_i \varphi_j) \rangle \longrightarrow H \longrightarrow 1$$

The free-by-free case

Take $F = \langle x_1, \ldots, x_n \mid \rangle$, $H = \langle t_1, \ldots, t_m \mid \rangle$, $\varphi_1, \ldots, \varphi_m \in Aut(F_n)$, and consider

$$1 \longrightarrow F \longrightarrow G = \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid x_i t_j = t_j (x_i \varphi_j) \rangle \longrightarrow H \longrightarrow 1$$

$$\boxed{CP(G) \text{ is solvable} \quad \Longleftrightarrow \quad A_G = \langle \varphi_1, \ldots, \varphi_m \rangle \leq Aut(F) \text{ is O.D.}}$$

The free-by-free case

Take $F = \langle x_1, \ldots, x_n \mid \rangle$, $H = \langle t_1, \ldots, t_m \mid \rangle$, $\varphi_1, \ldots, \varphi_m \in Aut(F_n)$, and consider

$$1 \longrightarrow F \longrightarrow G = \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid x_i t_j = t_j(x_i \varphi_j) \rangle \longrightarrow H \longrightarrow 1$$

$CP(G)$ is solvable $\iff$ $A_G = \langle \varphi_1, \ldots, \varphi_m \rangle \leq Aut(F)$ is O.D.

Theorem. *(Brinkmann) Cyclic subgroups of $Aut(F_n)$ are O.D.*

Corollary. *Free-by-cyclic groups have solvable conjugacy problem.*

The free-by-free case

Take $F = \langle x_1, \ldots, x_n \mid \rangle$, $H = \langle t_1, \ldots, t_m \mid \rangle$, $\varphi_1, \ldots, \varphi_m \in Aut(F_n)$, and consider

$$1 \longrightarrow F \longrightarrow G = \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid x_i t_j = t_j (x_i \varphi_j) \rangle \longrightarrow H \longrightarrow 1$$

$$\boxed{CP(G) \text{ is solvable} \quad \Longleftrightarrow \quad A_G = \langle \varphi_1, \ldots, \varphi_m \rangle \leq Aut(F) \text{ is O.D.}}$$

Theorem. *(Brinkmann) Cyclic subgroups of $Aut(F_n)$ are O.D.*

Corollary. *Free-by-cyclic groups have solvable conjugacy problem.*

Theorem. *(Whitehead) The full $Aut(F_n)$ is O.D.*

Corollary. *If $\langle \varphi_1, \ldots, \varphi_m \rangle = Aut(F_n)$ then G has solvable conjugacy problem.*

Proposition. *Every f.g. subgroup of* $Aut(F_2)$ *is O.D.*

Corollary. *Every* F_2*-by-free group* G *has solvable conjugacy problem.*

But...

Proposition. *Every f.g. subgroup of $Aut(F_2)$ is O.D.*

Corollary. *Every F_2-by-free group G has solvable conjugacy problem.*

But...

Theorem. *(Miller) There exists a free-by-free group G with $CP(G)$ unsolvable.*

Corollary. *There exists a 14-generated subgroup $A \leq Aut(F_3)$ which is orbit undecidable.*

The abelian-by-free case

$$1 \longrightarrow F = \mathbb{Z}^n \longrightarrow G \longrightarrow H = F_n \longrightarrow 1$$

Proposition. *Every f.g. subgroup of $Aut(\mathbb{Z}_2) = GL_2(\mathbb{Z})$ is O.D.*

Corollary. *Every $\mathbb{Z}^2$-by-free group G has $CP(G)$ solvable.*

But...

The abelian-by-free case

$$1 \longrightarrow F = \mathbb{Z}^n \longrightarrow G \longrightarrow H = F_n \longrightarrow 1$$

Proposition. *Every f.g. subgroup of $Aut(\mathbb{Z}_2) = GL_2(\mathbb{Z})$ is O.D.*

Corollary. *Every $\mathbb{Z}^2$-by-free group G has $CP(G)$ solvable.*

But...

Theorem. *There exists a subgroup of $GL_4(\mathbb{Z})$ which is orbit undecidable.*

Corollary. *There exists a $\mathbb{Z}^4$-by-free group G with $CP(G)$ unsolvable.*

Theorem. *There exists a subgroup of* $GL_4(\mathbb{Z})$ *which is orbit* *undecidable.*

Theorem. *There exists a subgroup of $GL_4(\mathbb{Z})$ which is orbit undecidable.*

Proof. Consider $F_2 \simeq \langle P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, Q = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \rangle \leq_{24} GL_2(\mathbb{Z})$.

