A Combinatorial Approach to the Word Problem for p-groups

Isaac Cheng, Karn Chutinan, and Anastasia Lee

January 10, 2025

Introduction

A Motivating Problem

- $D_8 = \langle a, b \mid a^4 = b^2 = abab = 1 \rangle$
- The **Word Problem**. Does $ba^2b^2aba^{-1} = 1$ in D_8? How about $a^7b^5a^2b^2a^3b$?

$$\begin{aligned} ba^2b^2aba^{-1} &= ba^3ba^{-1} \\ &= ba^{-1}ba^{-1} \\ &= b^{-1}a^{-1}b^{-1}a^{-1} \\ &= (abab)^{-1} \\ &= 1. \end{aligned}$$

This is too hard!

Counting Letters

- $B : D_8 \to \mathbb{Z}$ counts bs. Problem: $B(b^2) = 2$ but $B(1) = 0$, even though $b^2 = 1$ by relation.
- Fix: $B : D_8 \to \mathbb{Z}/2\mathbb{Z}$ and $A : D_8 \to \mathbb{Z}/2\mathbb{Z}$ are both well defined.
- $B(a^2b^2a) = 0$ but $A(a^2b^2a) = 1$, so $a^2b^2a \neq 1$. This is quick!

Thinking About Counting Functions

- Recall $D_8 = \langle a, b \mid a^4 = b^2 = abab = 1 \rangle$. Let $A, B : D_8 \to \mathbb{Z}/2\mathbb{Z}$ as previously defined.
- For what words w does $A(w) = B(w) = 0$?
- $A(w) = B(w) = 0$ if and only if w is commutator (i.e., w is of the form $w_1 w_2 w_1^{-1} w_2^{-1}$).
- So A, B distinguish commutators from non-commutators. Can we get more precise?
- For any two words w, w', we have $B(ww') = B(w) + B(w')$. This looks linear. What is the quadratic equivalent?

Letter Braiding Functions

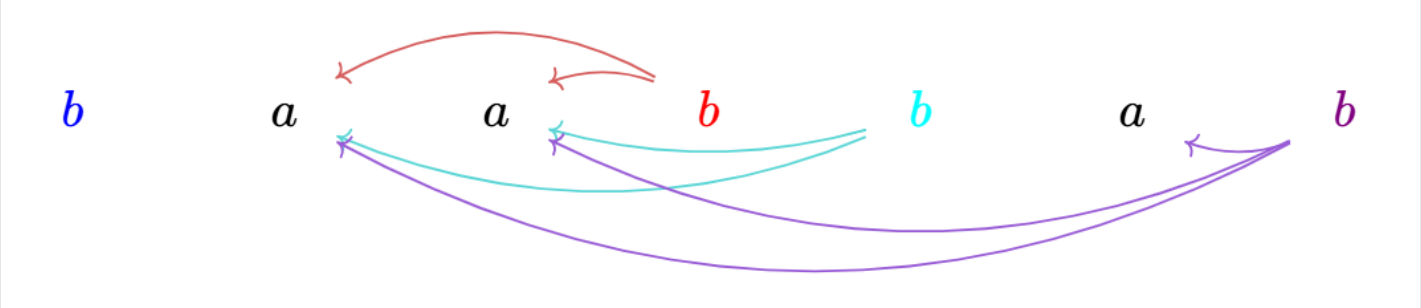
What is Letter Braiding?

Definition

Let $[\![A]\!]B$ denote the number of occurrences of some b after an a.

Example

In D_8, we have $[\![A]\!]B(ba^2b^2ab) = 7 \equiv 1 \pmod 2$.



LBFs as Quadratics

Recall: Finite Differences

Given a polynomial f, $\Delta f(x) = f(x+1) - f(x)$ is linear if and only if f is quadratic.

Definition

Given a letter braiding function b, let $\Delta_g b(w) = b(gw) - b(w)$.

Notice that $\Delta_a [\![A]\!] B = B$, so we say $[\![A]\!] B$ is degree 2.

Properties of LBFs

- Linear-time evaluation
- LBFs are well defined on a group if and only if they vanish on all relations and conjugates of relations
- Well-defined LBFs form a $\mathbb{Z}$-module with finite rank

Example

The basis of well-defined letter braiding functions in D_8 is $\{A, B, [\![A]\!]A + [\![B]\!]A, [\![A]\!]B + [\![B]\!]A\}$.

- Higher degree LBFs: For n letters $L_1, L_2, \ldots, L_n$, we similarly have $[\![\ldots [\![L_1]\!] L_2 \ldots]\!] L_n$.
- In p-groups, only need to work mod p

Solving the Word Problem for $\mathbb{Z}/2^k\mathbb{Z}$

For $k \in \mathbb{N}$, consider $\mathbb{Z}/2^k\mathbb{Z} = \langle a \mid a^{2^k} = 1 \rangle$.

Lemma

For $k \in \mathbb{N}$, w a fixed word, $\underbrace{[\![\ldots[\![A]\!]A\ldots]\!]A}_{k\ A\text{'s}}(w) = \binom{A(w)}{k}$.

