The first part of Whitehead's algorithm made polynomial

(joint work with A. Roig and P. Weil)

E. Ventura

(Universitat Politècnica Catalunya)

Whitehead Problem (WhP): For a given group G, find an algorithm s.t. given $u, v \in G$ decides whether there exists $\varphi \in Aut(G)$ with $u\varphi = v$ (or up to conjugacy).

Observation: In $\mathbb{Z}^r$ (and in any f.g. abelian group) the WhP is solvable.

Theorem (Whitehead): WhP is solvable in F_r.

• First part: Reduce the cyclic length of u, v as much as possible by applying autos:

$$u \to u_1 \to \cdots \to u', \qquad v \to v_1 \to \cdots \to v'.$$

• Second part: Analyze who is image of who by some auto, in the (finite!) sphere of given radius n:

$$S_n = \{w \in F_r \mid \|w\| = n\}.$$

Let us concentrate on the first part.

Wh. Min. Problem (WhMP): Given $u \in F_r$, find $\varphi \in Aut(F_r)$ s.t. $\|u\varphi\|$ is minimal.

Lemma (Whitehead): Let $u \in F_r$. If $\exists \varphi \in Aut(F_r)$ s.t. $\|u\varphi\| < \|u\|$ then $\exists$ a "Whitehead auto" α s.t. $\|u\alpha\| < \|u\|$.

Definition: Whitehead autos are those of the form

$$\begin{array}{rcl} F_r & \longrightarrow & F_r \\ x_i & \mapsto & x_i \text{ (the multiplier)} \\ x_i \neq x_j & \mapsto & x_i^{0,-1} x_j x_i^{0,1}. \end{array}$$

(There are about $2r \cdot 4^{r-1}$ such autos.)

Example:

$$\begin{array}{rcl} \alpha\colon F_3 = \langle a, b, c\rangle & \longrightarrow & F_3 \\ a & \mapsto & ab \\ b & \mapsto & b \\ c & \mapsto & \overline{b}cb. \end{array}$$

Classical Whitehead algorithm for WhMP:

- Keep applying Whitehead autos to the given $u \in F_r$ until finding one that decreases its cyclic length.

- Repeat until all Whitehead autos are non-decreasing.

This is quadratic on the length of input, $n = \|u\|$, but exponential on the ambient rank, r.

There are several theoretical, heuristic, probabilistic recent results (see Haralick, Miasnikov, Myasnikov) suggesting that Whitehead algorithm is faster in practice.

Theorem (Roig, V., Weil): $\exists$ algorithm which solves WhMP for F_r in time $O(n^2 r^3)$.

main idea: given $u \in F_r$, we find in polynomial time one of the Whitehead autos that decreases $\|u\|$ the most possible.

key point: how does a give Whitehead auto α affect the length of a given word u ?

three ingredients:

1) codify u as its Whitehead graph (classic in Group Theory),

2) codify α as a cut in this graph ($\approx$ classic in Group Theory),

3) use max-flow min-cut algorithm (classic in Computer Science),

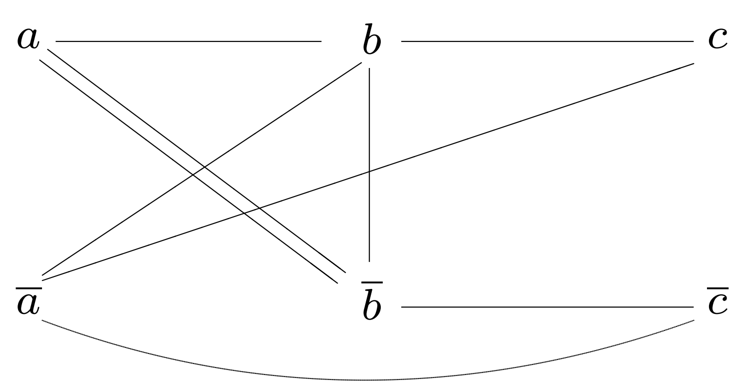
... put together and mix (new!).

First ingredient:
Given $u \in F_r$ (cyclically reduced), its (unoriented) Whitehead graph, $Wh(u)$, is:

- vertices: $X^{\pm 1}$,
- edges: for every pair of (cycl.) consecutive letters $u = \cdots x\, y \cdots$ put an edge between x and $\overline{y}$,

Example: $u = ab\overline{a}\,\overline{c}bbab\overline{c}$,

$Wh(u)=$



(remark: $Wh(u)$ does not remember u.)

