Computations with finitely presented groups

Susan Hermiller

University of Nebraska

22 May 2017

Presenting groups, elements, and subgroups to a computer

Input: A = a finite set

Defines: $F = F(A)$ = free group on A

Presenting groups, elements, and subgroups to a computer

Input: A = a finite set
Defines: $F = F(A)$ = free group on A

Input: w = a word over $A \cup A^{-1}$
Defines: w = an element of F

Input: R = a finite set of elements of F
Defines: $G = \langle A \mid R \rangle = F(A)/ < R >^N$ = finitely presented group

Presenting groups, elements, and subgroups to a computer

Input: A = a finite set
Defines: $F = F(A)$ = free group on A

Input: w = a word over $A \cup A^{-1}$
Defines: w = an element of F

Input: R = a finite set of elements of F
Defines: $G = \langle A \mid R \rangle = F(A)/ < R >^N$ = finitely presented group

Input: w = a word over $A \cup A^{-1}$
Defines: w = an element of G
Need to be careful in GAP to specify elements of F versus G.

Input:Y = a finite set of elements of G
Defines: $H = \langle Y \rangle$ = finitely generated subgroup of G

Computations are not always possible

Algorithms wanted:

Order Problem. Input: Finitely presented group G.
Output: Order of G.

Index Problem. Input: Finitely generated subgroup $H \leq G$.
Output: $|G : H|$.

Word Problem. Fix f.p. group G.
Input: Word w over $A^{\pm 1}$.
Output: Yes/no,whether $w =_G 1$.

H-Subgroup Membership Problem.
Fix f.p. group G, f.g. subgroup H.
Input: Word w over $A^{\pm 1}$.
Output: Yes/no, whether $w \in H$.

Computations are not always possible

Algorithms wanted:

Order Problem. Input: Finitely presented group G.
Output: Order of G.

Index Problem. Input: Finitely generated subgroup $H \leq G$.
Output: $|G : H|$.

Word Problem. Fix f.p. group G.
Input: Word w over $A^{\pm 1}$.
Output: Yes/no,whether $w =_G 1$.

H-Subgroup Membership Problem.
Fix f.p. group G, f.g. subgroup H.
Input: Word w over $A^{\pm 1}$.
Output: Yes/no, whether $w \in H$.

However:

Thm. (Boone; Novikov; 1955) There are finitely presented groups G for which none of these algorithms can exist.

Computations often are possible

- Many groups have algorithms to solve all 4 problems.

- Many computations for infinite groups are “procedures”: they answer the question if possible, but will not halt if the answer cannot be found.

Art and Philosophy:

Computations often are possible

- Many groups have algorithms to solve all 4 problems.

- Many computations for infinite groups are "procedures": they answer the question if possible, but will not halt if the answer cannot be found.

Art and Philosophy:

- **Art:** Many computations involve making a "guess" along the way, and then verifying whether the guess was correct.

- **Philosophy:** Use GAP to gather experimental data about a "nice" family of groups, and use the data to make a conjecture to be proved.

Overview

(I) Examples of some computations in GAP

(II) Coset Enumeration (ACE / Todd-Coxeter)
(Order and Index Problems)

- Using ACE to compute Stallings graphs
(Subgroup Membership Problem in free groups)

Overview

(I) Examples of some computations in GAP

(II) Coset Enumeration (ACE / Todd-Coxeter)
(Order and Index Problems)

- Using ACE to compute Stallings graphs
(Subgroup Membership Problem in free groups)

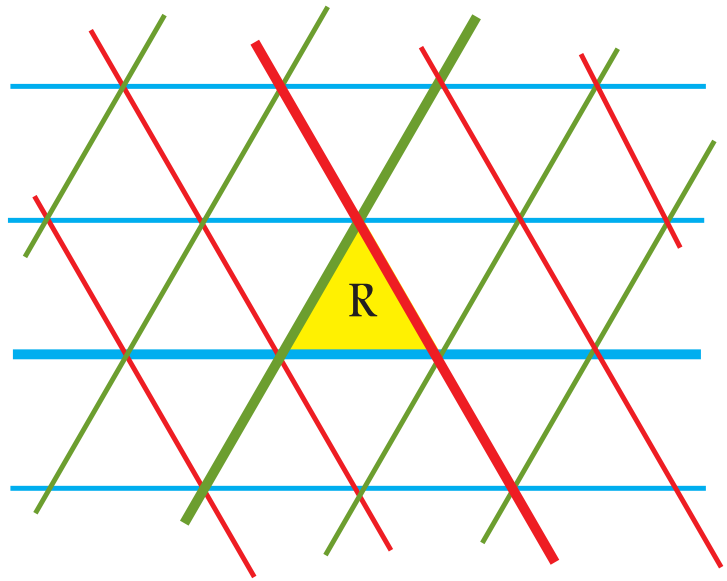
(III) Example: Computing growth of groups - definition, pictures, experimentation

(IV) Rewriting Systems
(Word Problem)