- $Stab(1,0) = \{M \mid (1,0)M = (1,0)\} = \{\begin{pmatrix} 1 & 0 \\ n & \pm 1 \end{pmatrix} \mid n \in \mathbb{Z}\}$.

Theorem. *There exists a subgroup of $GL_4(\mathbb{Z})$ which is orbit undecidable.*

Proof. Consider $F_2 \simeq \langle P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, Q = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \rangle \leq_{24} GL_2(\mathbb{Z})$.

- $Stab(1,0) = \{M \mid (1,0)M = (1,0)\} = \{\begin{pmatrix} 1 & 0 \\ n & \pm 1 \end{pmatrix} \mid n \in \mathbb{Z}\}$.
- $\langle P, Q \rangle \cap Stab(1,0) = \langle \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix} \rangle$.

Theorem. *There exists a subgroup of $GL_4(\mathbb{Z})$ which is orbit undecidable.*

Proof. Consider $F_2 \simeq \langle P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, Q = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \rangle \leq_{24} GL_2(\mathbb{Z})$.

- $Stab(1,0) = \{M \mid (1,0)M = (1,0)\} = \{\begin{pmatrix} 1 & 0 \\ n & \pm 1 \end{pmatrix} \mid n \in \mathbb{Z}\}$.
- $\langle P, Q\rangle \cap Stab(1,0) = \langle \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix} \rangle$.
- Choose a free subgroup $\langle P', Q'\rangle \leq \langle P, Q\rangle$ such that $\langle P, Q\rangle \cap Stab(1,0) = \{I\}$ and consider

$$B = \langle \left(\begin{array}{c|c} P' & 0 \\ \hline 0 & I \end{array}\right), \left(\begin{array}{c|c} Q' & 0 \\ \hline 0 & I \end{array}\right), \left(\begin{array}{c|c} I & 0 \\ \hline 0 & P' \end{array}\right), \left(\begin{array}{c|c} I & 0 \\ \hline 0 & Q' \end{array}\right) \rangle \leq GL_4(\mathbb{Z}).$$

Note that $B \simeq F_2 \times F_2$.

- Write $v = (1, 0, 1, 0)$. By construction, $B \cap Stab(v) = \{I\}$

- Write $v = (1, 0, 1, 0)$. By construction, $B \cap Stab(v) = \{I\}$
- Take $A \leq B$ with unsolvable membership problem.

- Write $v = (1, 0, 1, 0)$. By construction, $B \cap Stab(v) = \{I\}$
- Take $A \leq B$ with unsolvable membership problem.
- **Claim:** $A \leq GL_4(\mathbb{Z})$ is orbit undecidable.

In fact, given $\varphi \in B \leq GL_4(\mathbb{Z})$ let $w = v\varphi$ and

$$\{\phi \in B \mid v\phi = w\} = B \cap (Stab(v) \cdot \varphi) = (B \cap Stab(v)) \cdot \varphi = \{\varphi\}.$$

So, orbit decidability for A would imply membership problem for $A \leq B$. $\square$

Questions:

Question. *Does there exist an orbit undecidable subgroup of $GL_3(\mathbb{Z})$?*

Questions:

Question. *Does there exist an orbit undecidable subgroup of $GL_3(\mathbb{Z})$?*

Question. *Does there exist a $\mathbb{Z}^3$-by-free group G with $CP(G)$ unsolvable ?*

Questions:

Question. *Does there exist an orbit undecidable subgroup of $GL_3(\mathbb{Z})$?*

Question. *Does there exist a $\mathbb{Z}^3$-by-free group G with $CP(G)$ unsolvable ?*

Question. *Find more groups with twisted conjugacy problem*

Questions:

Question. *Does there exist an orbit undecidable subgroup of $GL_3(\mathbb{Z})$?*

Question. *Does there exist a $\mathbb{Z}^3$-by-free group G with $CP(G)$ unsolvable ?*

Question. *Find more groups with twisted conjugacy problem*

Question. *Can the twisted conjugacy problem be useful for cryptography ?*

THANKS