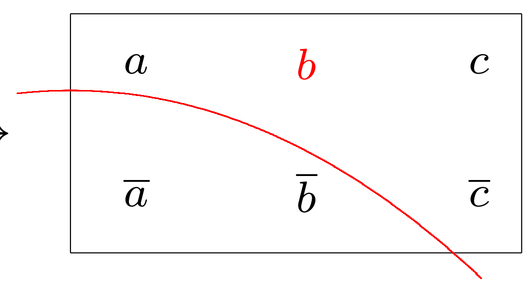
Second ingredient:
Codify a Whitehead auto α as a

- specified letter x_i (the multiplier), and
- the $(x_i, \overline{x}_i) - cut$ (i.e. a subset $Y \subseteq X^{\pm 1}$ with $x_i \in Y$ and $\overline{x}_i \notin Y$) given by

$Y = \{x_i\} \cup \{$letters multiplied on the right by $x_i\}$.

Example: The Wh. auto α is

$$\begin{array}{rcl} \alpha\colon F_3 & \longrightarrow & F_3 \\ a & \mapsto & ab \\ b & \mapsto & b \\ c & \mapsto & \overline{b}cb. \end{array} \quad \longleftrightarrow$$



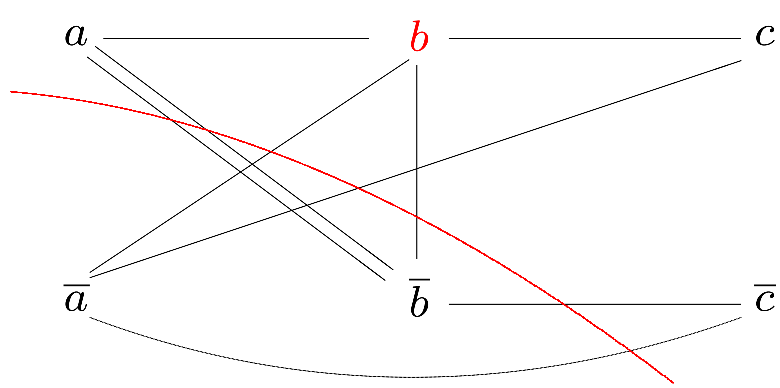
$$\alpha \qquad \longleftrightarrow \quad Y = \{a, b, c, \overline{c}\}.$$

Rephrasement of Wh. Lemma: Given a word $u \in F_r$ and a Wh. auto α, think α as a cut in $Wh(u)$. Then,

$$\|u\alpha\| - \|u\| = \text{cap(cut)} - \text{deg(multiplier)}.$$

Proof: Analyzing cases (see Lyndon-Schupp).

Example: α and u as before,



cap(α) = 7, deg(b) = 4 so, must be

$$\|u\alpha\| - \|u\| = 7 - 4 = 3.$$

In fact,

$$\begin{aligned}(ab\overline{a}\,\overline{c}bbab\overline{c})\alpha &= ab\cdot\ \cancel{b}\cdot\ \overline{\cancel{b}}\overline{a}\cdot\overline{b}\overline{c}b\cdot b\cdot b\cdot ab\cdot\ \cancel{b}\cdot\ \overline{\cancel{b}}\overline{c}b\\ &= ab\overline{a}\overline{b}\overline{c}bbbab\overline{c}b,\end{aligned}$$

$\|u\alpha\| - \|u\| = 12 - 9 = 3.$

Thus, WhMP reduces to:

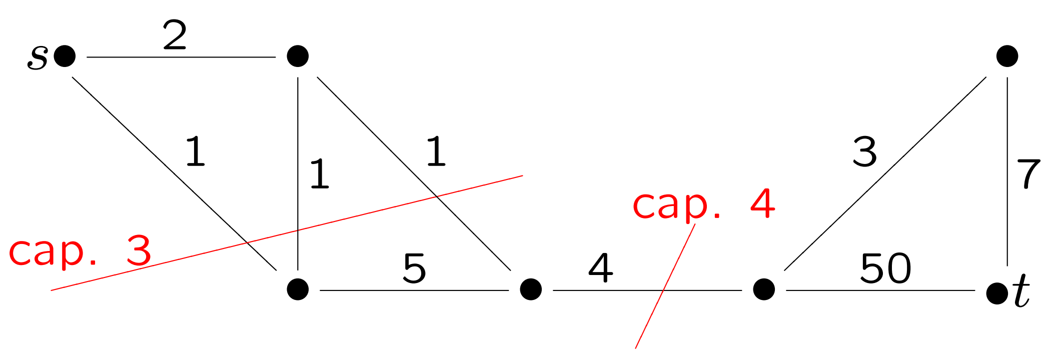
- run over all possible multipliers, say a, (there are $2r$),
- find an $(a, \overline{a}) - cut$ with minimal possible capacity, i.e. a minimal $(a, \overline{a}) - cut$.