(I) Examples of some computations in GAP

Script at www.math.unl.edu/∼smh/wam/firstexamples.g

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

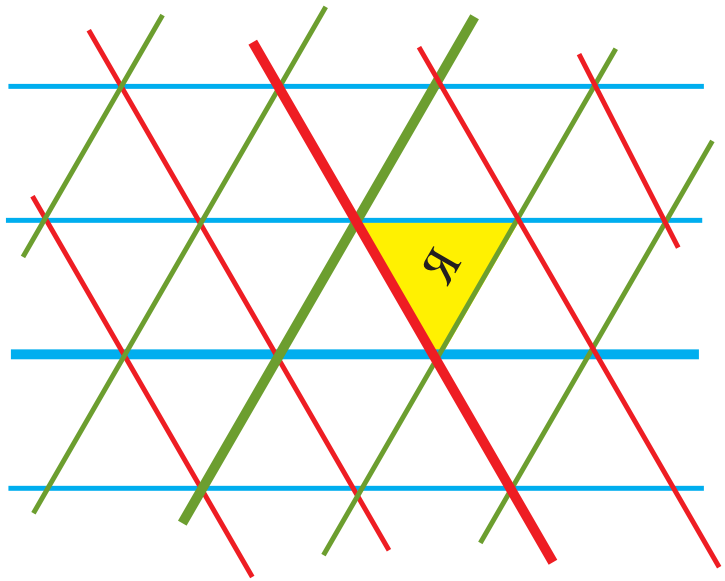
c = reflection across the thick green line

Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

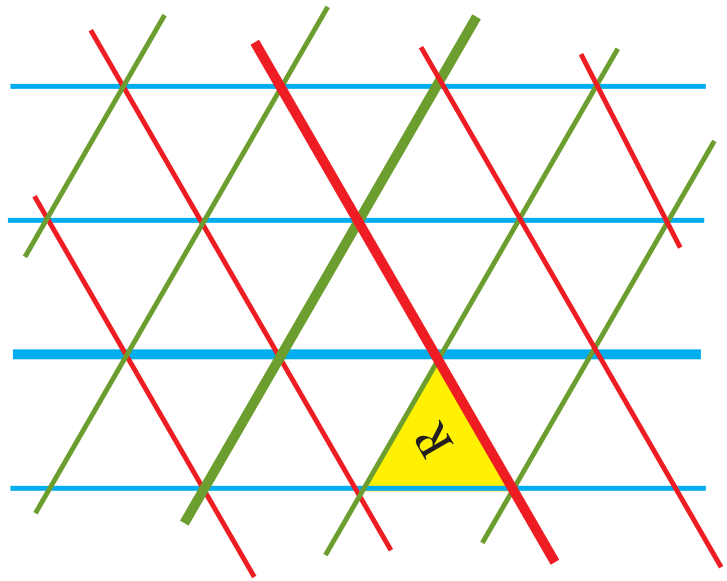
c = reflection across the thick green line

Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

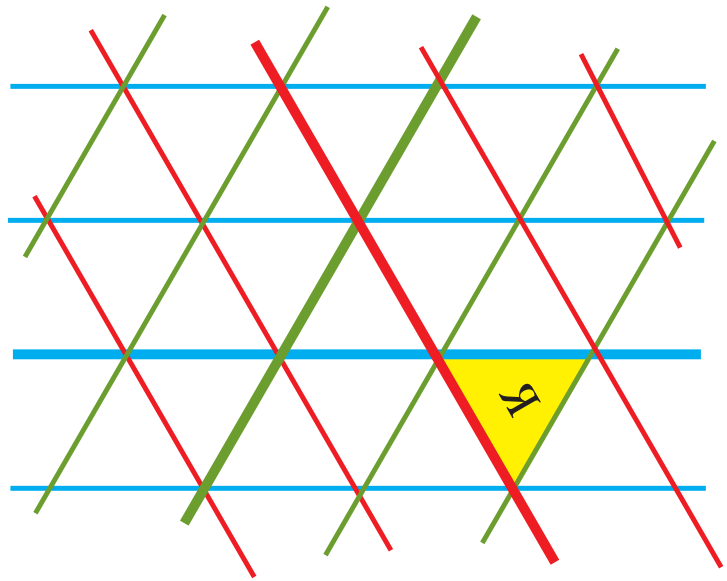
c = reflection across the thick green line

Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

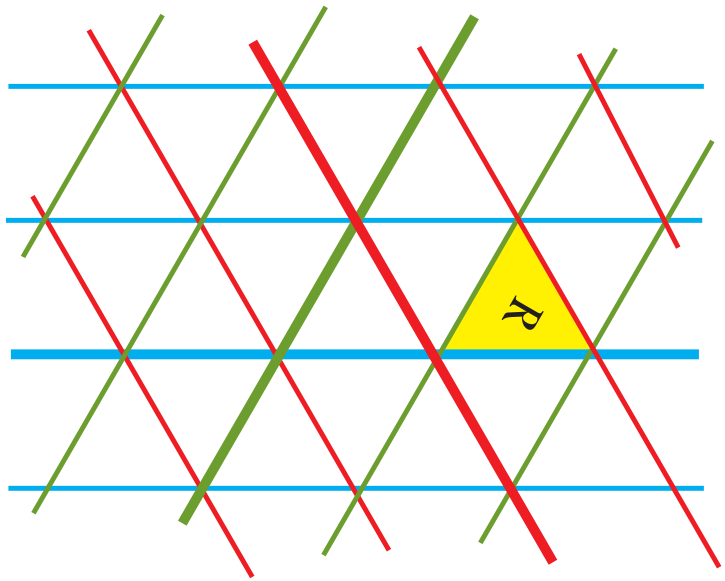
c = reflection across the thick green line

Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

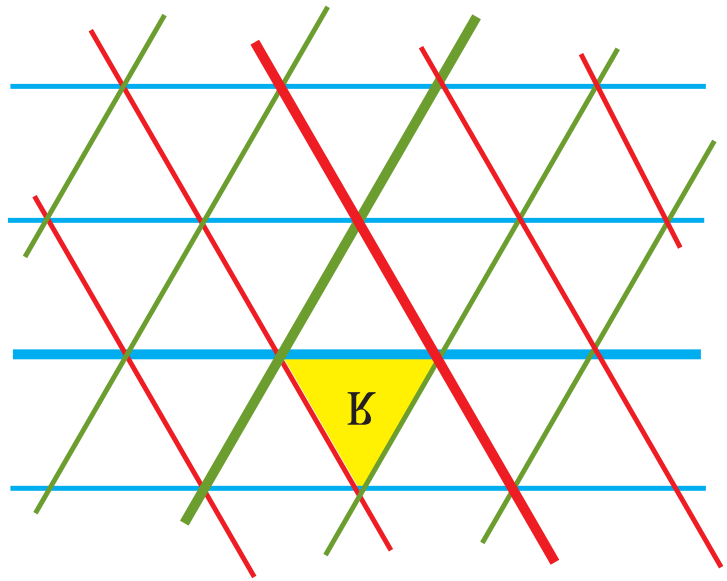
c = reflection across the thick green line

Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

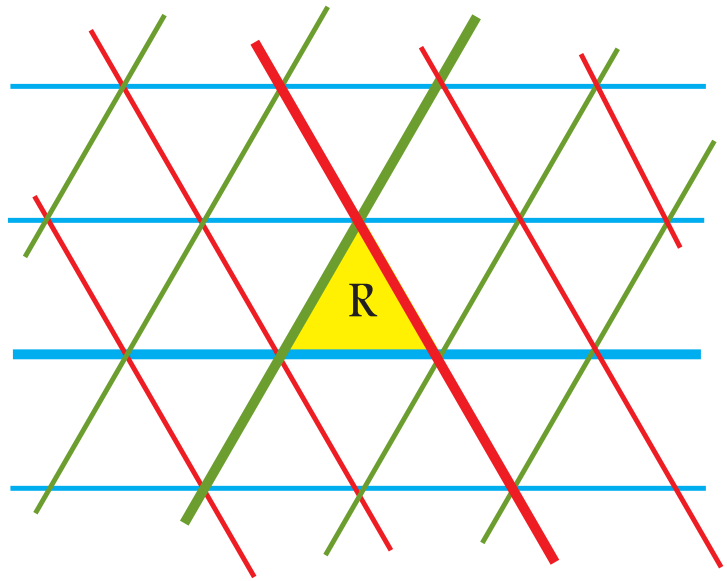
c = reflection across the thick green line

Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in the sides of an equilateral triangle



$G = \langle a, b, c \rangle$

a = reflection across the thick red line

b = reflection across the thick blue line

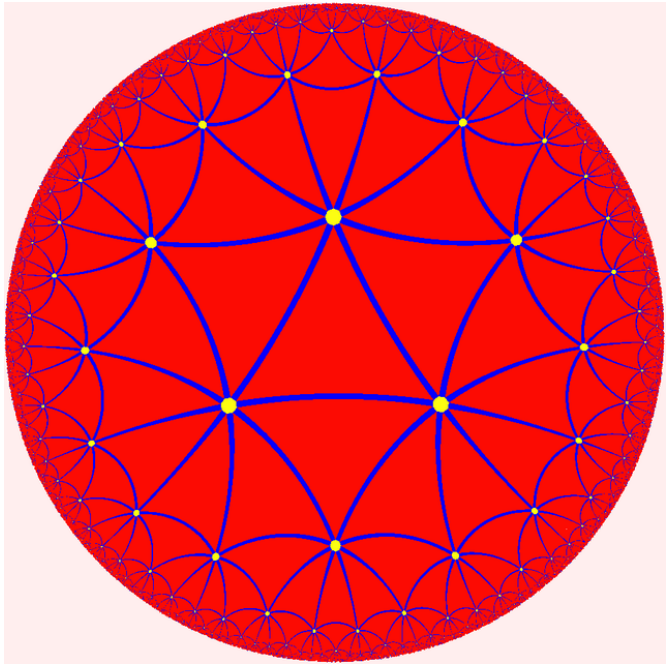
c = reflection across the thick green line

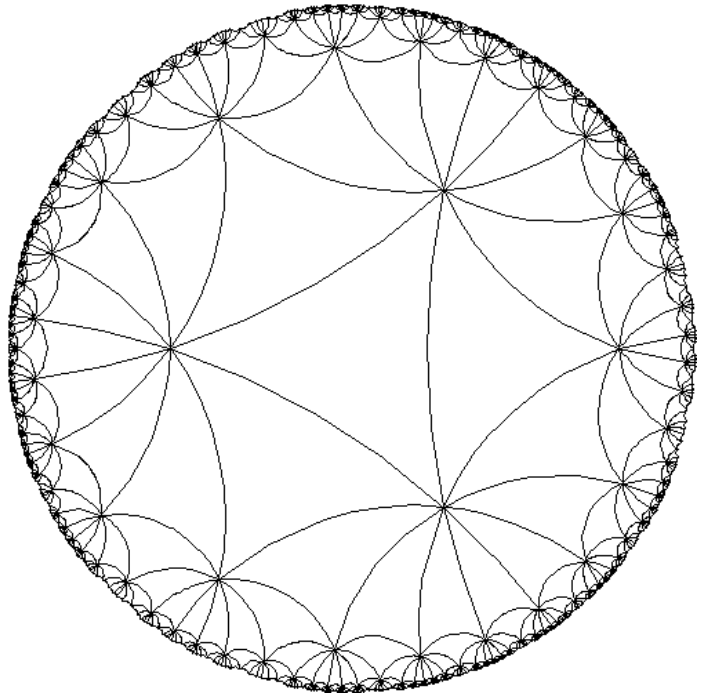
Note that aa, $ababab$ give the identity.

