## p-quotient algorithm

## Go to Presentations

- Go to $p$-Group Generation


## Conclusion Lecture 1

## Things we have discussed in the first lecture:

- polycyclic groups, sequences, and series
- polycyclic generating sets (pcgs) and relative orders
- polycyclic presentations (pcp), power exponents, and consistency
- normal forms and collection
- consistency checks
- weighted polycyclic presentations (wpcp)


## Conclusion Lecture 1

## weighted polycyclic presentation (wpcp):

- all relative orders $p$
- induced polycyclic series is chief series
- relations are partitioned into definitions and non-definitions


## Example

Consider

$$
\begin{aligned}
G=\operatorname{Pc}\left\langle x_{1}, \ldots, x_{5}\right| & x_{1}^{2}=x_{4}, x_{2}^{2}=x_{3}, x_{3}^{2}=x_{5}, x_{4}^{2}=x_{5}, x_{5}^{2}=1 \\
& {\left.\left[x_{2}, x_{1}\right]=x_{3},\left[x_{3}, x_{1}\right]=x_{5}\right\rangle . }
\end{aligned}
$$

Here $\left\{x_{1}, x_{2}\right\}$ is a minimal generating set, and we choose $\left[x_{2}, x_{1}\right]=x_{3}$ and $x_{1}^{2}=x_{4}$ and $\left[x_{3}, x_{1}\right]=x_{5}$ as definitions for $x_{3}, x_{4}$, and $x_{5}$, respectively.

Lecture 2: how to compute a wpcp?

## Lower exponent- $p$ series

## Lower exponent $p$-series

The lower exponent- $p$ series of a $p$-group $G$ is

$$
G=P_{0}(G)>P_{1}(G)>\ldots>P_{c}(G)=1
$$

where each $P_{i+1}(G)=\left[G, P_{i}(G)\right] P_{i}(G)^{p}$; the $p$-class of $G$ is $c$.

## Important properties

- each $P_{i}(G)$ is characteristic in $G$;
- $P_{1}(G)=[G, G] G^{p}=\Phi(G)$, and $G / P_{1}(G) \cong C_{p}^{d}$ with $d=\operatorname{rank}(G)$;
- each section $P_{i}(G) / P_{i+1}(G)$ is $G$-central and elementary abelian;
- if $G$ has $p$-class $c$, then its nilpotency class is at most $c$;
- if $\theta$ is a homomorphism, then $\theta\left(P_{i}(G)\right)=P_{i}(\theta(G))$;
- $G / N$ has $p$-class $c$ if and only if $P_{c}(G) \leq N$;
- weights: any wpcp on $\left\{a_{1}, \ldots, a_{n}\right\}$ satisfies $a_{i} \in P_{\omega\left(a_{i}\right)}(G) \backslash P_{\omega\left(a_{i}\right)+1}(G)$.


## Lower exponent- $p$ series

## Example 11

Consider

$$
\begin{aligned}
G=D_{16}=\operatorname{Pc}\left\langle a_{1}, a_{2}, a_{3}, a_{4} \quad\right| & a_{1}^{2}=1, a_{2}^{2}=a_{3} a_{4}, a_{3}^{2}=a_{4}, a_{4}^{2}=1 \\
& {\left.\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=a_{4}\right\rangle }
\end{aligned}
$$

Here we can read off:

- $P_{0}(G)=G$
- $P_{1}(G)=[G, G] G^{2}=\left\langle a_{3}, a_{4}\right\rangle$
- $P_{2}(G)=\left[G, P_{1}(G)\right] P_{1}(G)^{2}=\left\langle a_{4}\right\rangle$
- $P_{3}(G)=\left[G, P_{2}(G)\right] P_{2}(G)^{2}=1$

So $G$ has 2-class 3 .