This can be done using the classical max-flow min-cut algorithm...

...which works in polynomial time on the number of edges of the graph $(= \|u\| = n)$ and the number of vertices $(= 2r)$.

Third ingredient: max-flow min-cut algorithm.

Given a graph X (unoriented and with weights on edges), and two vertices $s, t \in VX$, find the max flow from s to t:

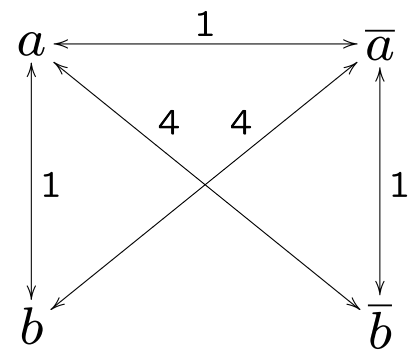


Observation:
maximal $(s \to t)$-flow $\leq$ cap. of any (s,t)-cut.

Theorem:
max. $(s \to t)$-flow $=$ cap. of min. (s,t)-cut,

and it is possible to find both in polynomial time w.r.t. the size of the graph.

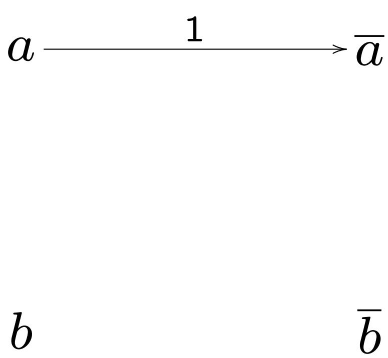
Example: Find one of the best Whitehead autos for $u = ba\overline{b}\,\overline{a}\,\overline{b}\,\overline{a}\,\overline{a}baba$.

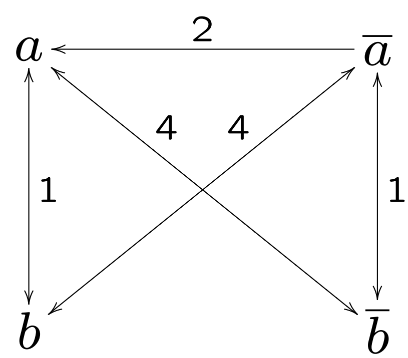
Wh. graph $=$ 

- Choose first multiplier, say a;
- Choose an augmenting path from a to $\overline{a}$:

$$a \xrightarrow{1} \overline{a}\,;$$

- Total flow: residual graph:

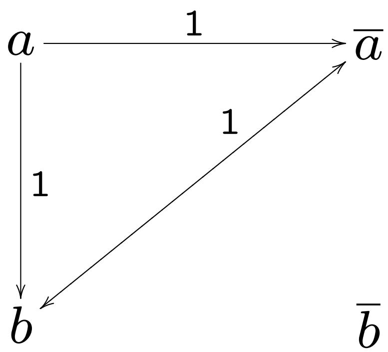
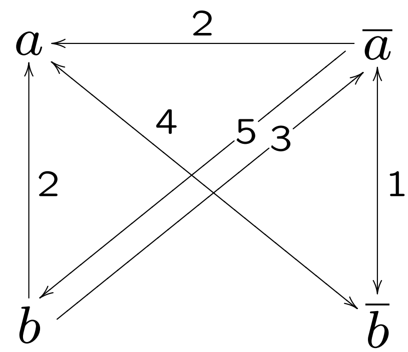




- Choose another augm. path from a to $\overline{a}$:

$$a \xrightarrow{1} b \xrightarrow{1} \overline{a}\,;$$

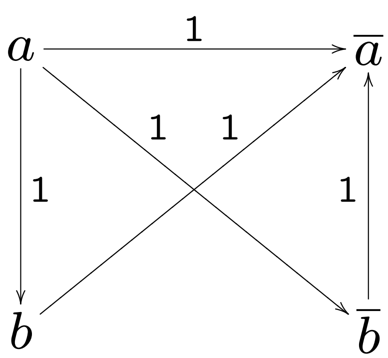
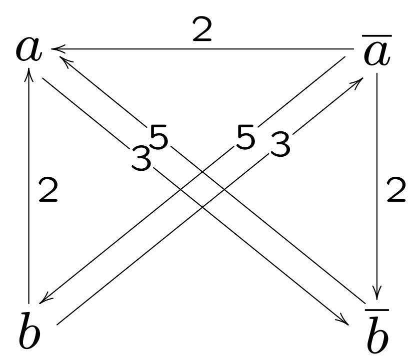
- Total flow: residual graph:

