Sublinear Time Algorithms for Abelian Group Property Testing

Nader H. Bshouty
Technion, Haifa, Israel

Abstract

In this paper, we study the problems of abelian group property testing in two models. In the *partially specified model* (PS-model), the algorithm does not know the group size but can access randomly chosen elements of the group, along with the Cayley table of these elements, which provides the result of the binary operation for every pair of selected elements. In the stronger *fully specified model* (FS-model), the algorithm knows the size of the group and has access to all its elements and the Cayley table.

In property testing of abelian group property, given a finite set G and oracle access to a binary operation $*: G^2 \to G$, we aim to distinguish whether $(G, *)$ is an abelian group or is ϵ-far from any abelian group over G.

Using a novel approach, we present a tester in the PS-model (and consequently in the FS-model) that runs in time $\tilde{O}(\sqrt{|G|} + 1/\epsilon)$, improving upon the Goldreich-Tauber tester, which runs in time $O(|G|/\epsilon)$. Additionally, our tester improves another tester by Goldreich and Tauber that runs in time $O(|G|^2)$ and makes $\tilde{O}(|G| + 1/\epsilon)$ queries.

We further extend our result to testing subclasses of abelian groups $\mathcal{G}$ that are closed under isomorphism. Specifically, if one can decide in time T whether an abelian group of the form $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ belongs to $\mathcal{G}$, then there exists a tester for $\mathcal{G}$ that runs in time $T + \tilde{O}(\sqrt{|G|} + 1/\epsilon)$ and makes $O(\sqrt{|G|} + 1/\epsilon)$ queries. This result gives testers that run in time $O(\sqrt{|G|} + 1/\epsilon)$ for subclasses such as abelian groups of rank at most k, abelian p-groups, and vector spaces over $\mathbb{Z}_p$.

We then present two subclasses, $\mathcal{G}_1$ and $\mathcal{G}_2$, of abelian groups that are closed under isomorphism for which any tester for $\mathcal{G}_1$ in the FS-model must run in time $\Omega(|G|^{1/4} + 1/\epsilon)$, and any tester for $\mathcal{G}_2$ in the PS-model must run in time $\Omega(\sqrt{|G|} + 1/\epsilon)$, showing that our approach provides tight bounds for certain subclasses of abelian groups.

2012 ACM Subject Classification Theory of computation

Keywords and phrases Property testing, Abelian group

Digital Object Identifier 10.4230/LIPIcs.MFCS.2026.89

1 Introduction

Given the $|G| \times |G|$ multiplication table of a set G. Consider the task of deciding whether it represents the Cayley table of an Abelian group. Any algorithm must inspect every entry of the table, implying a lower bound of $\Omega(|G|^2)$. Evra et al. [6] gave an $O(|G|^2)$-time algorithm.

In this paper, we consider the *property-testing* version of the problem: given query access to the table, determine whether it is the Cayley table of an Abelian group, or is far from any such table. We show that this can be done in time $O(\sqrt{|G|})$, even when the size of the table is unknown, and the elements of G are provided in a random order.

Property testing of sets of objects was first considered in the seminal works of Blum, Luby, and Rubinfeld [2] and Rubinfeld and Sudan [19]. It has since become a very active area of research; see, for example, the surveys and books [4, 10, 11, 17, 18].

In this paper, we study the problem of testing abelian groups: Given a finite set G and oracle access to a multiplication table $*: G^2 \to G$, a tester aims to distinguish whether $(G, *)$ is an abelian group or is ϵ-far from any abelian group over G; that is, for every abelian group $(G, \cdot)$, we have

$$|\{(x, y) | x * y \neq x \cdot y\}| \geq \epsilon |G|^2.$$

This is known as the *Hamming distance*. The *edit distance* has also been considered in the literature [8, 9].

In this paper, we study the problems of abelian group property testing in two models. In the *fully specified model* (FS-model), the size of the groups is known, and the algorithm has access to the group's elements and their Cayley table. In the *partially specified model* (PS-model), the size of the group is unknown; the algorithm can receive uniform random elements of the group and access the Cayley table of elements observed so far.

In the FS-model, Ergün et al. [5] presented a tester for groups that runs in time $\tilde{O}(|G|^{3/2}/\epsilon)$. Goldreich and Tauber [12] presented a tester for groups and abelian groups that runs in time $\tilde{O}(|G|/\epsilon)$ and makes $\tilde{O}(|G|/\epsilon)$ queries. They also provided another tester that runs in time $\tilde{O}(|G|^2)$ and makes $\tilde{O}(|G| + 1/\epsilon)$ queries.

In this paper, we give the first sublinear-time algorithm (in the size of the group).

