The conjugacy problem for some extensions of groups

E. Ventura

(Universitat Politècnica Catalunya)

June 18th, 2008

Based on

O. Bogopolski, A. Martino, O. Maslakova, E.V. *The conjugacy problem is solvable in free-by-cyclic groups*, **Bull. London Math. Soc. 38** (2006), 787-794.

and

O. Bogopolski, A. Martino, E.V. *Orbit decidability and the conjugacy problem for some extensions of groups*, to appear in **Trans. AMS**.

The conjugacy problem for groups

Let G be a finitely presented (f.p.) group, usually given as

$$G = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle.$$

The conjugacy problem for G (CP(G)) consists on, given words $u = u(x_1, \ldots, x_n)$ and $v = v(x_1, \ldots, x_n)$ decide whether they are conjugate in G, denoted $u \sim v$, i.e. whether

$$g^{-1}ug =_G v,$$

for some $g = g(x_1, \ldots, x_n)$.

The conjugacy problem for groups

Let G be a finitely presented (f.p.) group, usually given as

$$G = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle.$$

The conjugacy problem for G (CP(G)) consists on, given words $u = u(x_1, \ldots, x_n)$ and $v = v(x_1, \ldots, x_n)$ decide whether they are conjugate in G, denoted $u \sim v$, i.e. whether

$$g^{-1}ug =_G v,$$

for some $g = g(x_1, \ldots, x_n)$.

There are f.p. groups (Miller's groups, for example) where this problem is algorithmically unsolvable.

Free-by-cyclic groups

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

- Let $\phi \colon F_n \to F_n$ be an automorphism ($w \mapsto w\phi$).

- The corresponding free-by-cyclic group is defined by

$$\begin{aligned} F_n \rtimes_\phi \mathbb{Z} &= \langle x_1, \ldots, x_n, \, t \mid t^{-1}wt = w\phi \rangle \\ &= \langle x_1, \ldots, x_n, \, t \mid wt = t(w\phi) \rangle. \end{aligned}$$

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

.

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi \colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned} b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= \\ &= \\ &= \\ &= \\ &= \\ &= \\ &= \\ &= \\ &= \end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi\colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned} b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\ &= \\ &= \\ &= \\ &= \\ &= \\ &= \\ &= \\ &= \end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi\colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= \\
&= \\
&= \\
&= \\
&= \\
&= \\
&=
\end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi\colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^{2}b^{-1} \\
&= \\
&= \\
&= \\
&= \\
&= \\
&=
\end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \; \rangle$ and $\phi \colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$
\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^2b^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b \\
&= \\
&= \\
&= \\
&= \\
&=
\end{aligned}
$$

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

Example. Consider $F_3 = \langle a, b, c \mid \ \rangle$ and $\phi \colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^{2}b^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b \\
&= b^{-1}ct^{-1}tbaa^{-1}b^{-1}c^{-1}b \\
&= \\
&= \\
&= \\
&=
\end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi \colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^2b^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b \\
&= b^{-1}ct^{-1}tbaa^{-1}b^{-1}c^{-1}b \\
&= b^{-1}cbb^{-1}c^{-1}b \\
&= \\
&= \\
&=
\end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi\colon F_3 \to F_3$ given by $a \mapsto a,\ b \mapsto ba,\ c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^{2}b^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b \\
&= b^{-1}ct^{-1}tbaa^{-1}b^{-1}c^{-1}b \\
&= b^{-1}cbb^{-1}c^{-1}b \\
&= b^{-1}cc^{-1}b \\
&= \\
&=
\end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \, \rangle$ and $\phi \colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^2b^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b \\
&= b^{-1}ct^{-1}tbaa^{-1}b^{-1}c^{-1}b \\
&= b^{-1}cbb^{-1}c^{-1}b \\
&= b^{-1}cc^{-1}b \\
&= b^{-1}b \\
&=
\end{aligned}$$

