The Davenport Constant and Automorphically Equivalent Elements

(Mentors: Jim Coykendall and Jared Kettinger)

Arjun Agarwal, Rachel Chen, and Rohan Garg

Summer Workshop for Intrepid Mathematicians
SWIM 2024

8/19/2024

Title Page

Background

Let G be a finite abelian group.

Definition

A G-sequence $\{g_1, g_2, \ldots, g_n\}$ is a sequence consisting of (not necessarily distinct) elements of G.

- An example of this is the sequence $\{1, 3, 5, 3, 3\}$ in $\mathbb{Z}/6\mathbb{Z}$.

Definition

A G-sequence is a 0-sequence (alternatively zero-sequence) if $g_1 + g_2 + \cdots + g_n = 0$.

- An example if $\{1, 3, 5, 3\}$ in $\mathbb{Z}/6\mathbb{Z}$.

Definition

The G-sequence $\{g_1, g_2, \ldots, g_n\}$ has a 0-subsequence (alternatively zero-subsequence) if there exists a set $S \subseteq \{1, 2, \ldots, n\}$ such that $\sum_{i \in S} g_i = 0$.

- In $\{1, 3, 5, 3, 3\}$, some 0-subsequences are $\{1, 3, 5, 3\}$, $\{1, 5\}$, and $\{3, 3\}$.

Background

Definition

Let G be a finite abelian group. The Davenport constant, $D(G)$, of G is defined as the minimal integer n such that every G-sequence of length n has a 0-subsequence.

Definition

Let G be a finite abelian group. Then, $D(G)$ is the maximal n such that there exists a 0-sequence of length n with no proper 0-subsequences.

- The two above definitions are equivalent.

Background

Definition

We say a 0-sequence is maximal if it contains no proper 0-subsequences.

Throughout this paper, when a group G is written additively and $x \in G$, let kx denote $\underbrace{x + x + \cdots + x}_{k \text{ times}}$.

Background

Definition

Denote C_n to be the cyclic group of order n, commonly written as $\mathbb{Z}/n\mathbb{Z}$.

Theorem (Fundamental Theorem of Finite Abelian Groups)

Let G be a finite abelian group. G can be written as the product of several cyclic groups. In other words,

$$G = C_{a_1} \oplus C_{a_2} \oplus C_{a_3} \oplus \cdots \oplus C_{a_t}$$

for positive integers a_i. Furthermore, we can choose a_i in a way such that $a_{i-1} \mid a_i$ for each $2 \leq i \leq t$ and $a_i \geq 2$ for each $1 \leq i \leq t$.

When a_i are chosen in the way described, we say G is writen in its invariant factor decomposition. We say each a_i is an invariant factor and t is the rank of the group. If all a_i are powers of some prime p then we say G is a p-group. Additionally, define a_t as the exponent of the group.

Definition (Direct Summand)

Given finite abelian groups G and H we say G is a direct summand of H if there exists another finite abelian group K such that $H = G \oplus K$.

Background

Definition

Let $G \cong C_{m_1} \oplus C_{m_2} \oplus \cdots \oplus C_{m_t}$ be a finite abelian group uniquely expressed as its invariant factor decomposition. Define $D^*(G) = 1 + \sum_{i=1}^{t}(m_i - 1)$.

If $C_{m_1} \oplus C_{m_2} \oplus \cdots \oplus C_{m_t}$ is the invariant factor decomposition of G, consider the sequence consisting of the element $(1, 1, 1, \ldots 1)$ combined with $m_i - 1$ elements of ith component equal to 1 and all other components equal to 0 for all $1 \leq i \leq t$. The sequence is a maximal 0-sequence and has length $m_1 + \cdots + m_t - t + 1$, which motivates the above definition.

Background

- $D(G) \geq D^*(G)$ by the definition of $D(G)$
- A central question of the study of the Davenport constant is when $D(G) = D^*(G)$ and how far it differs for the cases where inequality is strict.

Background

Here are some known bounds of $D(G)$:

- $D(G) \leq |G|$.
- The above bound is only tight for cyclic groups. It is very weak for groups of large rank.
- $D(G) \leq \exp(G)\left(1 + \log\left(\frac{|G|}{\exp(G)}\right)\right)$.
- This is the strongest known bound for $D(G)$, attributed to Emde-Boas.
- Recall that $\exp(G)$ is the exponent of G, which is the smallest $n \in \mathbb{N}$ such that for each element g in G, $ng = 0$.