(Word Problem: What other words over a, b, c give the identity?)

$G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$.

(I) Reflections in hyperbolic triangles





Exercise:

Let n be a natural number,
$G_n := \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^n = (ac)^n = (bc)^n = 1 \rangle$, and
$H_n := \langle a, b, cac, cbc \rangle$.

Make a conjecture on the index $|G_n : H_n|$ as a function of n.

(II) Coset Enumeration

Start with:

$G = \langle A \mid R \rangle$ and $H = \langle B \rangle$

End with: Finite list of cosets 1,2,3,... and (Schreier) coset graph if $|G : H| < \infty$.

Coset 1 is H.

Build 3 sets of tables:

(Columns $\leftrightarrow$ interstices between letters of words.)

(1) Elements of $A^{\pm 1}$ (generators of G)

(Rows $\leftrightarrow$ set of cosets)

(2) Elements of B (generators of H)

(One row, $\leftrightarrow$ coset 1 = coset H)

(3) Elements of R (relators of G)

(Rows $\leftrightarrow$ set of cosets)

(II) Coset enumeration, continued

Steps - all repeated; “art” is in ordering the steps

- Add a coset
- “Scan” left and right, for all places each coset occurs
- Determine “deductions” - info on $C \cdot a$ for coset C, $a \in A$.
- Determine “collapses” - equality of 2 cosets in list

Examples:
(On board and using GAP)

(II) Example of coset enumeration and computing a Stallings graph in GAP

Script at www.math.unl.edu/∼smh/wam/ce_examples.g

Exercise:

Let $F := FreeGroup(\text{“}a\text{”}, \text{“}b\text{”})$ and
$H = \langle a^2,$
$b^{-2},$
$ab^2a^{-1},$
$b^{-1}a^2b,$
$ababab,$
$b^{-1}a^{-1}b^{-2}ab,$
$b^{-1}a^{-1}b^{-1}ab^{-1}a^{-1}\rangle.$
Compute (and draw) the Stallings graph for H, and determine $|G : H|$.

Overview

(I) Examples of some computations in GAP

(II) Coset Enumeration (ACE / Todd-Coxeter)
(Order and Index Problems)

- Using ACE to compute Stallings graphs
(Subgroup Membership Problem in free groups)

Overview

(I) Examples of some computations in GAP

(II) Coset Enumeration (ACE / Todd-Coxeter)
(Order and Index Problems)

- Using ACE to compute Stallings graphs
(Subgroup Membership Problem in free groups)

(III) Example: Computing growth of groups - definition, pictures, experimentation

(IV) Rewriting Systems
(Word Problem)

(III) Example: Computing growth of groups

Setup: $G = \langle A \rangle, \qquad |A| < \infty$

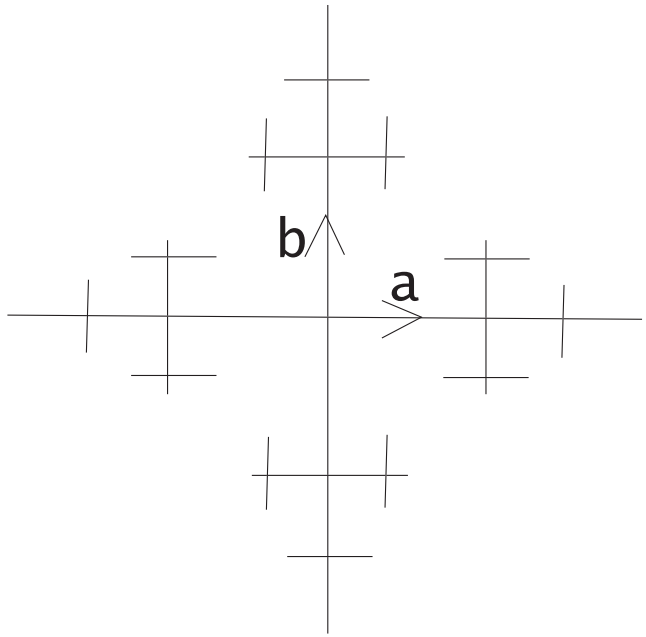
$S(n) := |\ \{g \in G \mid d(1,g) \leq n\}\ |$ = sphere of radius n