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

Example. Consider $F_3 = \langle a, b, c \mid \rangle$ and $\phi\colon F_3 \to F_3$ given by $a \mapsto a$, $b \mapsto ba$, $c \mapsto b^{-2}cba$. In $F_3 \rtimes_\phi \mathbb{Z}$ we have

$$
\begin{aligned}
b^{-1}cbt^{-1}ac^{-1}tb^{-1} &= b^{-1}ct^{-1}ba^{-1}ac^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bc^{-1}tb^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b^2b^{-1} \\
&= b^{-1}ct^{-1}bta^{-1}b^{-1}c^{-1}b \\
&= b^{-1}ct^{-1}tbaa^{-1}b^{-1}c^{-1}b \\
&= b^{-1}cbb^{-1}c^{-1}b \\
&= b^{-1}cc^{-1}b \\
&= b^{-1}b \\
&= 1.
\end{aligned}
$$

Observation. *If* $TCP(F_n)$ *solvable, then* $CP(F_n \rtimes_\phi \mathbb{Z})$ *solvable.*

Observation. *If $TCP(F_n)$ solvable, then $CP(F_n \rtimes_\phi \mathbb{Z})$ solvable.*

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in $F_n \rtimes_\phi \mathbb{Z}$.

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

Observation. *If $TCP(F_n)$ solvable, then $CP(F_n \rtimes_\phi \mathbb{Z})$ solvable.*

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in $F_n \rtimes_\phi \mathbb{Z}$.

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

Observation. *If $TCP(F_n)$ solvable, then $CP(F_n \rtimes_\phi \mathbb{Z})$ solvable.*

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in $F_n \rtimes_\phi \mathbb{Z}$.

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

- $$\boxed{t^r u \sim t^s v \quad \Longleftrightarrow \quad \begin{array}{l} r = s \\ v \sim_{\phi^r} (u\phi^k) \text{ for some } k \in \mathbb{Z}. \end{array}}$$

Observation. *If $TCP(F_n)$ solvable, then $CP(F_n \rtimes_\phi \mathbb{Z})$ solvable.*

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in $F_n \rtimes_\phi \mathbb{Z}$.

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

- $$\boxed{t^r u \sim t^s v \quad \Longleftrightarrow \quad \begin{array}{l} r = s \\ v \sim_{\phi^r} (u\phi^k) \text{ for some } k \in \mathbb{Z}. \end{array}}$$

where ϕ-twisted conjugacy, denoted $\sim_\phi$, in a group G is

$$v \sim_\phi u \quad \Longleftrightarrow \quad v = (g\phi)^{-1} ug, \text{ for some } g \in G.$$

Observation. *If $TCP(F_n)$ solvable, then $CP(F_n \rtimes_\phi \mathbb{Z})$ solvable.*

Proof. Let $t^r u$, $t^s v$, $t^k g$ be arbitrary elements in $F_n \rtimes_\phi \mathbb{Z}$.

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

- $$\boxed{t^r u \sim t^s v \quad \Longleftrightarrow \quad \begin{array}{l} r = s \\ v \sim_{\phi^r} (u\phi^k) \text{ for some } k \in \mathbb{Z}. \end{array}}$$

where ϕ-twisted conjugacy, denoted $\sim_\phi$, in a group G is

$$v \sim_\phi u \quad \Longleftrightarrow \quad v = (g\phi)^{-1}ug, \text{ for some } g \in G.$$

Note that: TCP(G) solvable $\underset{\not\Longleftarrow}{\Longrightarrow}$ CP(G) solvable.

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

$$t^r u \sim t^s v \quad \Longleftrightarrow \quad \begin{cases} r = s \\ v \sim_{\phi^r} (u\phi^k) \text{ for some } k = 0, \ldots, r-1. \end{cases}$$

• Hence, $CP(F_n \rtimes_\phi \mathbb{Z})$ reduces to finitely many checks of $TCP(F_n)$.
$\square$

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

$$t^r u \sim t^s v \quad \Longleftrightarrow \quad \begin{cases} r = s \\ v \sim_{\phi^r} (u\phi^k) \text{ for some } k = 0, \ldots, r-1. \end{cases}$$

• Hence, $CP(F_n \rtimes_\phi \mathbb{Z})$ reduces to finitely many checks of $TCP(F_n)$.
$\square$

Theorem. *(Bogopolski, Martino, Maslakova, V., 2006)*
a) TCP(F_n) is solvable,
b) CP($F_n \rtimes_\phi \mathbb{Z}$) is solvable.

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

$$u \sim v \quad \Longleftrightarrow \quad v \sim u\phi^k \text{ for some } k \in \mathbb{Z}.$$

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

$$u \sim v \quad \iff \quad v \sim u\phi^k \text{ for some } k \in \mathbb{Z}.$$

• 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 argument and algorithm.