▶ **Theorem 1.** *There exists a tester for abelian groups in the PS-model (and therefore in the FS-model) that runs in time*

$$\tilde{O}(\sqrt{|G|} + 1/\epsilon).$$

This is the first sublinear-time tester for the abelian groups.

We then extend this result to testing any subclass of abelian groups that is closed under isomorphism. In the PS-model, we prove the following.

▶ **Theorem 2.** *Let $\mathcal{G}$ be a subclass of abelian groups that is closed under isomorphism. If there exists an algorithm that can determine, in time T, whether any abelian group of the form $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ belongs to $\mathcal{G}$, then there exists a tester for $\mathcal{G}$ in the PS-model that runs in time $T + \tilde{O}(\sqrt{|G|} + 1/\epsilon)$ and makes $\tilde{O}(\sqrt{|G|} + 1/\epsilon)$ queries.*

In particular, there exist testers that run in time $\tilde{O}(\sqrt{|G|} + 1/\epsilon)$ for the classes: abelian groups of rank at most [1] k, abelian p-groups, vector spaces over $\mathbb{Z}_p$ and cyclic groups.

For cyclic groups in the FS-model, Gall and Yoshida [9] gave a tester that runs in time $poly(\log |G|)/\epsilon$. In the PS-model, they gave a lower bound of $\Omega(|G|^{1/6})$ for testing cyclic groups and linear space over $\mathbb{Z}_p$.

Two lower bounds are known for the number of queries in the FS-model. Goldreich and Tauber [12] gave the lower bound $\Omega(\log |G|)$ for testing any subclass of groups $\mathcal{G}$ that is closed under isomorphism and contains all the cyclic groups of prime order. Le Gall and Yoshida [9] gave a lower bound $\Omega(|G|^{1/6-4/(6(3k+1))})$ for testing the class of abelian groups of rank at most k.

In this paper, we prove the following lower bound.

▶ **Theorem 3.** *There exists a subclass $\mathcal{G}$ of abelian groups that is closed under isomorphism, for which any tester for $\mathcal{G}$ in the FS-model with $\epsilon < 1/4$ must make at least $\Omega(|G|^{1/4})$ queries.*

Additionally, we establish the following tight lower bound.

▶ **Theorem 4.** *There exists a subclass $\mathcal{G}$ of abelian groups that is closed under isomorphism, for which any tester for $\mathcal{G}$ in the PS-model with $\epsilon < 1/4$ must make at least $\Omega(\sqrt{|G|})$ queries.*

[1] A group G is abelian of rank at most k if is isomorphic to $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$ where $s \in [k]$ and $m_i \in \mathbb{N}$. It can also be defined as the minimal number of generators required to generate the group.

The paper is organized as follows: In Section 2, we introduce the techniques used to prove both upper and lower bounds. Section 3 presents preliminary results. In Section 4, we describe the one-sided error tester, followed by the two-sided error tester in Section 5. Section 6 extends our results to testers for any subclass of abelian groups that is closed under isomorphism. Finally, in Section 7, we establish the lower bounds.

2 Our Technique

Our approach is novel and does not rely on testing the associativity, commutativity, and cancellativity of $(G,*)$, as previous methods have done [5, 12, 15, 16].

Given a finite *magma* $(G,*)$ – a finite set G with a binary operation $*: G\times G\to G$ – we begin by running the algorithm from [3] that constructs generators for $(G,*)$ with triangular relations[2]. This algorithm runs in time $\tilde{O}(\sqrt{|G|})$. If the algorithm fails, we reject. If it successfully returns a set of generators with triangular relations, denoted as $\mathcal{R}$, we use these relations to construct an abelian group $(\Gamma(\mathcal{R}),\cdot)$ that satisfies those relations.

The key results ensuring the correctness of our approach are as follows:

1. If $(G,*)$ is an abelian group, then it is isomorphic to $\Gamma(\mathcal{R})$ via an isomorphism $\Psi: \Gamma(\mathcal{R})\to G$.
2. For every $x\in\Gamma(\mathcal{R})$, $\Psi(x)$ can be computed in time $poly(\log|G|)$.
3. Both multiplication and inversion in $\Gamma(\mathcal{R})$ can be computed in time $poly(\log|G|)$.

Before presenting our primary tester, we first introduce a simple tester that runs in time $\tilde{O}(|G|+1/\epsilon)$. The main idea is to construct, in time $\tilde{O}(|G|)$, a table of the isomorphic values $\Psi:\Gamma(\mathcal{R})\to G$. Once this table is constructed, we check whether Ψ is a bijective map. If not, then we reject.

If Ψ is bijective, we then, choose $O(1/\epsilon)$ pairs $(x,y)\in\Gamma(\mathcal{R})^2$ uniformly at random and verify whether $\Psi(x\cdot y)=\Psi(x)*\Psi(y)$.