Background

Here is the list of all groups where it is known that $D(G) = D^*(G)$:

- G has rank less than or equal to 2;
- G is a p-group;
- $G \cong G_1 \oplus C_{p^k n}$, where G_1 is a p-group and $p^k \geq D^*(G_1)$;
- $G \cong C_2^3 \oplus C_{2n}$ where n is odd;
- $G \cong C_{2p^{k_1}} \oplus C_{2p^{k_2}} \oplus C_{2p^{k_3}}$ where p is prime;
- $G \cong C_2 \oplus C_{2n}^2$ with $p \nmid n$ for every prime $p \geq 11$;
- $G \cong C_3 \oplus C_3 \oplus C_{3d}$ where $d \in \mathbb{N}$;
- $G \cong C_{3 \cdot 2^t} \oplus C_{3 \cdot 2^u} \oplus C_{3 \cdot 2^v}$ where $t \geq u \geq v$;
- $G \cong C_4 \oplus C_4 \oplus C_{4d}$ where $d \in \mathbb{N}$;
- $G \cong C_6 \oplus C_6 \oplus C_{6d}$ where $d \in \mathbb{N}$.

Additional Bounds on $D(G)$

- For a group G of rank d and exponent m, $D(G) \leq |G| - m(d-2)$.
- For groups $G_1, G_2, \ldots, G_k$,

$$D(G_1 \oplus G_2 \oplus \cdots \oplus G_k) \leq D(G_1) \cdot D(G_2) \cdots D(G_k).$$

- For a group G and a subgroup $H \leq G$,

$$D(G/H) \leq D(G) \quad \text{and} \quad D(G) - D(H) + 1 \leq D(G/H),$$

where the second inequality is due to Dimitrov.

Relation Between $D(G)$ and the Structure of G

Can $D(G)$ along with other group invariants determine the structure of G?

- $D(G) = |G|$ if and only if G is cyclic.
- Can $|G|$ and $D(G)$ uniquely determine G (Answer: no).

  $G_1 \cong C_2 \oplus C_{2^2}^4 \oplus C_{2^3}$, $G_2 \cong C_2^6 \oplus C_{2^3}^2$ is a counterexample.
- What if we add rank? Can $|G|$, rank(G) and $D(G)$ uniquely determine G (Answer: no).

  $G_1 \cong C_p^p \oplus C_{p^3}^{p+2}$, $G_2 \cong C_{p^2}^{2p+1} \oplus C_{p^4}$ is a counterexample.

Relation Between $D(G)$ and the Structure of G

Question

If $D(G) > D^*(G)$, then is $D(H) > D^*(H)$ for all groups H with $G \leq H$?

- The general answer is no as seen in the following counterexample:

$$G \cong C_2^4 \oplus C_6, H \cong C_2^4 \oplus C_{2d}$$

  $D(G) > D^*(G)$ from Alfred and $D(H) = D^*(H)$ for even $d \geq 70$ from Chen and Savchev.
- We conjecture this "healing" effect can only be achieved by increasing the size of the summands in the invariant factor decomposition of G and not by increasing the rank.
- This intuition is surprising because it implies that a subgroup can be repaired by taking it into a larger group, which is more complex.

Relation Between $D(G)$ and the Structure of G

Theorem (A.-C.-Coykendall.-G.-Kettinger, 2024)

Let G be a finite abelian group with $D(G) > D^*(G)$ and $G \leq H$. Let G be a direct summand of H such that the invariant factors of G appear as invariant factors of H also. Then, $D(H) > D^*(H)$.

- $H \cong C_{a_1} \oplus C_{a_2} \oplus \cdots \oplus C_{a_t}$ where $1 < a_1 \mid a_2 \mid \cdots \mid a_t$.
- $A \subset [t]$ such that $G = \bigoplus_{i \in A} C_{a_i}$, $K = \bigoplus_{j \in [t]-A} C_{a_j}$, $D(G) > D^*(G)$.
- Proof by contradiction follows by assuming $D(H) = D^*(H)$ and constructing a sequence of length $D^*(H)$ that has no 0 subsequence.

The $D(H) \mid D(G)$ Problem

Definition

A group G satisfies Property P if for every subgroup $H \leq G$, $D(H) \mid D(G)$.

- We conjecture that only cyclic groups satisfy Property P.

Theorem (Lagrange)

If G is a group and H is a subgroup of G, then $|H| \mid |G|$.

- By Lagrange's theorem, every subgroup of a cyclic group G is cyclic and has order dividing G, so the result follows for a cyclic group.
- We first solve a weaker version of this problem, presented on the next slide.

