Algorithmic problem in free groups

Pascal Weil (CNRS)

ISI, Sujata Ghosh's class, April 2024

Freely reduced words

- A a (finite) alphabet (= non-empty set), $\bar{A} = \{\bar{a} \mid a \in A\}$ disjoint from A, $\tilde{A} = A \cup \bar{A}$. $\tilde{A}^* =$ all words on $\tilde{A}$ (free monoid on $\tilde{A}$). 1 is the empty word.
- Notation: $\bar{\bar{a}} = a$,
- Want to see $\bar{a}$ as a (group) inverse of A: let $\sim$ be the congruence on $\tilde{A}^*$ generated by $a\bar{a} \sim \bar{a}a \sim 1$. That is: if $u, v \in \tilde{A}^*$, then $u \sim v$ iff there exist $u = u_0, u_1, \ldots, u_k = v$ such that, for each i, you go from u_i to u_{i+1} by deleting or inserting a factor $a\bar{a}$ ($a \in \tilde{A}$)
- Example
- u is *reduced* if it contains no factor $a\bar{a}$ ($a \in \tilde{A}$). Every word is $\sim$-equivalent to a reduced word (noetherian rewriting system $a\bar{a} \to 1$)
- confluent rewriting system = every $\sim$-class contains a single reduced word. Sketch of proof

Free group

- $F(A)$ = all reduced words. Multiplication: $u \cdot v = \mathrm{red}(uv)$. This operation is associative (because $\sim$ is a monoid congruence). Describe inverse. Thus $F(A)$ is a group, called *the free group on A*.
- Alternate description: $F(A) = \tilde{A}^*/\sim$ (monoid quotient, which turns out to be a group).
- If G is a group and $\varphi\colon A \to G$ is any map, then φ extends to a unique group homomorphism $\varphi\colon F(A) \to G$
- What if I change alphabet? Is $F(A)$ isomorphic to $F(B)$?
- Theorem: $F(A)$ is isomorphic to $F(B)$ if and only if $|A| = |B|$
- Sketch of proof: project $F(A)$ to the group $(\mathbb{Z}/2\mathbb{Z})^A = \bigoplus_{a \in A} \mathbb{Z}/2\mathbb{Z}a$, by mapping $a \in A$ and $\bar{a}$ to a. Surjective. An isomorphism $\varphi\colon F(A) \to F(B)$ yields an isomorphism $\varphi_2\colon (\mathbb{Z}/2\mathbb{Z})^A \to (\mathbb{Z}/2\mathbb{Z})^B$. Then linear algebra tells us that $|A| = \dim(\mathbb{Z}/2\mathbb{Z})^A$ and $|B| = \dim(\mathbb{Z}/2\mathbb{Z})^B$ are equal.

Rank and bases of a free group

- $|A|$ is **not** called the dimension of $F(A)$, it's called its *rank*
- and A is called a *basis* of $F(A)$, because every element of $F(A)$ can be written in a unique way as a reduced word on $\tilde{A}$
- Moreover, $F(A)$ has many bases! Suppose $A = \{a, b\}$
- Then $\{a, b\}$ is a basis. Also $\{a^{-1}, b\}$, $\{ab, b\}$, $\{b^{-1}ab, b\}$, $\{b^{-1}ab^2, b^{-1}ab\}$, etc.
- Infinitely many bases, in fact: if $\{u, v\}$ is a basis, so are $\{u^{-1}, v\}$ and $\{uv, u\}$
- Note that, $\{u, v\}$ is a basis of $F(A)$ if and only if the homomorphism $\varphi\colon F(c, d) \to F(a, b)$ given by $\varphi(c) = u$, $\varphi(d) = v$ is an isomorphism. So all the bases of $F(A)$ have cardinality 2. Extends to free groups of any rank.
- Question: let A be a r-letter alphabet and let $u_1, \cdots, u_r \in F(A)$. How do we decide whether $\{u_1, \ldots, u_r\}$ is a basis of $F(A)$?

Subgroups of a free group

- H, finitely generated subgroup of $F(A)$
- Theorem: Every subgroup of $F(A)$ is free. *Proof later*
- Contrary to vector spaces: if H is a subgroup of $F(A)$, the rank of H may be greater than $|A|$.
- Example: in $F(a, b)$, the set $\{b^i ab^{-i} \mid i \in \mathbb{Z}\}$ freely generates a subgroup, or infinite (countable) rank. *Proof later*
- Problems: given $g, g_1, \ldots, g_n \in F(A)$, and $H = \langle g_1, \ldots, g_n \rangle$,
  - is g in H? (uniform membership problem)
  - what is the rank of H? compute a basis for H

Stallings graph of a subgroup

- $H = \langle g_1, \ldots, g_n \rangle$, finitely generated subgroup of $F(A)$: construct a labeled graph (automaton) characterizing H
- Example: $\langle a^2ba, baba^{-1}, b^{-1}aba^{-1}, a^3, b^2 \rangle$
- Algorithm: write the g_i as circuits around a common vertex v_0
- fold
- It always stops
- It is confluent
- It depends on H only, not on the choice of $g_1, \ldots, g_n$ *elements of proof to come*

The language of the Stallings graph of H

- Seen as an automaton with initial and accepting state v_0: the languages of the intermediate Γ_i (over alphabet $\tilde{A}$) grow; for every $u \in H$, $L(\Gamma_i)$ contains some v such that $\mathrm{red}(v) = u$; if u is accepted by one of the intermediate Γ_i, then $\mathrm{red}(u)$ is an element of H; if u is reduced and in H, then $u \in L(\Gamma_i)$ for some i.
- So a reduced word is in H if and only if it is accepted by $L(\Gamma(H))$ = solution of the uniform membership problem (in polynomial time)

Applications: computation of a basis, intersection

- Is $g_1, \ldots, g_n$ a basis of $F(A)$: compute $\Gamma(H)$ and check whether it is the bouquet of n length 1 loops (using uniqueness)
- Basis of H: choose a spanning tree T of $\Gamma(H)$, get a generating set
- Theorem: This generating set freely generates H: H is free and our generating set is a basis
- So we know the rank
- Compute the intersection of two subgroups
- Corollary: Howson (1954)
- Tricky but elementary: $rank(H \cap K) - 1 \leq 2(rank(H) - 1)(rank(K) - 1)$ (Hanna Neumann, 1957)
- Difficult: $rank(H \cap K) - 1 \leq (rank(H) - 1)(rank(K) - 1)$ (Mineyev, and also Friedman, 2012)

Applications: conjugation, finite index

- If H is a subgroup of G and $g \in G$, $g^{-1}Hg$ is also a subgroup, called a *conjugate* of H (written H^g)
- On example: H^g when g can be read, and when it cannot
- Characterization of finite index
- Nielsen-Schreier formula: if H has index n in F free of rank r, then $rank(H) - 1 = (r - 1)n$
- Decidability of the conjugacy problem

Thank you for your attention!