We then prove that this algorithm provides a tester that runs in time $\tilde{O}(|G|+1/\epsilon)$.

To achieve an improved time complexity of $\tilde{O}(\sqrt{|G|}+1/\epsilon)$, we avoid constructing the entire table of Ψ and, therefore, cannot directly verify whether Ψ is bijective. Instead, we first check whether Ψ is $\Theta(1)$-close to a bijective map and then verify whether $\Psi(x\cdot y)=\Psi(x)*\Psi(y)$. The first step requires $O(\sqrt{|G|})$ queries, and the second step requires $O(1/\epsilon)$ queries.

Although this two-step approach may not be universally applicable, we show that it holds for abelian groups due to their specific algebraic structure.

For testing subclasses $\mathcal{G}$ of abelian groups that are closed under isomorphism, we use the same tester and add a verification procedure to check that $\Gamma(\mathcal{R})$ belongs to $\mathcal{G}$.

The lower bound results follow directly from Theorems 7 and 8 in [3]. Theorem 6 establishes a lower bound of $\Omega(|G|^{1/4})$ on the number of queries required by any algorithm in the FS-model to distinguish between groups $\mathcal{G}$ that are isomorphic to either $H_1=\mathbb{Z}_{p^2}^m$ or $H_2=\mathbb{Z}_{p^2}^{m-1}\times\mathbb{Z}_p^2$. Theorem 7 establishes the lower bound $\Omega(\sqrt{|G|})$ on the number of queries required by any algorithm in the PS-model to distinguish between abelian groups $\mathcal{G}$ that are isomorphic to either $G_1=\mathbb{Z}_p^m$ or $G_2=\mathbb{Z}_p^{m-1}$.

2.1 One-sided vs. Two-sided Error Tester

A tester is called a *one-sided error tester* if it accepts with probability 1 when $(G,*)$ is an abelian group.

[2] A set of generators $\{a_1,a_2,\ldots,a_t\}$ of a group G has a *triangular relations* if, for each $i\in[t]$, there exists a relation that depends on $a_1,\ldots,a_i$.

Our algorithm that identifies generators of G is randomized. Therefore, there is a nonzero probability that the tester may fail even when $(G, *)$ is an abelian group. As a result, our tester is a *two-sided error* tester.

In [3], Bshouty also gives a deterministic algorithm that identifies generators with triangular relations for $(G, *)$ in time $O(|G|)$. Using this algorithm, we obtain a one-sided tester that runs in time $\tilde{O}(|G| + 1/\epsilon)$, improving upon the one-sided tester of Goldreich and Tauber, which runs in time $O(|G|/\epsilon)$.

We further extend the result to testing subclasses of abelian groups that are closed under isomorphism. Specifically, for any subclass of abelian group $\mathcal{G}$, if there exists an algorithm that can determine in time T whether an abelian group of the form $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ belongs to $\mathcal{G}$, then there exists a one-sided error tester for $\mathcal{G}$ that runs in time $T + \tilde{O}(|G| + 1/\epsilon)$ and makes $O(|G| + 1/\epsilon)$ queries.

This gives one-sided error testers that run in time $O(|G| + 1/\epsilon)$ for the subclasses such as abelian groups of rank at most k, abelian p-groups and vector spaces over $\mathbb{Z}_p$.

3 Abelian Groups and Preliminary Results

In this section, we provide definitions and preliminary results that will be used to prove the main results.

3.1 Basic Facts in Groups

Let $(G, \cdot)$ be an abelian (commutative) group, and let e be its identity element. For a nonempty subset A of G, we define $\langle A \rangle := \{a_1 \cdots a_k | a_i \in A, k \in \mathbb{N}\}$ as the subgroup *generated* by A. If $\langle A \rangle = G$, we say that A is a *set of generators* of G.

A *relation* among elements of a group describes an equation that holds between those elements, typically reflecting how generators interact to define the group's structure. We say that a set of generators $A = \{a_1, \ldots, a_m\}$ of a group G satisfies a *triangular relation* if, for every i, there exists a relation that depends on a_i and some elements in $\{a_1, a_2, \ldots, a_{i-1}\}$. For example, if $A = \{a, b, c\}$ then $a^5 = e$, $b^3 = a^2$ and $c^7 = ab^2$ are triangular relations[3].

It is well known that every finite abelian group G is isomorphic to a direct product of cyclic groups $G_1 \times G_2 \times \cdots \times G_t$, where each G_i is a cyclic group of order $m_j \geq 2$. If a_i generates the cyclic group G_i, $i = 1, 2, \ldots, t$, i.e., $G_i = \langle a_i \rangle$, then the elements $a_1, a_2, \ldots, a_t$ are called a *basis* of G. Since each $\langle a_i \rangle$ is isomorphic to $\mathbb{Z}_{m_i}$ for $m_i = |\langle a_i \rangle|$, it follows that G is isomorphic to $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$.