Question

Find all groups G such that for each $H \leq G$, $D(H)D(G/H) = D(G)$.

- G satisfies the condition if and only if G is cyclic. If G is cyclic, the condition holds since H and G/H are cyclic.
- Let $G = C_{a_1} \oplus C_{a_2} \oplus \cdots \oplus C_{a_t}$ with $t \geq 2$. Consider $H = C_{a_t}$. Then

$$a_t(a_1 + a_2 + \cdots + a_{t-1} - t + 2) \leq D(H)D(G/H) = D(G),$$

but $D(G) \leq a_t(1 + \log(a_1 a_2 \cdots a_{t-1}))$, so

$$\sum_{i=1}^{t-1}(a_i - 1) \leq \sum_{i=1}^{t-1} \log(a_i).$$

Clearly $a_i - 1 > \log(a_i)$ for all a_i, so this inequality never holds.

The $D(H) \mid D(G)$ Problem

Proposition

A group G with rank equal to 2, 3, or 4 does not satisfy Property P. If G is a p-group, it does not satisfy Property P either.

- The rank 2 case follows from the fact that $D(C_a \oplus C_b) = a + b - 1$ and if $a \mid b$, then
$$a = D(C_a) \nmid a + b - 1.$$

- p-groups follow easily as the Davenport constant of every subgroup is known. It is not hard to check that
$$D(C_{a_2} \oplus C_{a_3} \oplus \cdots \oplus C_{a_k}) \nmid D(C_{a_1} \oplus C_{a_2} \oplus \cdots \oplus C_{a_k}).$$

The $D(H) \mid D(G)$ Problem

For a group $G = C_{a_1} \oplus C_{a_2} \oplus \cdots \oplus C_{a_k}$ with $k \geq 2$, consider the subgroups $C_{a_{k-1}} \oplus C_{a_k}$ and $C_{a_{k-1}}$. Clearly

$$a_{k-1} = C_{a_{k-1}} \mid D(G)$$
$$a_{k-1} + a_k - 1 = D(C_{a_{k-1}} \oplus C_{a_k}) \mid D(G).$$

Since $\gcd(a_{k-1}, a_{k-1} + a_k - 1) = 1$,

$$a_{k-1}(a_{k-1} + a_k - 1) \mid D(G).$$

The $D(H) \mid D(G)$ Problem

- Using the result from the previous slide along with the Emde-Boas bound, we conclude that

$$a_{k-1}(a_{k-1} + a_k - 1) \leq a_k \left(1 + \log(a_1 a_2 \cdots a_{k-1})\right).$$

- The inequality can be used to prove that a majority of the rank 3 and rank 4 groups do not satisfy Property P, leaving a few classes of groups that can be resolved manually or by results in papers.

The $D(H) \mid D(G)$ Problem

- The previous inequality can also be used to prove that if all the invariant factors are distinct, then G does not satisfy Property P.
- It helps to rewrite G as $C_{a_1} \oplus C_{a_1 a_2} \oplus \cdots \oplus C_{a_1 a_2 \ldots a_k}$, as the condition translates to $a_i \geq 2$ for $1 \leq i \leq k$.
- The proof inducts on the rank. It can be shown that adding another invariant factor increases the quantity on the left hand side of the inequality more than the quantity on the right hand side, which implies the inequality still does not hold.

Additional Background

Definition (Homomorphism)

Let G and H be groups. A function $\varphi : G \to H$ is a homomorphism if $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all a, b in G.

Example

A very common homomorphism is the linear map. Consider $G, H \cong \mathbb{Z}$ and the map $\varphi(x) = 2x$. Then φ is a homomorphism because

$$\varphi(a+b) = 2(a+b) = 2a + 2b = \varphi(a) + \varphi(b).$$

Definition (Isomorphism)

A bijective homomorphism φ is called an isomorphism. If such a mapping exists we say G and H are isomorphic.

Example

The group $C_2 \oplus C_3$ is isomorphic to C_6 through the following map: $\varphi((x, y)) = 3x + 2y$. This is obviously a homomorphism and can be manually verified to be bijective.

Additional Background

Definition (Automorphism)

If $\varphi : G \to G$ is an injective mapping then φ is an automorphism. The set of all such φ is called $\mathrm{Aut}(G)$ and is also a group under composition.

Example

In the group C_9 the map $\varphi : G \to G$ with $\varphi(x) = 5x$ is an automorphism since $\gcd(5, 9) = 1$.