Def. The **growth series** of G over A is

$$\gamma(z) := \sum_{n=0}^{\infty} |\ S(n)\ | z^n.$$

(III) Example: Growth, continued

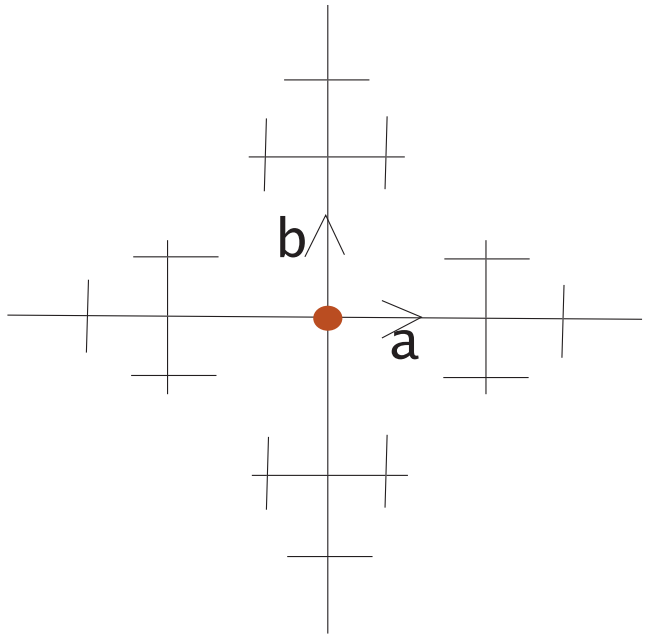
Example: $G = F_2 = \langle a, b \mid \ \rangle$



$$\gamma(z) =$$

(III) Example: Growth, continued

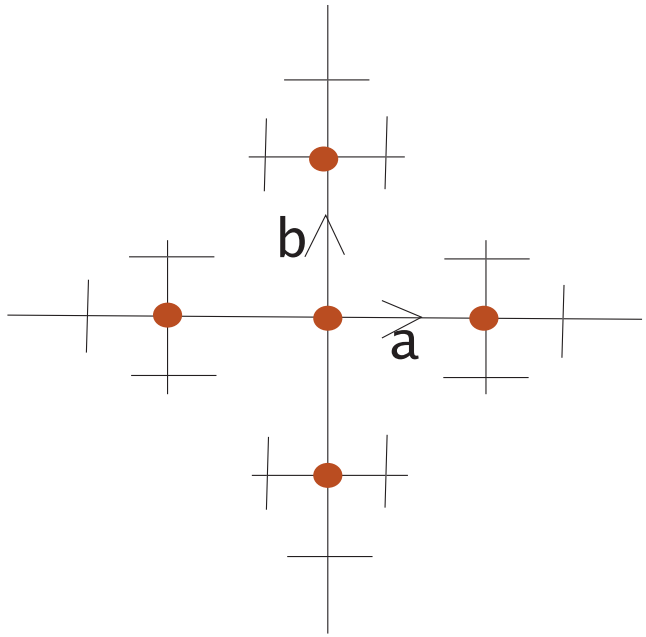
Example: $G = F_2 = \langle a, b \mid \ \rangle$



$$\gamma(z) = 1+$$

(III) Example: Growth, continued

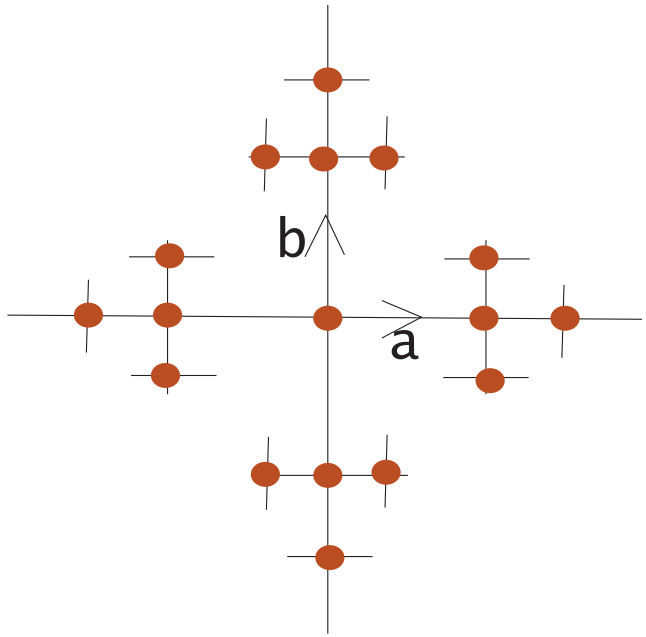
Example: $G = F_2 = \langle a, b \mid \ \rangle$



$$\gamma(z) = 1 + 4z +$$

(III) Example: Growth, continued

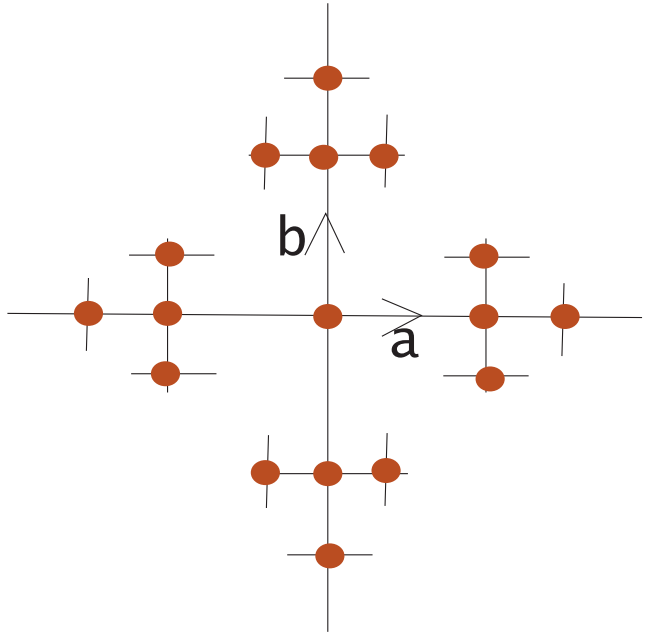
Example: $G = F_2 = \langle a, b \mid \ \rangle$