## Computing a wpcp of a p-group

$p$-quotient algorithm ${ }^{3}$
Input: $\quad$ a $p$-group $G=F / R=\left\langle x_{1}, \ldots, x_{n} \mid \mathcal{R}\right\rangle$
Output: a wpcp of $G$

## Top-level outline:

a compute wpcp of $G / P_{1}(G)$ and epimorphism $G \rightarrow G / P_{1}(G)$, then iterate:
${ }^{2}$ given wpcp of $G / P_{k}(G)$ and epimorphism $G \rightarrow G / P_{k}(G)$, compute wpcp of $G / P_{k+1}(G)$ and epimorphism $G \rightarrow G / P_{k+1}(G)$;

For the second step, we use the so-called $p$-cover of $G / P_{k}(G)$.
More general: a "p-quotient algorithm" computes a consistent wpcp of the largest $p$-class $k$ quotient (if it exists) of any finitely presented group.
${ }^{3}$ Historically: MacDonald (1974), Havas \& Newman (1980), Newman \& O'Brien (1996)

## Computing a wpcp of $G / P_{1}(G)$

Note that $G / P_{1}(G)$ is elementary abelian.
Computing wpep of $G / P_{1}(G)$
Input: $\quad$ a $p$-group $G=F / R=\left\langle x_{1}, \ldots, x_{n} \mid \mathcal{R}\right\rangle$
Output: a wpcp of $G / P_{1}(G)$ and epimorphism $\theta: G \rightarrow G / P_{1}(G)$

## Approach:

1 abelianise relations, take exponents modulo $p$, write these in matrix $M$
2 compute solution space of $M$ over $\operatorname{GF}(p)$

## Then:

- dimension $d$ of solution space is rank of $G$, that is, $G / P_{1}(G) \cong C_{p}^{d}$
- generating set of $G / P_{1}(G)$ lifts to subset of given generators; set $G / P_{1}(G)=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{d} \mid a_{1}^{p}=\ldots=a_{d}^{p}\right\rangle$ and define $\theta$ by

$$
\theta\left(x_{i}\right)=a_{i} \quad \text { for } \quad i=1, \ldots, d ;
$$

images of $\theta\left(x_{j}\right)$ with $j>d$ are determined accordingly.

## Computing a wpcp of $G / P_{1}(G)$

## Example 12

$G=\left\langle x_{1}, \ldots, x_{6} \mid x_{6}^{10}, x_{1} x_{2} x_{3}, x_{2} x_{3} x_{4}, \ldots, x_{4} x_{5} x_{6}, x_{5} x_{6} x_{1}, x_{1} x_{6} x_{2}\right\rangle$ and $p=2$
Write coefficients of abelianised and mod-2 reduced equations as rows of matrix, use row-echelonisation, and determine that solution space has dimension 2 :

$$
\left(\begin{array}{llllll}
1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1
\end{array}\right) \rightsquigarrow\left(\begin{array}{llllll}
1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0
\end{array}\right) ;
$$

Modulo $P_{1}(G)$, this shows that $x_{1}=x_{5} x_{6}, x_{2}=x_{5}, x_{3}=x_{6}, x_{4}=x_{5} x_{6}$, and Burnside's Basis Theorem implies that $G=\left\langle x_{5}, x_{6}\right\rangle$. Lastly, set

$$
G / P_{1}(G)=\operatorname{Pc}\left\langle a_{1}, a_{2} \mid a_{1}^{2}=a_{2}^{2}=1\right\rangle,
$$

and define $\theta: G \rightarrow G / P_{1}(G)$ via $x_{5} \mapsto a_{1}$ and $x_{6} \mapsto a_{2}$.
This determines $\theta\left(x_{1}\right)=a_{1} a_{2}, \quad \theta\left(x_{2}\right)=a_{1}, \quad \theta\left(x_{3}\right)=a_{2}$, and $\theta\left(x_{4}\right)=a_{1} a_{2}$.