Definition (Cosets)

If G is a group and $H \leq G$ is a subgroup of G. For all $g \in G$, the sets $g + H = \{g + h : h \in H\}$ and $H + g = \{h + g : h \in H\}$ are called the left cosets and right cosets of H. For finite abelian groups, the left and right cosets are the same. We define $(a + H) + (b + H) = (a + b) + H$ and the cosets form a group under this operation.

Example

Consider the group C_4 and its subgroup $H = \{0, 2\}$. The two cosets of H are $\{0, 2\}$ and $\{1, 3\}$.

Definition (Quotient Groups)

Let G be a finite abelian group and $H \leq G$ be a subgroup of G. The quotient group G modulo H denoted by G/H is the collection of all cosets of H.

$$G/H = \{g + H \mid g \in G\}.$$

Example

Let $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$. Then the cosets of H are

$$\{\cdots, -10, -5, 0, 5, \cdots\}$$
$$\{\cdots, -6, -1, 4, \cdots\}$$
$$\{\cdots, -7, -2, 3, \cdots\}$$
$$\{\cdots, -8, -3, 2, \cdots\}$$
$$\{\cdots, -9, -4, 1, \cdots\}.$$

This quotient group $\mathbb{Z}/5\mathbb{Z}$ is isomorphic to C_5.

The Inverse Davenport Problem

- The inverse Davenport problem is the study of the structure of maximal 0-sequences of length $D(G)$. Let $\{x_i\}_{1 \le i \le D(G)}$ and $\{y_i\}_{1 \le i \le D(G)}$ be two maximal 0-sequences of length $D(G)$. We investigate the following equivalence classes of sequences.
- (Condition 1) $\{x_i\} \sim \{y_i\}$ if there exists a $\varphi \in \mathrm{Aut}(G)$ and a permutation σ of $1, 2, \ldots, D(G)$ such that $\varphi(x_i) = y_{\sigma(i)}$ for each $1 \le i \le D(G)$.
- (Condition 2) $\{x_i\} \approx \{y_i\}$ if there exists a permutation σ of $1, 2, \ldots, D(G)$ and $D(G)$ automorphisms, call them $\varphi_1, \varphi_2, \ldots, \varphi_{D(G)}$, such that $\varphi_i(x_i) = y_{\sigma(i)}$.
- (Condition 3) $\{x_i\} \approxeq \{y_i\}$ if there exists a permutation σ of $1, 2, \ldots, D(G)$ such that $|x_i| = |y_{\sigma(i)}|$ for each $1 \le i \le D(G)$.
- $\{x_i\} \sim \{y_i\} \implies \{x_i\} \approx \{y_i\} \implies \{x_i\} \approxeq \{y_i\}$.

The Inverse Davenport Problem

Question

If $\{x_i\}$ and $\{y_i\}$ are two maximal 0-sequences of length $D(G)$, is $\{x_i\} \sim \{y_i\}$?

- No. For example, consider $G \cong C_2 \oplus C_6$ with $D(G) = 2 + 6 - 1 = 7$. Consider maximal 0 sequences:

$$\{x_i\} = \{(0,1),(0,1),(0,1),(0,1),(0,1),(1,0),(1,1)\}.$$

$$\{y_i\} = \{(0,1),(0,1),(0,1),(1,1),(1,1),(1,1),(1,0)\}.$$

The element $(0,1)$ appears fives times in $\{x_i\}$ and there is no element of $\{y_i\}$ appearing five times. Therefore, $\{x_i\} \not\sim \{y_i\}$.

The Inverse Davenport Problem

Question

Can the equivalence relation for two maximal 0-sequences be relaxed? If $\{x_i\}$ and $\{y_i\}$ are two maximal 0-sequences of length $D(G)$, is $\{x_i\} \approx \{y_i\}$ or $\{x_i\} \approxeq \{y_i\}$?

- No. Consider this counterexample $G \cong C_2 \oplus C_2 \oplus C_4$ with $D(G) = 6$.

$$\{x_i\} = \{(1,1,1),(1,0,0),(0,1,0),(0,0,1),(0,0,1),(0,0,1)\}.$$

$$\{y_i\} = \{(0,0,1),(0,0,1),(0,0,1),(1,0,1),(0,1,1),(1,1,3)\}.$$

where the order of the elements in the sequences are 4, 2, 2, 4, 4, 4, and 4, 4, 4, 4, 4, 4, respectively. Therefore, $\{x_i\} \not\approx \{y_i\}$ and $\{x_i\} \not\approxeq \{y_i\}$.