$$\gamma(z) = 1 + 4z + 4 \cdot 3z^2 +$$

(III) Example: Growth, continued

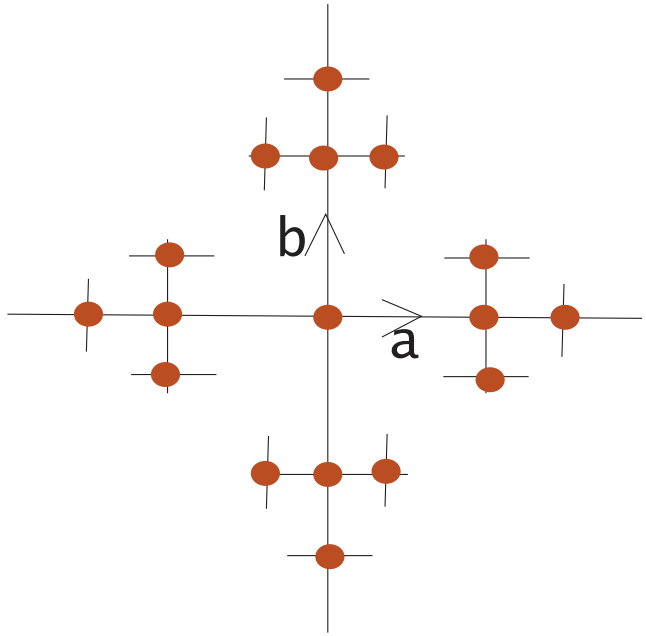
Example: $G = F_2 = \langle a, b \mid \ \rangle$



$$\gamma(z) = 1 + 4z + 4 \cdot 3z^2 + \cdots + 4 \cdot 3^n z^{n+1} + \cdots$$

(III) Example: Growth, continued

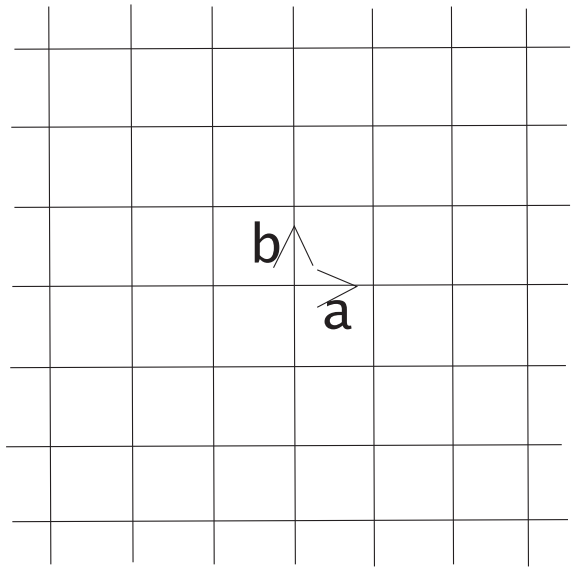
Example: $G = F_2 = \langle a, b \mid \ \rangle$



$$\gamma(z) = 1 + 4z(\sum_{n=0}^{\infty}(3z)^n) = 1 + 4z(\frac{1}{1-3z}) = \frac{1+z}{1-3z}$$

(III) Example: Growth, continued

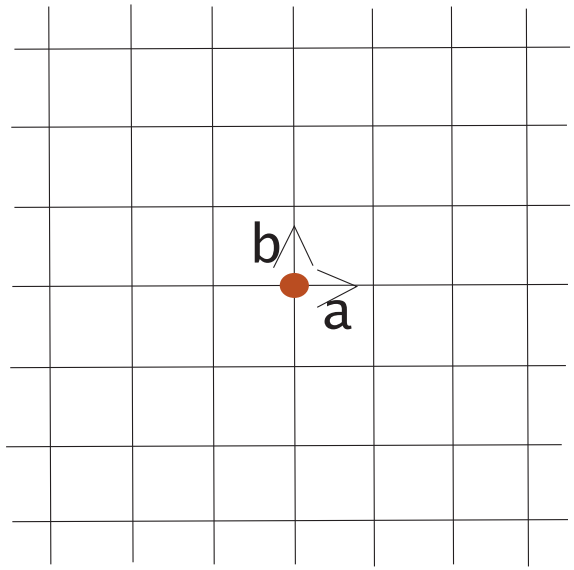
Example: $G = \mathbf{Z}^2 = \langle a, b \mid ab = ba \rangle$



$$\gamma(z) =$$

(III) Example: Growth, continued

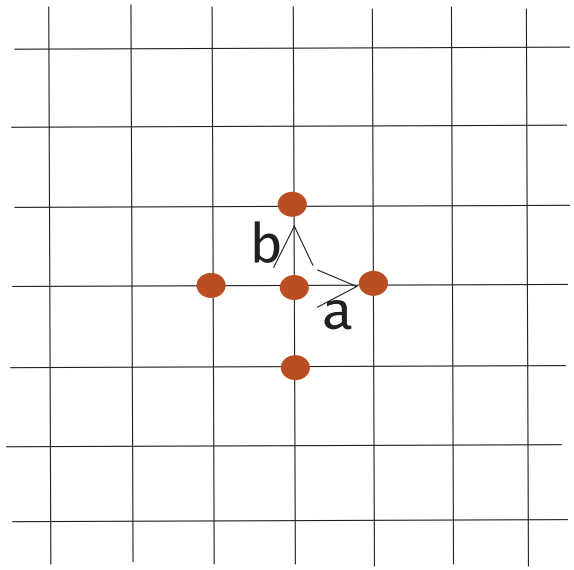
Example: $G = \mathbf{Z}^2 = \langle a, b \mid ab = ba \rangle$