## Compute wpcp for $G / P_{k+1}(G)$ from that of $G / P_{k}(G)$

## Given:

- wpcp of $d$-generator $p$-group $G / P_{k}(G)$ and epimorphism $\theta: G \rightarrow G / P_{k}(G)$


## Want:

- wpcp of $G / P_{k+1}(G)$ and epimorphism $G \rightarrow G / P_{k+1}(G)$


## In the following:

- $H=G / P_{k}(G)$ and $K=G / P_{k+1}(G)$ and $Z=P_{k}(G) / P_{k+1}(G)$
- note that $Z$ is elementary abelian, $K$-central, and $K / Z \cong H$

Approach: Construct a covering $H^{*}$ of $H$ such that every $d$-generator $p$-group $L$ with $L / M \cong H$ and $M \leq L$ central elementary abelian, is a quotient of $H^{*}$.

Thus, the next steps are:
(1) define $p$-cover $H^{*}$ and determine a pcp of $H^{*}$;

2 make this presentation consistent;
3 construct $K$ as quotient of $H^{*}$ by enforcing defining relations of $G$.

## $p$-covering group: definition

## Theorem 13: p-covering group

Let $H$ be a $d$-generator $p$-group; there is a $d$-generator $p$-group $H^{*}$ with:

- $H^{*} / M \cong H$ for some central elementary abelian $M \unlhd H^{*}$;
- if $L$ is a $d$-generator $p$-group with $L / Y \cong H$ for some central elementary abelian $Y \leq L$, then $L$ is a quotient of $H^{*}$.
The group $H^{*}$ is unique up to isomorphism.


## Proof.

Let $H=F / S$ with $F$ free of rank $d$. Define $H^{*}=F / S^{*}$ with $S^{*}=[S, F] S^{p}$.
Now $S / S^{*}$ is elementary abelian $p$-group, so $H^{*}$ is (finite) $d$-generator $p$-group.
Let $L$ be as in the theorem, and let $\psi: L \rightarrow H$ with kernel $Y$.
Let $\theta: F \rightarrow H$ with kernel $S$. Since $F$ is free, $\theta$ factors through $L$, that is, $\theta: F \xrightarrow{\varphi} L \xrightarrow{\psi} H$, and so $\varphi(S) \leq \operatorname{ker} \psi=Y$. This implies that $\varphi\left(S^{*}\right)=1$. In conclusion, $\varphi$ induces surjective map from $H^{*}=F / S^{*}$ onto $L$.

If $H^{*}$ and $\tilde{H}^{*}$ are two such covers, then each is an image of the other.

## $p$-covering group: presentation

Given: a wpcp $\operatorname{Pc}\left\langle a_{1}, \ldots, a_{m} \mid \mathcal{S}\right\rangle$ for $H=G / P_{k}(G) \cong F / S$ and epimorphism $\theta: G \rightarrow H$ with $\theta\left(x_{i}\right)=a_{i}$ for $i=1, \ldots, d$
Want: a wpcp for $H^{*} \cong F / S^{*}$ where $S^{*}=[S, F] S^{p}$

Recall: each of $a_{d+1}, \ldots, a_{m}$ occurs as right hand side of one relation in $\mathcal{S}$; write $\mathcal{S}=\mathcal{S}_{\text {def }} \cup \mathcal{S}_{\text {nondef }}$ with $\mathcal{S}_{\text {nondef }}=\left\{s_{1}, \ldots, s_{q}\right\}$.

## Theorem 14

Using the previous notation, $H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{m}, b_{1}, \ldots, b_{q} \mid \mathcal{S}^{*}\right\rangle$, where

$$
\mathcal{S}^{*}=\mathcal{S}_{\text {def }} \cup\left\{s_{1} b_{1}, \ldots, s_{q} b_{q}\right\} \cup\left\{b_{1}^{p}, \ldots, b_{q}^{p}\right\} .
$$

Note: $M=\left\langle b_{1}, \ldots, b_{q}\right\rangle \unlhd H^{*}$ is elementary abelian, central, and $H^{*} / M \cong H$.
(see Newman, Nickel, Niemeyer: "Descriptions of groups of prime-power order", 1998)
In practice: fewer new generators are introduced.