The Inverse Davenport Problem

Question

When do maximal 0-sequences satisfy the equivalence conditions 1, 2, or 3?

- A condition on when two elements of finite abelian groups are automorphic images of each other would be helpful to answer this question.

Condition for Automorphic Equivalence of Two Elements

Let G be a finite abelian group with $x, y \in G$.

- We say x and y satisfy Condition A if $G/\langle x \rangle \cong G/\langle y \rangle$.
- We say x and y satisfy Condition B if for all $k \in \mathbb{N}$, x has k^{th} root (exists x' where $kx' = x$) if and only if y also has a k^{th} root; furthermore, $|x|$ must equal to $|y|$.
- We say x and y satisfy Condition C if there exists $\varphi \in \text{Aut}(G)$ such that $\varphi(x) = y$.

Automorphic Equivalence of Two Elements: Exploring A and B

First, we explore whether Condition A and Condition B are equivalent.

- It is well-known that for a finite abelian group G and $x \in G$, $G/\langle x \rangle$ can be computed with Smith Normal Form.
- This is often given in terms of finitely generated modules over a principal ideal domain.

Automorphic Equivalence of Two Elements: Exploring A and B

Let $G \cong C_{m_1} \oplus C_{m_2} \oplus \cdots \oplus C_{m_k}$ and $x = (x_1, x_2, \ldots, x_k)$. Then, $G/\langle x \rangle$ can be computed by writing the matrix

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_k \\ m_1 & & & \\ & m_2 & & \\ & & \ddots & \\ & & & m_k \end{bmatrix}$$

in Smith Normal Form.

Automorphic Equivalence of Two Elements: Exploring A and B

We apply the Smith Normal Form algorithm from Artin's Algebra to compute $G/\langle x \rangle$ where $G \cong C_4 \oplus C_4 \oplus C_8 \oplus C_8$ and $x = (2, 1, 2, 4)$:

$$\begin{bmatrix} 2 & 1 & 2 & 4 \\ 4 & & & \\ & 4 & & \\ & & 8 & \\ & & & 8 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & & & \\ & 4 & & \\ & 8 & 8 & 16 \\ & & 8 & \\ & & & 8 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & & & \\ & 4 & & \\ & & 8 & \\ & & & 16 \\ & & & 8 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & & & \\ & 4 & & \\ & & 8 & \\ & & & 8 \\ & & & \end{bmatrix}.$$

Thus, the quotient group is $C_4 \oplus C_8 \oplus C_8$.

Automorphic Equivalence of Two Elements: Exploring A and B

Looking at p-groups is sufficient.

- All three conditions are true if and only if they are true for each p-group component of G.

Now, we describe an "easier" algorithm to compute Smith Normal Form in p-groups, where we do Smith Normal Form in terms of ν_p. We define $\nu_p(n)$ to be the largest non-negative integer k such that $p^k \mid n$ where p is prime and n is a positive integer.

Automorphic Equivalence of Two Elements: Exploring A and B

- Suppose that $G \cong C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e^k}}$ and $x = (a_1 p^{f_1}, a_2 p^{f_2}, \ldots, a_k p^{f_k})$ where $p \nmid a_i$ if $a_i \neq 0$ for $1 \leq i \leq k$.
- If any of the a_i are equal to 0, we can simply remove the zero and remove the component of G that a_i is in.
- For example, if $x = (0, a_2 p^{f_2}, \ldots, a_k p^{f_k})$, we only need to consider $x = (a_2 p^{f_2}, \ldots, a_k p^{f_k})$ and $G \cong C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e^k}}$, and the result is $C_{p^{e_1}} \oplus (C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e^k}})/\langle (a_2 p^{f_2}, \ldots, a_k p^{f_k}) \rangle$.

Therefore, assume $a_i \neq 0$ for all i.

Automorphic Equivalence of Two Elements: Exploring A and B

- Without loss of generality, let $f_1 \leq f_2 \leq \cdots \leq f_k$ (so the invariant factors of G do not need to be from least to greatest).
- Since Condition A and Condition B are both preserved under automorphism, we only need to consider $x = (p^{f_1}, p^{f_2}, \ldots, p^{f_k})$ since it is an automorphic image of $(a_1 p^{f_1}, a_2 p^{f_2}, \ldots, a_k p^{f_k})$.