Lemma

As a polynomial, $\binom{n}{2^k} \equiv 0 \pmod 2$ if and only if $n \equiv 0, 1, \ldots, 2^k - 1 \pmod{2^{k+1}}$.

Proposition

For $k \in \mathbb{N}$, the functions A, $[\![A]\!]A$, $[\![[\![[\![A]\!]A]\!]A]\!]A$, ..., $\underbrace{[\![\ldots[\![A]\!]A\ldots]\!]A}_{2^{k-1}\ A\text{'s}}$ solve the word problem for $\mathbb{Z}/2^k\mathbb{Z}$ going to $\mathbb{Z}_2$.

Intuitive Proof

Consider $\mathbb{Z}/8\mathbb{Z} = \langle a \mid a^8 = 1 \rangle$, for which the word problem is solved by the functions A, $[\![A]\!]A$, and $[\![[\![[\![A]\!]A]\!]A]\!]A$.

	A	$[\![A]\!]A$	$[\![[\![[\![A]\!]A]\!]A]\!]A$
1	0	0	0
a	1	0	0
a^2	0	1	0
a^3	1	1	0
a^4	0	0	1
a^5	1	0	1
a^6	0	1	1
a^7	1	1	1

Binary representations!

Solving the Word Problem for Finite Abelian 2-Groups

Lemma

Given finite groups G, H for which the word problem is solved, the word problem is also solved for $G \times H$.

Theorem

The word problem is solved for all finite abelian 2-groups.

Proof

By the structure theorem, any finite abelian 2-group G satisfies $G \cong (\mathbb{Z}/2^{k_1}\mathbb{Z}) \times (\mathbb{Z}/2^{k_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2^{k_n}\mathbb{Z})$. Since the word problem is solved for each of the $\mathbb{Z}/2^{k_i}\mathbb{Z}$, we have that the word problem is solved for G.

Solving the Word Problem with Augmentation Ideal Filtration

Group Rings

- Given a group G and ring R, the group ring $R[G]$ is defined to be all finite combinations of elements in G with coefficients in R.
- If $G = D_8 = \langle a, b \mid a^4 = b^2 = abab = 1 \rangle$, $R = \mathbb{Z}/2\mathbb{Z}$, some elements are $a + ab$, $b + ab + 1$.
- Functions $G \to R$ can be extended to functions $R[G] \to R$. For instance, $f(2a + b) = 2f(a) + f(b)$.
- A group ring is a free module, but also a ring, using group multiplication.

$$\begin{aligned}(a + b)(b + ab + 1) &= ab + aab + a + bb + bab + b \\ &= ab + aab + a + 1 + a^{-1} + b\end{aligned}$$

A Deeper Meaning for LBFs

- The **augmentation ideal** J of a group ring $R[G]$ is all elements of $R[G]$ whose coefficients sum to 0.
- For $G = D_8, R = \mathbb{Z}/2\mathbb{Z}$, $a + b \in J$ but $a \notin J$.
- The **augmentation ideal filtration** is the series $J \supseteq J^2 \supseteq J^3 \supseteq \ldots$. If G is a p-group and $R = \mathbb{Z}/p\mathbb{Z}$, this terminates in the zero ideal after finitely many steps.

Theorem (Gadish)

Let G be a group and R be a PID. For any i, the well-defined degree i letter braiding functions $G \to R$, extended to letter braiding functions $R[G] \to R$, are in one-to-one correspondence with the homomorphisms $J^i/J^{i+1} \to R$.

Solving the Word Problem

Theorem (Cheng, Chutinan, Lee)

Let G be a p-group and let $g \in G$. g is the identity in G if and only if $f(g) = 0$ for every well-defined letter braiding function $f : G \to \mathbb{Z}/p\mathbb{Z}$.

- Filtration terminates in finitely many steps, so only need to check finitely many degrees. LBFs of any degree have a finite basis. So only have to check on finitely many LBFs.
- Evaluating an LBF is linear time in the length of g, so checking whether g is the identity is linear time.
- **Further research:** How do we efficiently compute the bases?

Thank you!

Lemma

The word $a^7b^5a^2b^2a^3b$ is not the identity in D_8.

Proof.

The space of well-defined LBFs in D_8 is generated by $A, B, [\![A]\!]A + [\![B]\!]A$, and $[\![A]\!]B + [\![B]\!]A$. Evaluating to $\mathbb{Z}/2\mathbb{Z}$, we have $B(a^7b^5a^2b^2a^3b) = 0$, $A(a^7b^5a^2b^2a^3b) = 0$, $([\![A]\!]A + [\![B]\!]A)(a^7b^5a^2b^2a^3b) = 1$, and $([\![A]\!]B + [\![B]\!]A)(a^7b^5a^2b^2a^3b) = 0$. Since one of these is nonzero, $a^7b^5a^2b^2a^3b$ is not the identity. □

Acknowledgments

Thank you to Dev Sinha for proposing this project and mentoring us and to PROMYS for giving us this opportunity. Thank you also to Nir Gadish and Ben Walter for sharing their results with us. Lastly, thank you to John Sim, Josephine Xie, and David Fried for their supervision.