The central comment.

<u>Armando:</u> *"the same will aprox. work for several stable letters"*

Given $\phi_1, \ldots, \phi_m \in Aut(F_n)$, the free-by-free group is

$$\begin{aligned} F_n \rtimes_{\phi_1,\ldots,\phi_m} F_m &= \langle x_1, \ldots, x_n, \, t_1, \ldots, t_m \mid t_i^{-1} w t_i = w\phi_i \rangle \\ &= \langle x_1, \ldots, x_n, \, t_1, \ldots, t_m \mid w t_i = t_i (w\phi_i) \rangle. \end{aligned}$$

The central comment.

Armando: *"the same will aprox. work for several stable letters"*

Given $\phi_1, \ldots, \phi_m \in Aut(F_n)$, the free-by-free group is

$$\begin{aligned} F_n \rtimes_{\phi_1,\ldots,\phi_m} F_m &= \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid t_i^{-1} w t_i = w\phi_i \rangle \\ &= \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid w t_i = t_i (w\phi_i) \rangle. \end{aligned}$$

Enric: *"no!!! Miller's examples have unsolvable CP"*

Theorem. *(Miller, 1971) There are $\phi_1, \ldots, \phi_{14} \in Aut(F_3)$ such that CP($F_3 \rtimes_{\phi_1,\ldots,\phi_{14}} F_{14}$) is unsolvable.*

The central comment.

Armando: *"the same will aprox. work for several stable letters"*

Given $\phi_1, \ldots, \phi_m \in Aut(F_n)$, the free-by-free group is

$$\begin{aligned} F_n \rtimes_{\phi_1,\ldots,\phi_m} F_m &= \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid t_i^{-1} w t_i = w\phi_i \rangle \\ &= \langle x_1, \ldots, x_n, t_1, \ldots, t_m \mid w t_i = t_i (w\phi_i) \rangle. \end{aligned}$$

Enric: *"no!!! Miller's examples have unsolvable CP"*

Theorem. *(Miller, 1971) There are $\phi_1, \ldots, \phi_{14} \in Aut(F_3)$ such that CP($F_3 \rtimes_{\phi_1,\ldots,\phi_{14}} F_{14}$) is unsolvable.*

Armando: *" Ummm... Yes...ish"*

The central comment.

Armando: *"the same will aprox. work for several stable letters"*

Given $\phi_1, \ldots, \phi_m \in Aut(F_n)$, the free-by-free group is

$$F_n \rtimes_{\phi_1,\ldots,\phi_m} F_m \; = \langle x_1, \ldots, x_n, \, t_1, \ldots, t_m \mid t_i^{-1} w t_i = w\phi_i \rangle \\ = \langle x_1, \ldots, x_n, \, t_1, \ldots, t_m \mid w t_i = t_i (w\phi_i) \rangle.$$

Enric: *"no!!! Miller's examples have unsolvable CP"*

Theorem. *(Miller, 1971) There are $\phi_1, \ldots, \phi_{14} \in Aut(F_3)$ such that CP($F_3 \rtimes_{\phi_1,\ldots,\phi_{14}} F_{14}$) is unsolvable.*

Armando: *" Ummm... Yes...ish"*

He was almost right...

Extensions of groups.

Given a short exact sequence of groups

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

every $g \in G$ defines an action on F,

$$\psi_g \colon F \to F, x \mapsto g^{-1}xg.$$

(Note that $\psi_g \in Aut(F)$ is not in general in $Inn(F)$.)

The action subgroup of the short exact sequence is

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

We have two natural examples:

$$\begin{array}{ccccccccc} 1 \longrightarrow & F_n & \xrightarrow{\alpha} & F_n \rtimes_\phi \mathbb{Z} & \xrightarrow{\beta} & \mathbb{Z} & \longrightarrow 1, \\ & x_i & \mapsto & x_i & \mapsto & 1 & \\ & & & t & \mapsto & t & \end{array}$$

with action subgroup $A = \langle \phi \rangle \cdot Inn(F_n) \leqslant Aut(F_n)$,

and

$$\begin{array}{ccccccccc} 1 \longrightarrow & F_n & \xrightarrow{\alpha} & F_n \rtimes_{\phi_1,\ldots,\phi_m} F_m & \xrightarrow{\beta} & F_m & \longrightarrow 1, \\ & x_i & \mapsto & x_i & \mapsto & 1 & \\ & & & t_j & \mapsto & t_j & \end{array}$$

with action subgroup $A = \langle \phi_1, \ldots, \phi_m \rangle \cdot Inn(F_n) \leqslant Aut(F_n)$.