Automorphic Equivalence of Two Elements: Exploring A and B

First, we write down the following list:

$$\begin{array}{cccc} f_1 & f_2 & \dots & f_k \\ e_1 & e_2 & \dots & e_k \end{array}$$

Let a_{mn} denote the element of that list in the mth row and the nth column.

- For each $1 \leq i \leq k-1$, add $\max(0, a_{2i} - a_{1i})$ to all a_{1j} where $i+1 \leq j \leq k$ and then erase the larger one among a_{2i} and a_{1i}.
- Erase the larger one among a_{2k} and a_{1k}.
- There should be one value left per column, which are the powers of the invariant factors of the quotient group.

Automorphic Equivalence of Two Elements: Exploring A and B

As an example, we compute the above $(C_4 \oplus C_4 \oplus C_8 \oplus C_8)/\langle(2,1,2,4)\rangle$.

- Here, $f_1 = 0$, $f_2 = f_3 = 1$, $f_4 = 2$, $e_1 = 2$ (because the component with power 0 is in C_{2^2}, not because the first invariant factor of G is C_{2^2}), $e_2 = 2$, $e_3 = e_4 = 3$. Our list is

$$\begin{matrix} 0 & 1 & 1 & 2 \\ 2 & 2 & 3 & 3 \end{matrix}.$$

Running the algorithm,

$$\begin{matrix} 0 & 3 & 3 & 4 \\ & 2 & 3 & 3 \end{matrix} \to \begin{matrix} 0 & & 3 & 4 \\ & 2 & 3 & 3 \end{matrix} \to \begin{matrix} 0 & & & 3 & 4 \\ & 2 & & & 3 \end{matrix} \to \begin{matrix} 0 & & & 3 \\ & 2 & & & 3 \end{matrix}$$

so the quotient group is $C_{2^2} \oplus C_{2^3} \oplus C_{2^3}$.

Automorphic Equivalence of Two Elements: Exploring A and B

Lemma

If G is a finite abelian group, every element $x \in G$ has a k^{th} root if $\gcd(k, |G|) = 1$.

Theorem

Condition A implies Condition B.

- In a p-group, an element x has a k^{th} root if and only if it has a $p^{\nu_p(k)}$th root.
- Let $n = \nu_p(k)$. Then, x has a k^{th} root if and only if all f_i (as defined above) are greater than or equal to n.
- Just run the algorithm.

Automorphic Equivalence of Two Elements: Exploring A and B

From just running the algorithm, we also get that Condition B implies Condition A for groups of rank 2.

- Does Condition B imply Condition A in general?
- The answer to this question is no, which is motivated by our Smith Normal Form algorithm.
- Condition B only states that the term in the first column in the lists for both x and y after the algorithm is complete is equal, and the sum of the elements in the lists after the algorithm is complete are equal.
- We use this as our motivation to find a counterexample.

Automorphic Equivalence of Two Elements: Exploring A and B

Consider $G \cong C_8 \oplus C_{16} \oplus C_{32}$, $x = (2, 4, 4)$ and $y = (2, 2, 16)$. We can run our algorithm to show that

$$(C_8 \oplus C_{16} \oplus C_{32})/\langle(2, 4, 4)\rangle \cong C_2 \oplus C_{16} \oplus C_{16}$$

and

$$(C_8 \oplus C_{16} \oplus C_{32})/\langle(2, 2, 16)\rangle \cong C_2 \oplus C_8 \oplus C_{32}.$$

However, both x and y have k^{th} roots if and only if $\nu_2(k) \leq 1$.

Automorphic Equivalence of Two Elements: Exploring A and C

Question

Does Condition A imply Condition C? i.e., Does $G/\langle x \rangle \cong G/\langle y \rangle$ imply there exists φ in $\mathrm{Aut}(G)$ such that $\varphi(x) = y$?

Automorphic Equivalence of Two Elements: Exploring A and C

- If H and K are finite abelian groups with relatively prime orders, $\mathrm{Aut}(H) \oplus \mathrm{Aut}(K) \cong \mathrm{Aut}(H \oplus K)$ (Hillar).
- Any finite abelian group is isomorphic to a product of p-groups. $G \cong \bigoplus_{i=1}^{n} H_{p_i}$, where the p_i are distinct primes.
- $x = (x_{p_1}, x_{p_2}, \ldots, x_{p_n})$ where $x_{p_i} \in H_{p_i}$.
- $y = (y_{p_1}, y_{p_2}, \ldots, y_{p_n})$ where $y_{p_i} \in H_{p_i}$.
- We can prove $G/\langle x \rangle \cong G/\langle y \rangle \Leftrightarrow H_{p_i}/\langle (x_{p_i}) \rangle \cong H_{p_i}/\langle (y_{p_i}) \rangle$ for all $1 \leq i \leq n$.
- Therefore, it suffices to prove the theorem for p-groups.