- Choose another augm. path from a to $\overline{a}$:

$$a \xrightarrow{1} \overline{b} \xrightarrow{1} \overline{a}\,;$$

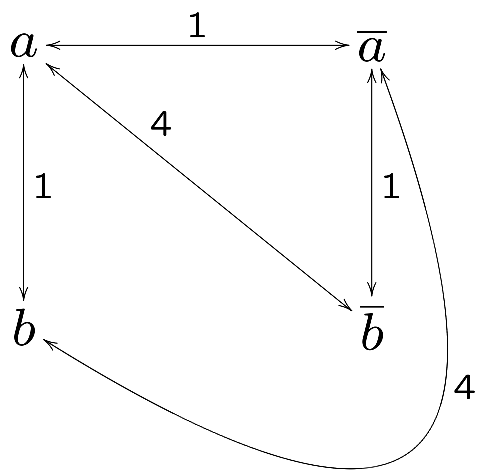
- Total flow: residual graph:

- No paths from a to $\overline{a}$, so STOP.

The total flow carried from a to $\overline{a}$ is 3 and corresponds to the cut

$$Y = \{v \mid \exists \text{ path } a \to v \text{ in res. graph}\}.$$



; $\qquad$ $\text{cap}(\{a, \overline{b}\}) = 3$.

So, the Whitehead auto

$$Y = \{a, \overline{b}\} \quad \equiv \quad \begin{array}{ccc} a & \overset{\alpha}{\mapsto} & a \\ b & \mapsto & \overline{a}b \end{array}$$

satisfies $\|u\alpha\| - \|u\| = 3 - 6 = -3$.

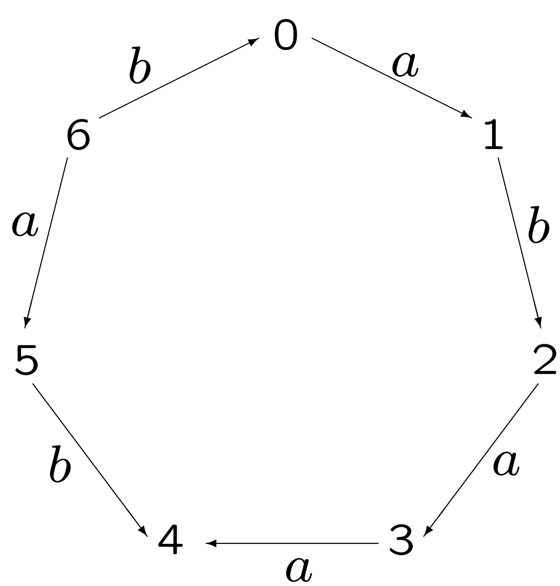
- Repeat for multiplier b (and get less).

$$\boxed{\begin{array}{rcl} u = ba\overline{b}\,\overline{a}\,\overline{b}\,\overline{a}\,\overline{a}baba & \mapsto & (\cancel{\overline{a}}b)a(\overline{b}\cancel{a})\cancel{\overline{a}}(\overline{b}\cancel{a})\cancel{\overline{a}}\,\overline{a}(\overline{a}b)\cancel{a}(\cancel{\overline{a}}b)\cancel{a} \\ & \sim & ba\overline{b}\,\overline{b}\overline{a}\,\overline{a}bb \\ \\ \|u\| = 11 & , & \|u\alpha\| = 8. \end{array}}$$

An extension to subgroups

A cyclically reduced word can be thought as a circular graph:

$$u = abaa\overline{b}\overline{a}b \quad \leftrightarrow \quad \langle abaa\overline{b}\overline{a}b \rangle$$



and $Wh(u)$ just describes the in-links of the vertices:

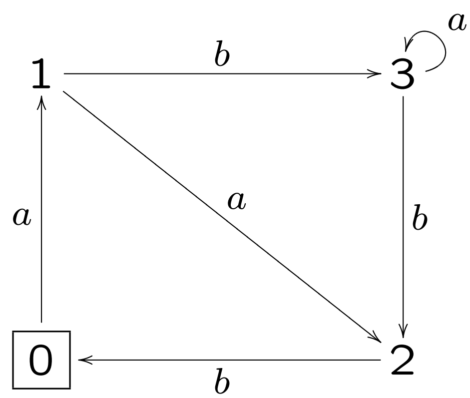
$$\xrightarrow{b} \underset{0}{\cdot} \xleftarrow{\overline{a}} \qquad \xrightarrow{a} \underset{1}{\cdot} \xleftarrow{\overline{b}} \qquad \xrightarrow{b} \underset{2}{\cdot} \xleftarrow{\overline{a}} \qquad \xrightarrow{a} \underset{3}{\cdot} \xleftarrow{\overline{a}}$$

$$\xrightarrow{a} \underset{4}{\cdot} \xleftarrow{b} \qquad \xrightarrow{\overline{b}} \underset{5}{\cdot} \xleftarrow{a} \qquad \xrightarrow{\overline{a}} \underset{6}{\cdot} \xleftarrow{\overline{b}}$$

Any f.g. subgroup $H \leq F_r$ has a (unique) representation as a core-graph labeled by generators (think about covering spaces over the bouquet):

$$H = \langle a^2 b,\, ab^3,\, abab^2 \rangle \leq F_2$$

$$\Gamma(H) \quad =$$



Looking at the in-links of vertices,

$$\xrightarrow{b} \underset{0}{\cdot} \xleftarrow{\overline{a}} \qquad \xrightarrow{a} \overset{1}{\underset{\uparrow \overline{a}}{\cdot}} \xleftarrow{\overline{b}} \qquad \xrightarrow{\overline{b}} \overset{2}{\underset{\uparrow a}{\cdot}} \xleftarrow{b} \qquad \xrightarrow{b} \overset{\downarrow a}{\underset{\uparrow \overline{b}}{\cdot}} \xleftarrow{\overline{a}}$$

we can built the Whitehead hypergraph $Wh(H)$:

$$VWh(H) = \{a,\, \overline{a},\, b,\, \overline{b}\},$$

$$EWh(H) = \{\{\overline{a},\, b\},\, \{a,\, \overline{a},\, \overline{b}\},\, \{a,\, b,\, \overline{b}\},\, \{a,\, \overline{a},\, b,\, \overline{b}\}\}.$$

Extension of Wh. Lemma: Given a f.g. subgroup $H \leq F_r$ and a Wh. auto α, think α as a cut in $Wh(H)$. Then,

$$\|H\alpha\| - \|H\| = \text{cap(cut)} - \text{deg(multiplier)},$$

where $\|\cdot\|$ means number of vertices of $\Gamma(H)$.

Theorem: There is an algorithm which, given a f.g. $H \leq F_r$, finds $\varphi \in Aut(F_r)$ s.t. the number of vertices in $H\varphi$ is minimal. It works in time $O(n^3 r^4)$.

Why?... Unfortunately flows for hypergraphs make no sense, but it is still possible to find min-cuts in polynomial time:

Definition: Let V be a finite set. A map $f\colon \mathcal{P}(V) \to \mathbb{R}$ is called submodular if

$$f(A \cup B) + f(A \cap B) \leq f(A) + f(B), \ \forall A, B \subseteq V.$$

Observation: For a f.g. $H \leq F_r$, $W = Wh(H)$, the map $\mathcal{P}(X^{\pm 1}) \to \mathbb{N}$, $\quad Y \mapsto \text{cap}_W(Y)$ is submodular.

Efficient minimization of submodular functions f is an active research topic in computer science, and there are several known algorithms for this, making a polynomial number of oracle calls (queries to evaluate f).

So, we have the result like in the word case.

Corollary: There is a polynomial time algorithm to decide, given two f.g. subgroups $H \leq K \leq F_r$, whether H is a free factor of K.
(note that $r(H)$ and $r(K)$ can be arbitrarily bigger than r).

Open questions

1) Any algebraic interpretation of "flow" ?

2) Cut-vertices:

$$u \text{ is primitive } \Rightarrow Wh(u) \text{ has a cut vertex}$$

$$H \text{ is a f.f. of } F_r \overset{?}{\Rightarrow} Wh(H) \text{ has a cut vertex}$$

3) Can also the second part of Whitehead algorithm be made polynomial ?

$\longrightarrow$ Miasnikov-Shpilrain: yes for $r = 2$.
$\longrightarrow$ Lee: yes for fix r under a technical condition on the original word.

4) What about minimizing (and counting) the number of Whitehead autos used ?

Thank you