## $p$-covering group: example

## Example 15

If $H=\operatorname{Pc}\left\langle a_{1}, a_{2} \mid a_{1}^{2}=a_{2}^{2}=1\right\rangle \cong C_{2} \times C_{2}$, then

$$
H^{*}=\operatorname{Pc}\left\langle a_{1}, a_{2}, b_{1}, b_{2}, b_{3} \mid a_{1}^{2}=b_{1}, a_{2}^{2}=b_{2},\left[a_{1}, a_{2}\right]=b_{3}, b_{1}^{2}=b_{2}^{2}=b_{3}^{2}=1\right\rangle ;
$$

indeed, $H^{*} \cong\left(C_{4} \times C_{2}\right): C_{4}$, thus we have found a consistent wpcp!

## Example 16

If $H=\operatorname{Pc}\left\langle a_{1}, a_{2}, a_{3} \mid a_{1}^{2}=a_{3}^{2}=1, a_{2}^{2}=a_{3},\left[a_{2}, a_{1}\right]=a_{3}\right\rangle \cong D_{8}$, then

$$
\begin{gathered}
H^{*}=\operatorname{Pc}\left\langle a_{1}, a_{2}, a_{3}, b_{1}, \ldots, b_{5} \mid \mathcal{T} \cup\left\{b_{1}^{2}, \ldots, b_{5}^{2}\right\}\right\rangle \text { with } \\
\mathcal{T}=\left\{a_{1}^{2}=b_{1}, a_{2}^{2}=a_{3} b_{2}, a_{3}^{2}=b_{3},\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=b_{4},\left[a_{3}, a_{2}\right]=b_{5}\right\} ;
\end{gathered}
$$

this pcp has power exponents $[2,2,2,2,2,2,2,2]$.
However, $H^{*} \cong\left(C_{8} \times C_{2}\right): C_{4}$, so presentation is not consistent!

Next step: make the presentation of $H^{*}$ consistent.

## $p$-covering group: consistency algorithm

By Theorem 8, the presentation $H^{*}=\operatorname{Pc}\left\langle u_{1}, \ldots, u_{m+q} \mid \mathcal{S}^{*}\right\rangle$ with $\left(u_{1}, \ldots, u_{m+q}\right)=\left(a_{1}, \ldots, a_{m}, b_{1}, \ldots, b_{q}\right)$ is consistent if and only if

$$
\begin{array}{rlrl}
u_{k}\left(u_{j} u_{i}\right) & =\left(u_{k} u_{j}\right) u_{i} & (1 \leq i<j<k \leq m+q) \\
\left(u_{j}^{p}\right) u_{i} & =u_{j}^{p-1}\left(u_{j} u_{i}\right) \text { and } & u_{j}\left(u_{i}^{p}\right)=\left(u_{j} u_{i}\right) u_{i}^{p-1} & (1 \leq i<j \leq m+q) \\
u_{j}\left(u_{j}^{p}\right) & =\left(u_{j}^{p}\right) u_{j} & & (1 \leq j \leq m+q) .
\end{array}
$$

## Consistency Algorithm ${ }^{4}$ : find consistent presentation for $H^{*}$

- If each pair of words in the above "consistency checks" collects to the same normal word, then the presentation is consistent.
- Otherwise, the quotient of the two different words obtained from one of these conditions is formed and equated to the identity word: this gives a new relation which holds in the group.
- The pcp for $H$ is consistent, so any new relation is an equation in the elementary abelian subgroup $M$ generated by the new generators $\left\{b_{1}, \ldots, b_{q}\right\}$, which implies that one of these generators is redundant.

