Decision Problems in Algebra

(FCUL Summer School)

António Malheiro

CMA/FCT
Universidade Nova de Lisboa

Acknowledgement:
This work was supported by CMA within the projects
UID/MAT/00297/2013
PTDC/MHC-FIL/2583/2014
financed by 'Fundação para a Ciência e a Tecnologia'

June 2018

Outline

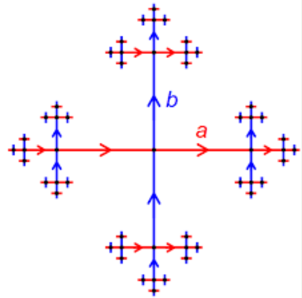
The Cayley graph of a group

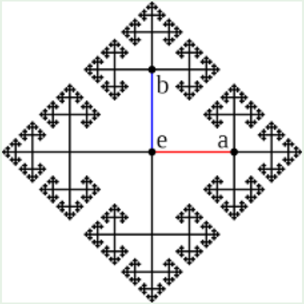
Let G be a group with generators A.

The Cayley graph $\Gamma(G, A)$ is the coloured directed graph with:

- vertices: G
- colors: A
- edges $g \xrightarrow{a} ga$

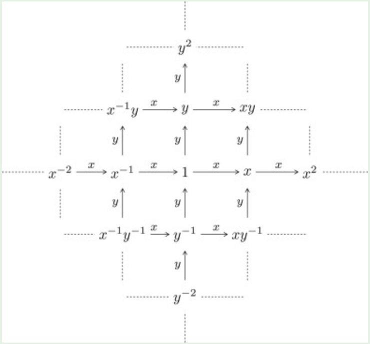
Example (Free group of rank 2: $\langle a, b \mid \rangle_{gr}$)

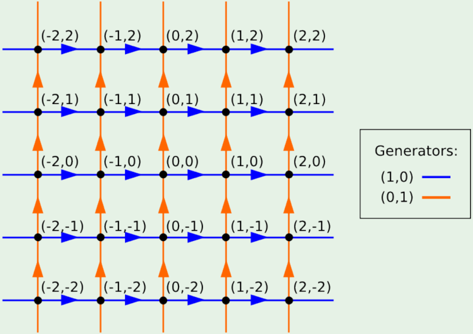




The Cayley graph of a group

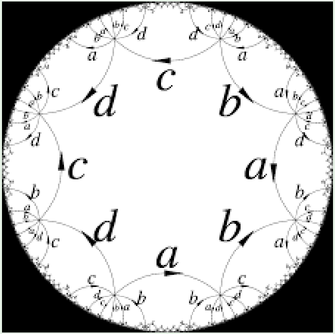
Example (Free abelian group of rank 2: $\langle a, b \mid [a,b] \rangle$)





The Cayley graph of a group

Example (Fundamental group of double torus: $\langle a, b, c, d \mid [a, b][c, d] \rangle$)

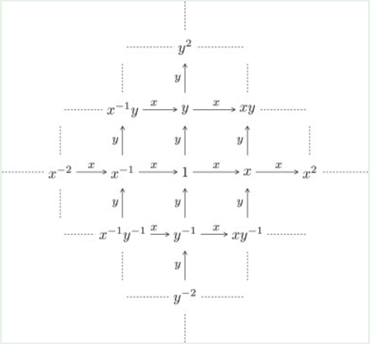


Hyperbolic groups

In a Cayley graph Γ of a group we can define:

- distance between g and h - minimal number of edges of a path in Γ connecting g and h;
- geodesic between g and h - a shortest path in Γ connecting g and h.

Example (Free abelian group of rank 2: $\langle a, b \mid [a, b] \rangle$)

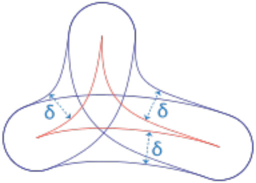


Hyperbolic groups

Let Γ be the Cayley graph of a group.

Geodesic triangle

A geodesic triangle Δ in Γ, is a triangle where each side is a geodesic.



δ-hyperbolic

Γ is said to be δ-hyperbolic (for $\delta > 0$) if for every geodesic triangle Δ in Γ, each edge in Δ lies in the δ-neighborhood of the two other paths.

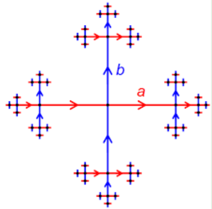
Hyperbolic groups

Word hyperbolic group

A finitely generated group G is said to be hyperbolic if the Cayley graph associated to some (and hence any) generating set is δ-hyperbolic for some δ.

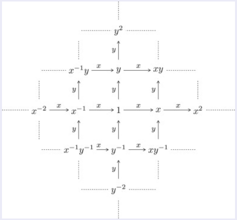
Example

Finite groups; free groups.



Non-example

Free abelian group of rank 2, $\mathbb{Z}^2$.