The following lemma is straightforward to prove.

▶ **Lemma 5.** *Let $(G, \cdot)$ be a group, and A be any set such that $|A| = |G|$. Let $\Pi : G \to A$ be a bijective function. Then $(A, \circ)$, where the operation $\circ$ is defined as $a \circ b = \Pi(\Pi^{-1}(a) \cdot \Pi^{-1}(b))$ is a group that is isomorphic to $(G, \cdot)$.*

3.2 The Monomial Abelian Group

Let $n \in \mathbb{N}$, $n \geq 2$, and $K = (\kappa_1, \ldots, \kappa_t) \in \mathbb{N}^t$ such that $\kappa_i \geq 2$ and $\kappa_1 \kappa_2 \cdots \kappa_t = n$. Let $0 \leq \ell_{i,j} \leq \kappa_j - 1$ for $i = 2, \ldots, t$ and $j = 1, \ldots, i-1$, and define $L = (\ell_{i,j})$. We define

$$\Gamma(K, L) = \langle x_1, x_2, \ldots, x_t \mid x_i^{\kappa_i} = x_1^{\ell_{i,1}} \cdots x_{i-1}^{\ell_{i,i-1}}, i = 2, \ldots, t \ ; \ x_1^{\kappa_1} = 1 \rangle$$

[3] The name "triangular relations" originates from triangular matrices, where – using + and 0 instead of $\cdot$ and e in an abelian group – such relations can be expressed as a triangular matrix multiplied by a vector of the element in A equal to the zero vector.

as the set of all monomials over the variables $x_1, x_2, \ldots, x_t$ of the form $x_1^{j_1} x_2^{j_2} \cdots x_t^{j_t}$, where $0 \le j_i \le \kappa_i - 1$ for all $i \in [t]$, with multiplication modulo $x_i^{\kappa_i} - x_1^{\ell_{i,1}} \cdots x_{i-1}^{\ell_{i,i-1}}$ for all $i = 2, \ldots, t$ and $x_1^{\kappa_1} - 1$.

Example. Let $n = 36$, $K = (4, 3, 3)$, and $L = (\ell_{2,1}, \ell_{3,1}, \ell_{3,2}) = (3, 2, 1)$. Then

$$\Gamma(K, L) = \langle x_1, x_2, x_3 \mid x_1^4 = 1;\ x_2^3 = x_1^3;\ x_3^3 = x_1^2 x_2 \rangle.$$

The multiplication of $x_1^2 x_2^2 x_3^2$ with $x_1^3 x_2 x_3^2$ is

$$(x_1^2 x_2^2 x_3^2)(x_1^3 x_2 x_3^2) = x_1^5 x_2^3 x_3^4 = x_1 x_1^3 (x_1^2 x_2 x_3) = x_1^2 x_2 x_3.$$

The following lemma, proved in [3], shows that for any K and L, the set $\Gamma(K, L)$ is an abelian group.

▶ **Lemma 6** ([3]). *Let $\kappa_1, \ldots, \kappa_t \in \mathbb{N}$ such that $\kappa_i \ge 2$ and $\kappa_1 \kappa_2 \cdots \kappa_t = n$. Let $0 \le \ell_{i,j} \le \kappa_j - 1$ for $i = 2, \ldots, t$ and $j = 1, \ldots, i-1$. Then, for $K = (\kappa_i)$ and $L = (\ell_{i,j})$,*

1. *$\Gamma(K, L)$ is an abelian group of size $|\Gamma(K, L)| = n$.*
2. *The multiplication of two elements and finding the inverse of an element in $\Gamma(K, L)$ can be computed in time $\tilde{O}(\log^2 n)$.*

We refer to $\Gamma(K, L)$ the *monomial group generated by K and L*. In this abelian group, $X = \{x_1, \ldots, x_t\}$ is a set of generators with the triangular relations $x_1^{\kappa_1} = 1$ and $x_i^{\kappa_i} = x_1^{\ell_{i,1}} \cdots x_{i-1}^{\ell_{i,i-1}}$ for all $i = 2, \ldots, t$.

The following result follows from Kannan and Bachem [14] and Item 2 in Lemma 6. See details in [3].

▶ **Lemma 7.** *There is a deterministic poly$(t, \log n)$ time algorithm that, for any monomial abelian group $\Gamma(K, L)$, returns integers $m_1 | m_2 | \cdots | m_r$ such that $\Gamma(K, L)$ is isomorphic to $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. The algorithm also provides a basis $y_1, \ldots, y_r$ for $\Gamma(K, L)$.*

There is also a randomized algorithm [13] with better time complexity, but the above lemma is sufficient for our purposes.