[^0]
## p-covering group: consistency algorithm

By Theorem 8, the presentation $H^{*}=\operatorname{Pc}\left\langle u_{1}, \ldots, u_{m+q} \mid \mathcal{S}^{*}\right\rangle$ with $\left(u_{1}, \ldots, u_{m+q}\right)=\left(a_{1}, \ldots, a_{m}, b_{1}, \ldots, b_{q}\right)$ is consistent if and only if

$$
\begin{array}{rlrl}
u_{k}\left(u_{j} u_{i}\right) & =\left(u_{k} u_{j}\right) u_{i} & (1 \leq i<j<k \leq m+q) \\
\left(u_{j}^{p}\right) u_{i} & =u_{j}^{p-1}\left(u_{j} u_{i}\right) \text { and } u_{j}\left(u_{i}^{p}\right)=\left(u_{j} u_{i}\right) u_{i}^{p-1} & (1 \leq i<j \leq m+q) \\
u_{j}\left(u_{j}^{p}\right) & =\left(u_{j}^{p}\right) u_{j} & & (1 \leq j \leq m+q) .
\end{array}
$$

## Example 17

Consider $G=\operatorname{Pc}\left\langle u_{1}, u_{2}, u_{3} \mid u_{1}^{2}=u_{2}, u_{2}^{2}=u_{3}, u_{3}^{2}=1,\left[u_{2}, u_{1}\right]=u_{3}\right\rangle$. The last test applied to $u_{1}$ yields

$$
u_{1}^{3}=\left(u_{1}^{2}\right) u_{1}=u_{2} u_{1}=u_{1} u_{2} u_{3} \quad \text { and } \quad u_{1}^{3}=u_{1}\left(u_{1}^{2}\right)=u_{1} u_{2}
$$

so $u_{3}=1$ in $G$, hence $G=\operatorname{Pc}\left\langle u_{1}, u_{2} \mid u_{1}^{2}=u_{2}, u_{2}^{2}=1\right\rangle \cong C_{4}$.

## Construct $K$ from cover $H^{*}$ of $H$

## So what have we got so far...

- $p$-group $G=F / R=\left\langle x_{1}, \ldots, x_{n} \mid \mathcal{R}\right\rangle$
- consistent wpcp of $H=G / P_{k}(G)=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{m} \mid \mathcal{S}\right\rangle$
- epimorphism $\theta: G \rightarrow H$ with $\theta\left(x_{i}\right)=a_{i}$ for $i=1, \ldots, d$
- consistent wpcp of cover $H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{m}, b_{1}, \ldots, b_{q} \mid \mathcal{S}^{*}\right\rangle$; note that $H^{*} / M \cong H$ where $M=\left\langle b_{1}, \ldots, b_{q}\right\rangle$


## Want:

- consistent wpcp of $K=G / P_{k+1}(G)$ and epimorphism $G \rightarrow G / P_{k+1}(G)$

Know:

- $K / Z \cong H$ where $Z=P_{k}(G) / P_{k+1}(G)$ is elementary abelian, central
- $K$ is quotient of $H^{*}$


## Idea:

- construct $K$ as quotient of $H^{*}$ : add relations enforced by $G$ to $\mathcal{S}^{*}$


## Construct $K$ from cover $H^{*}$ of $H$

## So what have we got so far...

- p-group $G=F / R=\left\langle x_{1}, \ldots, x_{n} \mid \mathcal{R}\right\rangle$
- consistent wpcp of $H=G / P_{k}(G)=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{m} \mid \mathcal{S}\right\rangle$
- epimorphism $\theta: G \rightarrow H$ with $\theta\left(x_{i}\right)=a_{i}$ for $i=1, \ldots, d$
- consistent pcp of cover $H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{m}, b_{1}, \ldots, b_{q} \mid \mathcal{S}^{*}\right\rangle$; note that $H^{*} / M \cong H$ where $M=\left\langle b_{1}, \ldots, b_{q}\right\rangle$