Orbit decidability.

A subgroup $A \leqslant Aut(F)$ (or equivalently $A \cdot Inn(F) \leqslant Aut(F)$) is orbit decidable when one can algorithmically decide, given $u, v \in F$, whether $v \sim u\psi$ for some $\psi \in A$.

Orbit decidability.

A subgroup $A \leqslant Aut(F)$ (or equivalently $A \cdot Inn(F) \leqslant Aut(F)$) is orbit decidable when one can algorithmically decide, given $u, v \in F$, whether $v \sim u\psi$ for some $\psi \in A$.

For example,

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

i.e. given $\phi\colon F_n \to F_n$ and $u, v \in F_n$, one can decidable whether $v \sim u\phi^k$ for some $k \in \mathbb{Z}$.

Theorem. *Let* $1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$ *be a 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* $C_H(h)$*).*

Theorem. *Let* $1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$ *be a 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), (ii) and (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), (ii) and (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), (ii) and (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), (ii) and (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), (ii) and (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

$$x^{-1} g p_i x = g f \iff \begin{array}{l} g^{-1} x^{-1} g p_i x = f \\ (x\psi_g)^{-1} p_i x = f \\ f \sim_{\psi_g} p_i, \end{array}$$

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

This applies, for example, to 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 torsion-free hyperbolic.

But, let us concentrate on the free-by-free, and free abelian-by-free cases.

The free-by-free case.

Take $F = \langle x_1, \ldots, x_n \mid \; \rangle$, $H = \langle t_1, \ldots, t_m \mid \; \rangle$, $\phi_1, \ldots, \phi_m \in Aut(F_n)$, and consider

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

The free-by-free case.

Take $F = \langle x_1, \ldots, x_n \mid \ \rangle$, $H = \langle t_1, \ldots, t_m \mid \ \rangle$, $\phi_1, \ldots, \phi_m \in Aut(F_n)$, and consider

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

$$\boxed{CP(G) \text{ is solvable} \quad \Longleftrightarrow \quad A_G = \langle \phi_1, \ldots, \phi_m \rangle \leq Aut(F) \text{ is O.D.}}$$

The free-by-free case.

Take $F = \langle x_1, \ldots, x_n \mid \rangle$, $H = \langle t_1, \ldots, t_m \mid \rangle$, $\phi_1, \ldots, \phi_m \in Aut(F_n)$, and consider

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

$$\boxed{CP(G) \text{ is solvable} \quad \Longleftrightarrow \quad A_G = \langle \phi_1, \ldots, \phi_m \rangle \leq Aut(F) \text{ is O.D.}}$$

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

Corollary. *(B.M.M.V.) Free-by-cyclic groups have solvable conjugacy problem.*

The free-by-free case.

Take $F = \langle x_1, \ldots, x_n \mid \ \rangle$, $H = \langle t_1, \ldots, t_m \mid \ \rangle$, $\phi_1, \ldots, \phi_m \in Aut(F_n)$, and consider

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

$$\boxed{CP(G) \text{ is solvable} \quad \Longleftrightarrow \quad A_G = \langle \phi_1, \ldots, \phi_m \rangle \leq Aut(F) \text{ is O.D.}}$$

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

Corollary. *(B.M.M.V.) Free-by-cyclic groups have solvable conjugacy problem.*

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

Corollary. *If $\langle \phi_1, \ldots, \phi_m \rangle = Aut(F_n)$ 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 free 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 free 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 $F_2 \simeq \langle P', Q' \rangle \leq \langle P, Q \rangle$ 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 $A \leq B \simeq F_2 \times F_2$ with unsolvable membership problem.

- Write $v = (1, 0, 1, 0)$. By construction, $B \cap Stab(v) = \{I\}$
- Take $A \leq B \simeq F_2 \times F_2$ 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 solvable TCP.*

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 solvable TCP.*

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

THANKS