3.3 Algorithms in Abelian Group

In [3], Bshouty proves the following result.

▶ **Lemma 8.** *Given a Cayley multiplication table of an abelian group G, where each entry in the table can be accessed in constant time, there exists a deterministic algorithm* **Generators** *(in the FS-model) that runs in time $\tilde{O}(|G|)$ and a randomized algorithm* **Random-Generators** *(in the PS-model) that runs in time $\tilde{O}(\sqrt{|G|})$. These algorithms provide*

1. *A set $A = \{a_1, \ldots, a_t\}$ of generators for G of size at most $\log |G|$.*
2. *Integers $K = (k_i)$, $i \in [t]$, where $k_i \ge 2$, $\prod_{i \in [t]} k_i = |G|$ along with integers $L = (\lambda_{i,j})$, where $i \in [t], j \in [i-1]$ and $0 \le \lambda_{i,j} \le k_i - 1$.*
3. *K and L satisfy*

$$a_i^{k_i} = a_1^{\lambda_{i,1}} \cdots a_{i-1}^{\lambda_{i,i-1}}.$$

Additionally, G is isomorphic to $\Gamma(K, L)$ via the isomorphism

$$\Psi(x_1^{j_1} \cdots x_t^{j_t}) = a_1^{j_1} \cdots a_t^{j_t},$$

for every $0 \le j_i \le k_i - 1$ and $i \in [t]$.

4 A One-Sided Tester for Abelian Group

In this section, we prove the following two theorems in the FS-model.

Why not the PS-model? The one-sided tester presented in this section is stated only in the FS-model. In the PS-model, the size of the group is unknown and the algorithm only receives uniformly random elements from an oracle. Since a one-sided tester must accept every abelian group with probability 1, its behavior on Accept-instances must be correct for every possible sequence of oracle outputs. However, after any finite sequence of samples, there is always a positive probability that the oracle continues returning only previously seen elements. Therefore, no deterministic procedure can certify that all elements of the group have been observed and hence cannot determine $|G|$ with certainty.

▶ **Theorem 9.** *There exists a one-sided tester for abelian groups that runs in time $\tilde{O}(|G|+1/\epsilon)$.*

▶ **Theorem 10.** *Let $\mathcal{G}$ be a subclass of abelian groups that is closed under isomorphism. If there exists a deterministic algorithm that can determine, in time T, whether any abelian group of the form $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ belongs to $\mathcal{G}$, then there exists a one-sided tester for $\mathcal{G}$ in the PS-model that runs in time $T + \tilde{O}(|G| + 1/\epsilon)$ and makes $\tilde{O}(|G| + 1/\epsilon)$ queries.*

In particular, there exist testers that run in time $\tilde{O}(|G| + 1/\epsilon)$ for the classes: abelian groups of rank at most k, abelian p-groups, vector spaces over $\mathbb{Z}_p$ and cyclic groups.

We first prove Theorem 9.

Given a binary operation $* : G^2 \to G$, where each entry in the table can be accessed in constant time, we aim to test whether $(G, *)$ is an abelian group or ϵ-far from being an abelian group.

Consider the tester in Algorithm 1. The tester runs the deterministic Algorithm **Generators** from Lemma 8. By Lemma 8, if G is an abelian group, then the algorithm provides:

1. A set $A = \{a_1, \ldots, a_t\}$ of generators for G of size at most $\log |G|$.
2. Integers $K = (k_i)$, where $i \in [t]$ such that $k_i \geq 2$, $\prod_{i\in[t]} k_i = |G|$, along with integers $L = (\lambda_{i,j})$, where $i \in [t], j \in [i-1]$ and $0 \leq \lambda_{i,j} \leq k_i - 1$.

Additionally, G is isomorphic to $\Gamma(K, L)$ via the isomorphism

$$\Psi(x_1^{j_1} \cdots x_t^{j_t}) = a_1^{j_1} * a_2^{j_2} * \cdots * a_t^{j_t}$$

for every $0 \leq j_i \leq k_i - 1$ and $i \in [t]$.

When G is not an abelian group, we cannot guarantee any of the conditions above. If the algorithm **Generators** runs more than time $\tilde{O}(|G|)$ time, or if $K = (k_i)$ and $L = (\lambda_{i,j})$ do not satisfy item 2, or if $|A| > \log |G|$, then $(G, *)$ is not an abelian group, and the tester rejects. See steps 2 and 4.

Otherwise, the tester computes $\Psi(z)$ for all $z \in \Gamma(K, L)$, build a table $\Psi : \Gamma(K, L) \to G$, and verifies whether Ψ is bijective function. If not, the tester rejects. See step 6.