## Enforcing relations of $G$ :

- know that $K=G / P_{k+1}(G)$ is quotient of $H^{*}$
- lift $\theta: G \rightarrow H$ to $\hat{\theta}: F \rightarrow H^{*}$ such that $\hat{\theta}\left(x_{i}\right)=a_{i}$ for $i=1, \ldots, d$
- for every relator $r \in \mathcal{R}$ compute $n_{r}=\hat{\theta}(r) \in M$; let $L$ be the subgroup of $M$ generated by all these $n_{r}$
- by von Dyck's Theorem $H^{*} / L \rightarrow K$ and $G \rightarrow H^{*} / L$ are surjective; since $K$ is the largest $p$-class $k+1$ quotient of $G$, we deduce $K=H^{*} / L$

Finally: find consistent wpcp of $K=H^{*} / L$ and get epimorphism $G \rightarrow K$

## Big example: $p$-quotient algorithm in action

Let $G=\left\langle x, y \mid[[y, x], x]=x^{2},(x y x)^{4}, x^{4}, y^{4},(y x)^{3} y=x\right\rangle$ and $p=2$.

## First round:

- compute $G / P_{1}(G)$ using abelianisation and row-echelonisation:
obtain $H=G / P_{1}(G) \cong \operatorname{Pc}\left\langle a_{1}, a_{2} \mid a_{1}^{2}=a_{2}^{2}=1\right\rangle$
and epimorphism $\theta: G \rightarrow H$, which is defined by $(x, y) \rightarrow\left(a_{1}, a_{2}\right)$.
- construct covering of $H$ by adding new generators and tails:

$$
H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{5} \mid a_{1}^{2}=a_{3}, a_{2}^{2}=a_{4},\left[a_{2}, a_{1}\right]=a_{5}, a_{3}^{2}=a_{4}^{2}=a_{5}^{2}=1\right\rangle
$$

- the consistency algorithm shows that this presentation is consistent
- evaluate relations of $G$ in $H^{*}$ :

$$
\begin{aligned}
& \text { - } 1=\left[\left[a_{2}, a_{1}\right], a_{1}\right]=\hat{\theta}([[y, x], x])=\hat{\theta}\left(x^{2}\right)=a_{1}^{2}=a_{3} \text { forces } a_{3}=1 \\
& \text { - }(x y x)^{4}, x^{4}, y^{4} \text { impose no conditions } \\
& \text { - } a_{1} a_{3}=\hat{\theta}\left((y x)^{3} y\right)=\hat{\theta}(x)=a_{1} \text { also forces } a_{3}=1
\end{aligned}
$$

- construct $G / P_{2}(G)$ as $H^{*} /\left\langle a_{3}\right\rangle$; after renaming $a_{4}, a_{5}$ :

$$
G / P_{2}(G) \cong \operatorname{Pc}\left\langle a_{1}, \ldots, a_{4} \mid a_{1}^{2}=1, a_{2}^{2}=a_{4},\left[a_{2}, a_{1}\right]=a_{3}, a_{3}^{2}=a_{4}^{2}=1\right\rangle
$$

and epimorphism $G \rightarrow G / P_{2}(G)$ defined by $(x, y) \rightarrow\left(a_{1}, a_{2}\right)$.

## Big example: $p$-quotient algorithm in action

$G / P_{2}(G)=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{4} \mid a_{1}^{2}=1, a_{2}^{2}=a_{4},\left[a_{2}, a_{1}\right]=a_{3}, a_{3}^{2}=a_{4}^{2}=1\right\rangle$

## Second round:

- construct covering of $H=G / P_{2}(G)$ by adding new generators and tails:

$$
\begin{aligned}
H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{12}\right| & a_{1}^{2}=a_{12}, a_{2}^{2}=a_{4}, a_{3}^{2}=a_{11}, a_{4}^{2}=a_{10} \\
& {\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=a_{5},\left[a_{3}, a_{2}\right]=a_{6},\left[a_{4}, a_{1}\right]=a_{7} } \\
& {\left.\left[a_{4}, a_{2}\right]=a_{8},\left[a_{4}, a_{3}\right]=a_{9}, a_{5}^{2}=\ldots=a_{12}^{2}=1\right\rangle }
\end{aligned}
$$