Automorphic Equivalence of Two Elements: Exploring A and C

- Let $G \cong \bigoplus_{i=1}^{n} C_{p^{e_i}}$ for some prime p.
- Since $\langle x \rangle$ and $\langle y \rangle$ are cyclic and $G/\langle x \rangle \cong G/\langle y \rangle$, there exists φ_1 in $\mathrm{Aut}(G)$ that maps the elements of $\langle x \rangle$ to the elements of $\langle y \rangle$ (Buzasí).
- Therefore, $\varphi_1(x) = ky$ for some $k \in \mathbb{N}$.
- Since φ_1 preserves orders we can prove $\gcd(k, p) = 1$ and k^{-1} exists modulo p^m for all $m \in \mathbb{N}$. Therefore for every p^{e_i}, there exists some $a_i \in \mathbb{N}$ such that $a_i k \equiv 1 \pmod{p^{e_i}}$.
- Consider $x = (x_1, x_2, \ldots, x_n)$. Then $\varphi_2 : G \to G$ with $\varphi_2(x) = (a_1 x_1, \ldots, a_n x_n)$ can be shown to be in $\mathrm{Aut}(G)$.
- Therefore, $\varphi_2 \circ \varphi_1 \in \mathrm{Aut}(G)$ with $(\varphi_2 \circ \varphi_1)(x) = y$.

Automorphic Equivalence of Two Elements: Exploring A and C

Question

Does Condition C imply Condition A. i.e., if φ in $\mathrm{Aut}(G)$ such that $\varphi(x) = y$ do we have $G/\langle x \rangle \cong G/\langle y \rangle$?

Automorphic Equivalence of Two Elements: Exploring A and C

- Let $X = \langle x \rangle$, $Y = \langle y \rangle$.
- Define $\psi : a + X \mapsto \varphi(a) + Y$ for all $a \in G$.
- If $a, b \in G$ such that a, b are in same coset of X then we can show ψ is well defined. i.e., $\psi(a + X) = \psi(b + X)$.
- Surjectivity of ψ follows from the surjectivity of φ. Injectivity follows from $|G/\langle x \rangle| = |G/\langle y \rangle|$.
- $\psi(a + X) + \psi(b + X) = \varphi(a + b) + X = \psi((a + X) + (b + X))$. Therefore ψ is a homomorphism.
- Therefore ψ is an isomorphism and $G/\langle x \rangle \cong G/\langle y \rangle$.

Condition for Automorphic Equivalence of Two Elements: Our Main Result

To conclude,

Theorem (A.-C.-Coykendall.-G.-Kettinger, 2024)

In a finite abelian group G, there exists an automorphism φ such that $\varphi(x) = y$ if and only if $G/\langle x \rangle \cong G/\langle y \rangle$.

Automorphic Equivalence of Two Elements: Significance of Results

This result can also be combined with other results to produce corollaries.

Theorem (A.-C.-Coykendall.-G.-Kettinger, 2024)

If x and y are both of maximal order in G, they are automorphic images of each other.

Corollary (A.-C.-Coykendall.-G.-Kettinger, 2024)

Given two elements x, $y \in G$ of maximal order, $G/\langle x \rangle \cong G/\langle y \rangle$.

Automorphic Equivalence of Two Elements: Significance of Results

How can we efficiently determine if two elements are automorphic images of each other?

- No known algorithm for this task exists in finite abelian groups.
- Our theorem combined with SNF manipulation to check if $G/\langle x \rangle \cong G/\langle y \rangle$ gives a faster way to determine this.
- By Storjohann, the time complexity to compute SNF for integer matrices in $\mathbb{Z}(n \times m)$ is $O(n^{\theta-1} mM(n \log(||A||)))$ where $||A|| = \max\{A(i,j) \mid 1 \leq i,j \leq n\}$, $M(t)$ bounds the cost of multiplying two t-bit integers and θ is the exponent for multiplication of two $n \times n$ matrices.
- The theoretical best complexity for $n \times n$ matrix multiplication by Coppersmith and Winograd gives $\theta = 2.37$ resulting in an $O(n^{2.37})$ algorithm.
- However this matrix multiplication algorithm has impractically high constant factors.