Here, the tester computes Ψ as follows

$$\Psi(x_1^{j_1} \cdots x_t^{j_t}) = a_1^{j_1} * (a_2^{j_2} * (\cdots (a_{t-1}^{j_{t-1}} * a_t^{j_t})) \cdots)$$

where the exponent is handled recursively as follows

$$a^m = \begin{cases} (a^{m/2}) * (a^{m/2}) & \text{if } m \text{ is even,} \\ a * (a^{(m-1)/2} * a^{(m-1)/2}) & \text{if } m \text{ is odd.} \end{cases}$$

If Ψ is a bijective function, then the tester chooses $O(1/\epsilon)$ pairs $(x, y) \in \Gamma(K, L)^2$ uniformly at random and, using the table, verifies whether

$$\Psi(xy) = \Psi(x) * \Psi(y).$$

If this condition holds for all tested pairs, the tester accepts; otherwise, it rejects.

Algorithm 1 One-Sided Tester for Abelian Group.

1: Run the deterministic algorithm **Generators**$(G, *)$.
2: **if** the algorithm runs more than $\tilde{O}(|G|)$ steps **then** Reject.
3: **else** By Lemma 8 obtain:
   1. A set $A = \{a_1, \ldots, a_t\}$ of size at most $\log |G|$.
   2. Integers $K = (k_i)$ for $i \in [t]$, where $k_i \geq 2$ and $\prod_{i\in[t]} k_i = |G|$ along with integers $L = (\lambda_{i,j})$ for $i \in [t], j \in [i-1]$, where $0 \leq \lambda_{i,j} \leq k_i - 1$.
4: **if** the output (A, K, L) does not satisfy the above conditions 1-2 **then** Reject
5: Construct a table of values for the map $\Psi : \Gamma(K, L) \to G$, where for every $j \in \prod_{i\in[t]}[k_i]$:

$$\Psi(x_1^{j_1} \cdots x_t^{j_t}) = a_1^{j_1} * (a_2^{j_2} * (\cdots (a_{t-1}^{j_{t-1}} * a_t^{j_t})) \cdots).$$

6: **if** Ψ is not bijective **then** Reject.
7: **Repeat** the following steps $O(1/\epsilon)$ times:
8: Choose $(x, y) \in \Gamma(K, L)^2$ uniformly at random.
9: **if**

$$\Psi(xy) \neq \Psi(x) * \Psi(y)$$

10: **then** Reject
11: Accept.

We now prove its correctness.

Completeness. If $(G, *)$ is an abelian group, then by Lemma 8, conditions 1 and 2 in the tester hold, and $\Gamma(K, L)$ is isomorphic to G via the isomorphism Ψ. Therefore, Ψ is bijective, and $\Psi(xy) = \Psi(x) * \Psi(y)$. Hence, the tester accepts.

Soundness. Suppose $(G, *)$ is ϵ-far from every abelian group. If the tester does not reject in step 2 or step 4, then, by Lemma 6, $\Gamma(K, L)$ is an abelian group of size $|\Gamma(K, L)| = |G|$. If the tester does not reject in step 6, then Ψ is bijective. By Lemma 5, the magma $(G, \circ)$ where $a \circ b = \Psi(\Psi^{-1}(a)\Psi^{-1}(b))$ is an abelian group isomorphic to $\Gamma(K, L)$. Since $(G, *)$ is ϵ-far from any abelian group, it is also ϵ-far from $(G, \circ)$. Therefore, since Φ is bijective, we have

$$\begin{aligned} \Pr_{x,y\sim\Gamma(K,L)}[\Psi(xy) \neq \Psi(x) * \Psi(y)] &= \Pr_{a,b\sim G}[\Psi(\Psi^{-1}(a)\Psi^{-1}(b)) \neq a * b] \\ &= \Pr_{a,b\sim G}[a \circ b \neq a * b] \geq \epsilon. \end{aligned}$$

Thus, with probability at least $1 - (1 - \epsilon)^{O(1/\epsilon)} \geq 2/3$, the tester rejects in step 10. This completes the proof of the tester's correctness.

Complexity. By Lemma 8, the algorithm **Generators** runs in time $\tilde{O}(|G|)$. Since $j \in \prod_{i\in[t]}[k_i]$ and $\prod_{i\in[t]} k_i = |G|$ computing $a_1^{j_1} * (a_2^{j_2} * (\cdots (a_{t-1}^{j_{t-1}} * a_t^{j_t}))\cdots)$ takes at most time

$$(t-1) + \sum_{i\in[t]} \lceil \log k_i \rceil \leq 2t + \log|G| \leq 3\log|G|.$$

Thus, building the table takes time $\tilde{O}(|G|)$. By Lemma 6, computing the product xy takes time $O(\log^2|G|)$. Hence, this final test takes time $O(\log^2|G|/\epsilon) = \tilde{O}(1/\epsilon)$. Therefore, the time complexity of the tester is $\tilde{O}(|G| + 1/\epsilon)$.