Mikhail Gromov

Hyperbolic groups

Properties of hyperbolic groups

- Finitely presented;
- Have solvable word and conjugacy problems.

Characterizations:

For a f.p. group G, TFAE:

- G is hyperbolic;
- G has a Dehn's algorithm;
- G has linear Dehn function.

Recall: A group G on the generators A has a Dehn algorithm if:

- there exists a finite list of pairs $(u_1, v_1), \ldots, (u_n, v_n)$ with $|u_i| > |v_i|$; and
- if w is a reduced word representing the identity, then w contains some u_i as a factor.

Abstract Reduction Systems (ARS)

An ARS is a pair $(X, \to)$ where;

- X is a set;
- $\to$ is a binary relation on X.

We write:

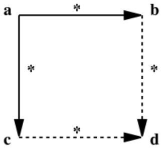
- $a \to b$ to indicate that $(a, b) \in \to$;
- $a \xrightarrow{*} b$ for $a = a_1 \to a_2 \to \cdots \to a_n = b$;

Two fundamental properties:

Termination: for every $a \in X$ there is no infinite sequence

$$a \to a_1 \to a_2 \to \cdots \to a_n \to \ldots.$$

Confluence: whenever $a \xrightarrow{*} b$ and $a \xrightarrow{*} c$, then $b \xrightarrow{*} d$ and $c \xrightarrow{*} d$, for some d; pictorially



Abstract Reduction Systems (ARS)

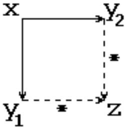
We write:

- $a \leftrightarrow b$ if either $a \to b$ or $a \leftarrow b$;
- $a \overset{*}{\leftrightarrow} b$ if $a = a_1 \leftrightarrow a_2 \leftrightarrow \cdots \leftrightarrow a_n = b$;
- a is said irreducible if there is no $b \in X$ s.t. $a \to b$; $a\downarrow$ denotes the unique (if exists) irreducible s.t. $a \overset{*}{\leftrightarrow} a\downarrow$.

Theorem

If $\to$ is terminating and confluent, then $x \overset{*}{\leftrightarrow} y \Leftrightarrow x\downarrow = y\downarrow$.

Locally confluent if $x \to y_1$ and $x \to y_2$ implies that $y_1 \overset{*}{\to} z$ and $y_2 \overset{*}{\to} z$, for some z, pictorially



Newman's Lemma

A terminating relation is confluent if it is locally confluent.

Word problem for D_3

Consider the presentation of D_3: $\langle a, b \mid a^3 \to 1,\ b^2 \to 1,\ ab \to ba^2 \rangle$.

The word problem for D_3 is decidable

For a word w in the generators $\{a, b\}$:

1. Compute the reduced word $\overline{w}$ such that $w \xrightarrow{*} \overline{w}$;
2. Check if $\overline{w}$ is the empty word.

This algorithm works because $\to$ is ...

- terminating;
- locally confluent.

To check termination: note that if $u \to v$ then ...

1. number of b's in u is greater than in v; or is equal and
2. $u = u_0 b u_1 b \dots b u_n$ and $v = v_0 v u_1 b \dots b v_n$; and thus $|u_0| > |v_0|$; or $u_0 = v_0$ and $|u_1| > |v_1|$; or .... ; or $u_0 = v_0, \dots, u_{n-1} = v_{n-1}$ and $|u_n| > |v_n|$.

Word problem for D_3

To check local confluence:

It is enough to check if all critical pairs are resolved.

Critical pair The pair of words resulting from a single step reduction from an overlap between left-hand sides of the relations.

Example (Critical pairs in $a^3 \to 1,\ b^2 \to 1,\ ab \to ba^2$)

Overlaps: $\underbrace{a^3}b = a^2\overbrace{ab}$ and $\underbrace{ab}b = a\overbrace{b^2}$;

1st critical pair: $\{b, a^2ba^2\}$ since $a^3b \to b$ and $a^3b \to a^2ba^2$.

2nd critical pair: $\{ba^2b, a\}$ since $ab^2 \to ba^2b$ and $ab^2 \to a$.

1st c.p. is resolved: $a^2ba^2 \to aba^4 \to ba^6 \xrightarrow{*} b$.

2nd c.p. is resolved: $ba^2b \to baba^2 \to b^2a^4 \to a^4 \to a$.

Gröbner bases

Buchberger Algorithm

Data: A finite set F of polynomials from $\mathbb{K}[X_1, \ldots, X_n]$
Result: A Gröbner bases for the ideal generated by F.
$G := F$;
$C := \{\{g, h\} : g, h \in G, g \neq h\}$;
while $C \neq \emptyset$ **do**
    remove a pair $\{g, h\}$ from C;
    $k := \overline{\mathrm{spol}(g, h)}^G$;
    if $k \neq 0$ **then**
        Add all pairs $\{k, l\}$ with $l \in G$ to C;
        $G := G \cup \{k\}$;
    end
    return G;
end