Automorphic Equivalence of Two Elements: Significance of Results

- Naive brute force algorithm will take $O(|G|^n)$.
- Our theorem combined with SNF manipulation to check if $G/\langle x \rangle \cong G/\langle y \rangle$ gives a faster way to determine this.
- Combining best known practical algorithms for computing SNF with Strassen's matrix multiplication algorithm, we get a time complexity of $O(n^{2.8074})$ where $n = \text{rank}(G)$.
- Comparing time complexity.

Rank	1	2	3	4	5	6	7	8	9
Our algorithm	10^0	10^1	10^2	10^2	10^2	10^3	10^3	10^3	10^3
Brute force algorithm	10^0	10^1	10^3	10^4	10^7	10^{10}	10^{14}	10^{19}	10^{24}

- This represents a significant speed up over naive brute force methods.

Acknowledgements

We would like to give our heartfelt gratitude to our amazing mentors Professor Coykendall and Jared Kettinger for their support and insights during the entire research process. We also kindly thank Dr. Felix Gotti and the PRIMES-USA research program for giving us this amazing opportunity to learn and conduct research.

References I

[1] Alford, W., Granville, A., & Pomerance, C. (1994). There are infinitely many Carmichael numbers. *Annals of Mathematics*, 140(3), 703–722.

[2] Artin, M. (1955). *Algebra*. Prentice Hall. ISBN 978-0132413770.

[3] Anderson, D., & Anderson, D. (1992). Elasticity of factorizations in integral domains. *Journal of Pure and Applied Algebra*, 80(3), 217–235.

[4] Buzasi, K. (1981). Invariants of pairs of finite abelian groups. *Publ. Math. Debrecen*, 28(3-4), 317–326. (Russian).

[5] Chen, F., & Savchev, S. (2014). Long minimal zero-sum sequences in the groups $C_2^{r-1} \oplus C_{2k}$. *Integers*, 14, Paper No. A23, 29.

[6] Coppersmith, D., & Winograd, S. (1990). Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3), 251–280.

[7] Delorme, C., Ordaz, O., & Quiroz, D. (2001). Some remarks on Davenport constant. *Discrete Mathematics*, 237, 119–128.

[8] Dimitrov, V. (2004). On the strong Davenport constant of nonabelian finite p-groups. *Math. Balkanica (N.S.)*, 18, 131–140.

References II

[9] Gao, W., Geroldinger, A., & Grynkiewicz, D. (2008). Inverse zero-sum problems III. *arXiv:0801.3792*.

[10] Geroldinger, A., & Schneider, R. (1992). On Davenport's constant. *Journal of Combinatorial Theory, Series A*, 61, 147–152.

[11] Hillar, J., & Rhea, D. L. (2006). Automorphisms of finite abelian groups. *arXiv:math/0605185v1*.

[12] Olson, J. (1969). A combinatorial problem on finite abelian groups, I. *Journal of Number Theory*, 1, 8–10.

[13] Olson, J. (1969). A combinatorial problem on finite abelian groups, II. *Journal of Number Theory*, 1, 195–199.

[14] Rogers, K. (1963). A combinatorial problem in abelian groups. *Proceedings of the Cambridge Philosophical Society*, 59, 559–562.

[15] Schmid, W. (2008). Inverse zero-sum problems II. *arXiv:0801.3747*.

[16] Sheikh, A. (2017). The Davenport constant of finite abelian groups. *Royal Holloway, University of London*.

References III

[17] Steffan, J. (1986). Longueurs des décompositions en produits d'éléments irréductibles dans un anneau de Dedekind. *Journal of Algebra*, 102(1), 229–236.

[18] Storjohann, A. (1996). Near optimal algorithms for computing Smith normal forms of integer matrices. *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation.* ISSAC '96, 267–274.

[19] Strassen, V. (1969). Gaussian elimination is not optimal. *Numerische Mathematik, 13*(4), 354-356. https://doi.org/10.1007/BF02165411

[20] van Emde Boas, P. (1969). A combinatorial problem on finite abelian groups, I. *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1969(ZW:007), 60.

[21] van Emde Boas, P. (1969). A combinatorial problem on finite abelian groups, II. *Math. Centrum Amsterdam Afd. Zuivere Wisk.*, 1969(ZW:007), 60.

[22] van Emde Boas, P., & Kruyswijk, D. (1969). A combinatorial problem on finite abelian groups III. *Stichting Mathematisch Centrum. Afd. Zuivere Wiskunde*.