This completes the proof of Theorem 9.

For testing subclasses of abelian groups $\mathcal{G}$ that are closed under isomorphism, Theorem 10, we modify the procedure as follows: After step 4, we run the deterministic algorithm from Lemma 7, which returns integers $m_1|m_2|\cdots|m_r$ such that $\Gamma(K,L)$ is isomorphic to $G' := \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$. We then run the deterministic algorithm to verify whether $G' \in \mathcal{G}$. If not, then we reject.

The same analysis applies, since by Lemma 5, $(G, \circ)$ is isomorphic to $\Gamma(K,L)$.

5 A Tester for Abelian Groups

In this section, we prove

▶ **Theorem 11.** *There exists a tester for abelian groups that runs in time* $\tilde{O}(\sqrt{|G|} + 1/\epsilon)$.

5.1 The Tester

Consider the following tester.

Algorithm 2 Tester For Abelian Groups.

1: Run the algorithm **Random-Generators**$(G, *)$.
2: **if** the algorithm runs in time more than[4] $\tilde{O}(\sqrt{|G|})$ **then** Reject.
3: **else** By Lemma 8 we obtain
   1. A set $A = \{a_1, \ldots, a_t\}$ of size at most $\log|G|$.
   2. Integers $K = (k_i)$ for $i \in [t]$, where $k_i \geq 2$, $\prod_{i\in[t]} k_i = |G|$ along with integers $L = (\lambda_{i,j})$ for $i \in [t], j \in [i-1]$, where $0 \leq \lambda_{i,j} \leq k_i - 1$.
4: **if** the output (A, K, L) does not satisfy the above conditions 1-2 **then** Reject
5: Define $\Psi : \Gamma(K,L) \to G$ where for every $j \in \prod_{i\in[t]}[k_i]$

$$\Psi(x_1^{j_1}\cdots x_t^{j_t}) = a_1^{j_1} * (a_2^{j_2} * (\cdots (a_{t-1}^{j_{t-1}} * a_t^{j_t}))\cdots).$$

6: Choose $m = O(\sqrt{|G|})$ elements $x^{(1)}, x^{(2)}, \ldots, x^{(m)} \in \Gamma(K,L)$ uniformly at random.
7: **If** $(\exists x^{(k)} \neq x^{(j)})\ \Psi(x^{(k)}) = \Psi(x^{(j)})$ **then** Reject.
8: **Repeat** the following steps $O(1/\epsilon)$ times:
9: Choose $(x, y) \in \Gamma(K,L)^2$ uniformly at random.
10: **if**

$$\Psi(xy) \neq \Psi(x) * \Psi(y)$$

11: **then** Reject
12: Accept

Consider the tester in Algorithm 2. The tester runs the randomized Algorithm **Random-Generators**[4] from Lemma 8. By Lemma 8, if G is an abelian group, then, with high probability, it provides:

1. A set $A = \{a_1, \ldots, a_t\}$ of generators for G of size at most $\log |G|$.
2. Integers $K = (k_i)$, where $i \in [t]$ such that $k_i \geq 2$, $\prod_{i\in[t]} k_i = |G|$, along with integers $L = (\lambda_{i,j})$, where $i \in [t], j \in [i-1]$ and $0 \leq \lambda_{i,j} \leq k_i - 1$.

Additionally, G is isomorphic to $\Gamma(K, L)$ via the isomorphism

$$\Psi(x_1^{j_1} \cdots x_t^{j_t}) = a_1^{j_1} * a_2^{j_2} * \cdots * a_t^{j_t}$$

for every $0 \leq j_i \leq k_i - 1$ and $i \in [t]$.

When G is not an abelian group, we cannot guarantee any of the conditions above. If the algorithm **Random-Generators** runs more than $\tilde{O}(\sqrt{|G|})$ time, or if $K = (k_i)$ and $L = (\lambda_{i,j})$ does not satisfy item 2 or if $|A| > \log |G|$, then $(G, *)$ is not an abelian group, and the tester rejects. See steps 2 and 4.

Now, since we require the time complexity to be at most $\tilde{O}(\sqrt{|G|})$, the tester cannot compute $\Psi(z)$ for all $z \in \Gamma(K, L)$, and build a table $\Psi : \Gamma(K, L) \to G$, and verify whether Ψ is a bijective function.

Instead, the tester performs the following two tests:

1. The first test verifies whether Ψ is $\Theta(1)$-close to being a bijective map (see steps 6-7).
2. The second test verifies whether Ψ is $\Theta(\epsilon)$-close to being an isomorphism (see step 9).

The analysis in the following subsection shows that those two tests are sufficient.

5.2 Proof of Correctness and Complexity

We now proceed to prove the correctness of the tester.