- the consistency algorithm shows only the following inconsistencies:
- $a_{2}\left(a_{2} a_{2}\right)=a_{2} a_{4}$ and $\left(a_{2} a_{2}\right) a_{2}=a_{4} a_{2}=a_{2} a_{4} a_{8} \quad \Longrightarrow a_{8}=1$
- $a_{2}\left(a_{1} a_{1}\right)=a_{2} a_{12}$ and $\left(a_{2} a_{1}\right) a_{1}=a_{1} a_{2} a_{3} a_{1}=\ldots=a_{2} a_{5} a_{11} a_{12} \quad \Longrightarrow a_{5} a_{11}=1$
- $a_{2}\left(a_{2} a_{1}\right)=a_{1} a_{2}^{2} a_{3}^{2} a_{6}=a_{1} a_{4} a_{6} a_{11}$ and $\left(a_{2} a_{2}\right) a_{1}=a_{1} a_{4} a_{7} \quad \Longrightarrow a_{6} a_{7} a_{11}=1$
- $a_{3}\left(a_{2} a_{2}\right)=a_{3} a_{4}$ and $\left(a_{3} a_{2}\right) a_{2}=a_{2} a_{3} a_{6} a_{2}=a_{2}^{2} a_{3} a_{6}^{2}=a_{3} a_{4} a_{9} \quad \Longrightarrow a_{9}=1$
- removing redundant gens (and renaming), we obtain the consistent wpcp

$$
\begin{array}{r}
H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{8}\right| a_{1}^{2}=a_{8}, a_{2}^{2}=a_{4}, a_{3}^{2}=a_{7}, a_{4}^{2}=a_{6}, a_{5}^{2}=\ldots=a_{8}^{2}=1 \\
\left.\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=a_{7},\left[a_{3}, a_{2}\right]=a_{5} a_{7},\left[a_{4}, a_{1}\right]=a_{5}\right\rangle
\end{array}
$$

## Big example: p-quotient algorithm in action

## Still second round:

- $G=\left\langle x, y \mid[[y, x], x]=x^{2},(x y x)^{4}, x^{4}, y^{4},(y x)^{3} y=x\right\rangle$ and $p=2$;
- epimorphism $\theta: G \rightarrow H$ onto $H=G / P_{2}(H)$ defined by $(x, y) \rightarrow\left(a_{1}, a_{2}\right)$
- $H^{*}=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{8}\right| a_{1}^{2}=a_{8}, a_{2}^{2}=a_{4}, a_{3}^{2}=a_{7}, a_{4}^{2}=a_{6}, a_{5}^{2}=\ldots=a_{8}^{2}=1$

$$
\left.\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=a_{7},\left[a_{3}, a_{2}\right]=a_{5} a_{7},\left[a_{4}, a_{1}\right]=a_{5}\right\rangle
$$

Evaluate relations of $G$ in $H^{*}$ :

- $a_{7}=\left[\left[a_{2}, a_{1}\right], a_{1}\right]=\hat{\theta}([[y, x], x])=\hat{\theta}\left(x^{2}\right)=a_{1}^{2}=a_{8}$ forces $a_{7}=a_{8}$
- $(x y x)^{4}$ forces $a_{6}=1 ; x^{4}$ and $y^{4}$ impose no condition
- $\hat{\theta}\left((y x)^{3} y\right)=\hat{\theta}(x)$ forces $a_{7} a_{8}=1$

Now construct $G / P_{3}(G)$ as $H^{*} /\left\langle a_{7} a_{8}, a_{6}\right\rangle$; after renaming:
$G / P_{3}(G)=\operatorname{Pc}\left\langle a_{1}, \ldots, a_{6}\right| a_{1}^{2}=a_{6}, a_{2}^{2}=a_{4}, a_{3}^{2}=a_{6}, a_{4}^{2}=1, a_{5}^{2}=a_{6}^{2}=1$,

$$
\left.\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=a_{6},\left[a_{3}, a_{2}\right]=a_{5} a_{6},\left[a_{4}, a_{1}\right]=a_{5}\right\rangle
$$

and the epimorphism $G \rightarrow G / P_{3}(G)$ is defined by $(x, y) \rightarrow\left(a_{1}, a_{2}\right)$.