$$\gamma(z) = 1+$$

(III) Example: Growth, continued

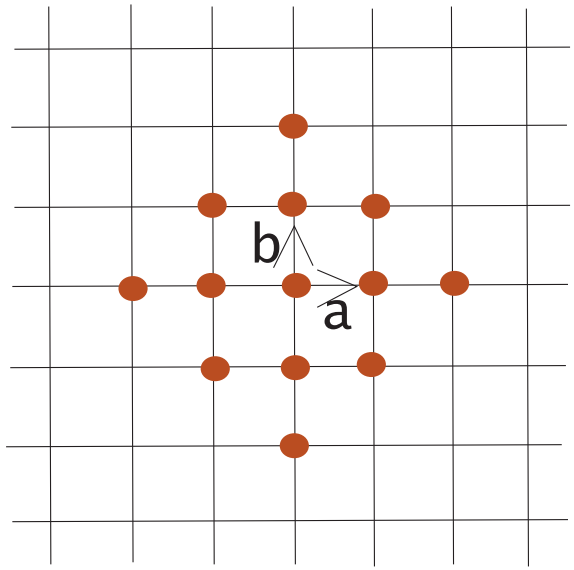
Example: $G = \mathbf{Z}^2 = \langle a, b \mid ab = ba \rangle$



$$\gamma(z) = 1 + 4z +$$

(III) Example: Growth, continued

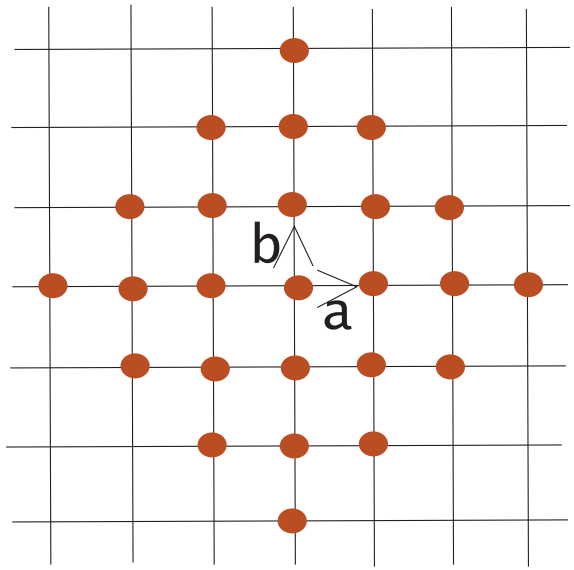
Example: $G = \mathbf{Z}^2 = \langle a, b \mid ab = ba \rangle$



$$\gamma(z) = 1 + 4z + 8z^2 +$$

(III) Example: Growth, continued

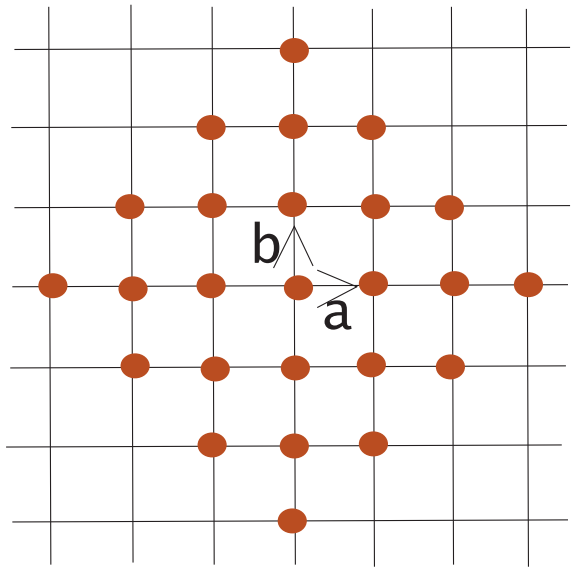
Example: $G = \mathbf{Z}^2 = \langle a, b \mid ab = ba \rangle$



$$\gamma(z) = 1 + 4z + 8z^2 + 12z^3 +$$

(III) Example: Growth, continued

Example: $G = \mathbf{Z}^2 = \langle a, b \mid ab = ba \rangle$



$$\gamma(z) = (z^2 + 2z + 1)/(z^2 - 2z + 1)$$

(III) Example: Growth series computations in GAP

Notes:
(1) The growth series is computable if and only if there is an algorithm to solve the Word Problem.
(Hence not all growth series are computable.)
(2) Not all computable growth series are rational functions.

Script at www.math.unl.edu/∼smh/wam/growthexamples.g

Exercise:

Let $n \geq 3$, and
$G_n := \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^n = (ac)^n = (bc)^n = 1 \rangle$.

Make a conjecture on the growth series of G_n as a function of n.