## Big example: p-quotient algorithm in action

## In conclusion:

We started with

$$
G=\left\langle x, y \mid[[y, x], x]=x^{2},(x y x)^{4}, x^{4}, y^{4},(y x)^{3} y=x\right\rangle
$$

and computed $G / P_{3}(G)$ as

$$
\begin{aligned}
\operatorname{Pc}\left\langle a_{1}, \ldots, a_{6}\right| & a_{1}^{2}=a_{6}, a_{2}^{2}=a_{4}, a_{3}^{2}=a_{6}, a_{4}^{2}=a_{5}^{2}=a_{6}^{2}=1 \\
& {\left.\left[a_{2}, a_{1}\right]=a_{3},\left[a_{3}, a_{1}\right]=a_{6},\left[a_{3}, a_{2}\right]=a_{5} a_{6},\left[a_{4}, a_{1}\right]=a_{5}\right\rangle }
\end{aligned}
$$

with epimorphism $G \rightarrow G / P_{3}(G)$ defined by $(x, y) \rightarrow\left(a_{1}, a_{2}\right)$.
One can check that $|G|=\left|G / P_{3}(G)\right|=2^{6}$, hence $G \cong G / P_{3}(G)$. In particular, we have found a consistent wpep for $G$.

In general: if our input group is a finite $p$-group, then the $p$-quotient algorithm constructs a consistent wpcp of that group.

## Motivation and Application: Burnside problem

## Burnside Problems

- Generalised Burnside Problem (GBP), 1902: Is every finitely generated torsion group finite?
- Burnside Problem (BP), 1902:

Let $B(d, n)$ be the largest $d$-generator group with $g^{n}=1$ for all $g \in G$. Is this group finite? If so, what is its order?

- Restricted Burnside Problem (RBP), ~1940: What is order of largest finite quotient $R(d, n)$ of $B(d, n)$, if it exists?
- Golod-Šafarevič (1964): answer to GBP is "no"; (cf. Ol'shanskii's Tarski monster)
- Various authors: $B(d, n)$ is finite for $n=2,3,4,6$, but in no other cases with $d>1$ is it known to be finite; is $B(2,5)$ finite?
- Higman-Hall (1956): reduced (RBP) to prime-power $n$.
- Zel'manov (1990-91): $R(d, n)$ always exists! (Fields medal 1994)


## Motivation and Application: Burnside problem

## Burnside groups:

- $B(d, n)=\left\langle x_{1}, \ldots, x_{d}\right| g^{n}=1$ for all words $g$ in $\left.x_{1}, \ldots, x_{n}\right\rangle$
- $R(d, n)$ largest finite quotient of $B(d, n)$; exists by Zel'manov

Recall: the $p$-quotient algorithm computes a consistent wpcp of the largest $p$-class $k$ quotient (if it exists) of any finitely presented group.

Implementations of the $p$-quotient algorithm have been used to determine the order and compute pcp's for various of these groups.

| Group | Order | Authors |
| :---: | :---: | :--- |
| $B(3,4)$ | $2^{69}$ | Bayes, Kautsky \& Wamsley (1974) |
| $R(2,5)$ | $5^{34}$ | Havas, Wall \& Wamsley (1974) |
| $B(4,4)$ | $2^{422}$ | Alford, Havas \& Newman (1975) |
| $R(3,5)$ | $5^{2282}$ | Vaughan-Lee (1988); Newman \& O'Brien (1996) |
| $B(5,4)$ | $2^{2728}$ | Newman \& O'Brien (1996) |
| $R(2,7)$ | $7^{20416}$ | O'Brien \& Vaughan-Lee (2002) |


[^0]:    ${ }^{4}$ Historically: Wamsley (1974), Vaughan-Lee (1984)