(IV) Rewriting systems

Setup: A = finite set $\qquad B := A \cup A^{-1}$

B^* = set of all words over B

Def. A **rewriting system** for a group G is a finite subset $R \subseteq B^* \times B^*$ such that the rewriting operations of the form $xuy \to xvy$ for all $(u, v) \in R$ and $x, y \in B^*$ satisfy:

Presentation: The set of equivalence classes $B^*/\sim$ for the least equiv. rel. such that $w \sim z$ whenever $w \to z$, with the concatenation operation, is a group isomorphic to G.

Termination: There is no infinite sequence of rewritings $x \to x_1 \to x_2 \to \ldots$

Confluence: If $(rs, v), (st, w) \in R$ with $s \neq 1$, there are rewritings $vt \to^* z$, $rw \to^* z$ for some $z \in B^*$.

(And if $(rst, v), (s, w) \in R$, there are rewritings $v \to^* z$, $rwt \to z$.)

(IV) Rewriting systems

Setup: A = finite set $\qquad B := A \cup A^{-1}$

B^* = set of all words over B

Def. A **rewriting system** for a group G is a finite subset $R \subseteq B^* \times B^*$ such that the rewriting operations of the form $xuy \to xvy$ for all $(u, v) \in R$ and $x, y \in B^*$ satisfy:

Presentation: The set of equivalence classes $B^*/\sim$ for the least equiv. rel. such that $w \sim z$ whenever $w \to z$, with the concatenation operation, is a group isomorphic to G.

Termination: There is no infinite sequence of rewritings $x \to x_1 \to x_2 \to \ldots$

Confluence: If $(rs, v), (st, w) \in R$ with $s \neq 1$, there are rewritings $vt \to^* z$, $rw \to^* z$ for some $z \in B^*$.

(And if $(rst, v), (s, w) \in R$, there are rewritings $v \to^* z$, $rwt \to z$.)

(IV) Rewriting systems, continued

Example. $G = \mathbb{Z}^2 = \langle a, b \mid ab = ba \rangle$.

$$A = \{a, b\} \qquad B = \{a, b, a^{-1}, b^{-1}\}.$$

$$R = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, ba \to ab\}$$

satisfies Presentation and Termination, but *not Confluence*.

(IV) Rewriting systems, continued

Example. $G = \mathbb{Z}^2 = \langle a, b \mid ab = ba \rangle$.

$$A = \{a, b\} \qquad B = \{a, b, a^{-1}, b^{-1}\}.$$

$$R = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, ba \to ab\}$$

satisfies Presentation and Termination, but *not Confluence*.

$$R = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, ba \to ab, ba^{-1} \to a^{-1}b, b^{-1}a \to ab^{-1}, b^{-1}a^{-1} \to a^{-1}b^{-1}\}$$

is complete.

(IV) Rewriting systems, continued

Example. $G = \mathbb{Z}^2 = \langle a, b \mid ab = ba \rangle$.

$$A = \{a, b\} \qquad B = \{a, b, a^{-1}, b^{-1}\}.$$

$$R = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, ba \to ab\}$$

satisfies Presentation and Termination, but *not Confluence*.

$$R = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, ba \to ab, ba^{-1} \to a^{-1}b, b^{-1}a \to ab^{-1}, b^{-1}a^{-1} \to a^{-1}b^{-1}\}$$

is complete.

Checking termination: Decrease shortlex ordering.
(Or other ordering on B^* with no $x > x_2 > x_3 > \cdots$.)

(IV) Rewriting systems, continued

Notes:
(1) Each $g \in G$ is represented by a unique irreducible word - one that cannot be rewritten - over B. (Knuth-Bendix; Newman)

(2) Word Problem solution: Input $w \in B^*$. Rewrite until an irreducible word w' is reached (by Termination). Then $w =_G 1$ if and only if w' is the empty word.

Example. $G = \mathbb{Z}^2$ $\qquad B = \{a, b, a^{-1}, b^{-1}\}$

$$R = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1,$$
$$ba \to ab, ba^{-1} \to a^{-1}b, b^{-1}a \to ab^{-1}, b^{-1}a^{-1} \to a^{-1}b^{-1}\}$$

Irreducible words: $\{a^i b^j \mid i, j \in \mathbb{Z}\}$

(IV) Rewriting system computations in GAP

Script at www.math.unl.edu/∼smh/wam/rewritingexamples.g

(IV) Rewriting system computations in GAP

Script at www.math.unl.edu/∼smh/wam/rewritingexamples.g

Exercise:

Let $G := \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^3 = 1 \rangle$ and $w = cacbabcaca$.

Compute (1) the complete rewriting systems for G,
(2) the irreducible words of length 6, and
(3) the reduced form of w,
with respect to the shortlex orders
(i) $a < b < c$, (ii) $b < c < a$, and (iii) $c < b < a$

(IV) Rewriting system computations in GAP, continued

Exercise:

Find a complete rewriting system for

$$G := \langle a, b, c, d \mid a^2 = b^2 = c^2 = d^2 = (ab)^4 = (ac)^4 = (ad)^3 = (bc)^3 = (bd)^4 = (cd)^4 = 1 \rangle$$

Art: Change the generators, change the ordering.

Explore the GAP and KBMAG manuals at

https://www.gap-system.org/Manuals/doc/ref/chap0.html

https://www.gap-system.org/Manuals/pkg/kbmag-1.5.4/htm/CHAP001.htm

for alternate strategies/options.

Happy computing!