Completeness. If $(G, *)$ is an abelian group, then, with high probability, **Random-Generators** procedure returns a valid set of generators A, along with K and L, that satisfy items 1 and 2. Thus, the tester does not reject in steps 2 and 4. Consequently, Ψ is bijective, and G is isomorphic to $\Gamma(K, L)$ via $\Psi : \Gamma(K, L) \to G$. Therefore, the tester does not reject in step 7 and 9, and with high probability, it accepts.

Soundness. Suppose $(G, *)$ is ϵ-far from any abelian group.

If the tester does not reject in steps 2 or 4, then, by Lemma 6, $\Gamma(K, L)$ is a group of size $\prod_{i\in[t]} k_i = |G|$. Thus

$$|\Gamma(K, L)| = |G|.$$

We now prove the following.

▶ **Lemma 12.** *Let x_1, x_2 be distinct elements in $\Gamma(K, L)$. If $\Psi(x_1) = \Psi(x_2)$, then for any $y \in \Gamma(K, L)$, at least one of the following holds:*

1. $\Psi(x_1 y) \neq \Psi(x_1) * \Psi(y)$.
2. $\Psi(x_2 y) \neq \Psi(x_2) * \Psi(y)$.
3. $\Psi(x_1 y) = \Psi(x_2 y)$.

[4] In the PS-model, the size $|G|$ is not given as input; however, the procedure **Random-Generators** returns $|G|$ as part of its output (Lemma 8).

Proof. If $\Psi(x_1y) \neq \Psi(x_2y)$ then since $\Psi(x_1) * \Psi(y) = \Psi(x_2) * \Psi(y)$, we must have either $\Psi(x_1y) \neq \Psi(x_1) * \Psi(y)$ or $\Psi(x_2y) \neq \Psi(x_2) * \Psi(y)$. ◀

Next, we partition $\Gamma := \Gamma(K, L)$ as $\Gamma = \Gamma_1 \cup \Gamma_*$ where

$$\Gamma_1 = \{x \in \Gamma | (\forall y \neq x)\ \Psi(x) \neq \Psi(y)\}, \quad \Gamma_* = \Gamma \backslash \Gamma_1 = \{x \in \Gamma | (\exists y \neq x)\ \Psi(x) = \Psi(y)\}.$$

By the birthday paradox (see also [1] subsection 1.2.3), we obtain the following result.

▶ **Lemma 13.** *If $|\Gamma_*| \geq |\Gamma|/8$, then for $m = O(\sqrt{|G|})$ elements $x^{(1)}, \ldots, x^{(m)} \in \Gamma$ chosen uniformly at random, with probability at least $5/6$, there is a pair $x^{(k)} \neq x^{(j)}$ such that $\Psi(x^{(k)}) = \Psi(x^{(j)})$.*

Thus, if $|\Gamma_*| \geq |\Gamma|/8$, then $(G, *)$ is not an abelian group, and with high probability, the algorithm rejects in steps 6-7. Therefore, we may assume that

$$|\Gamma_*| < |\Gamma|/8. \tag{1}$$

We now distinguish between two cases.

Case I. $|\Gamma_1| \leq (1 - \epsilon/8)|\Gamma|$.

Then $|\Gamma_*| = |\Gamma| - |\Gamma_1| \geq (\epsilon/8)|\Gamma|$. We aim to partition Γ_* into pairs $\{x, y\}$ such that $x \neq y$, $\Psi(x) = \Psi(y)$, and all the pairs are disjoint. While not every element in Γ_* will be included in a pair, we strive to create as many pairs as possible.

To achieve this, consider the relation $x \sim y$ if $\Psi(x) = \Psi(y)$, and partition $\Gamma_* = \Gamma_*^{(1)} \cup \Gamma_*^{(2)} \cup \cdots \cup \Gamma_*^{(w)}$ according to this relation (i.e., the equivalence classes). By definition of Γ_*, each $\Gamma_*^{(i)}$ contains at least two elements with the same image under Ψ. From each $\Gamma_*^{(i)}$, we can create $\lfloor |\Gamma_*^{(i)}|/2 \rfloor$ disjoint pairs. Therefore, we can create at least

$$\sum_{i=1}^{w} \left\lfloor \frac{|\Gamma_*^{(i)}|}{2} \right\rfloor \geq \sum_{i=1}^{w} \frac{|\Gamma_*^{(i)}|}{3} \geq \frac{|\Gamma_*|}{3} \geq \frac{\epsilon}{24}|\Gamma|$$

disjoint pairs.

Let $\{x_1, x_2\}$ be one such pair, where $x_1 \neq x_2$ and $\Psi(x_1) = \Psi(x_2)$. By Lemma 12, for every $y \in \Gamma$, one of the items 1-3 in Lemma 12 occurs. If item 3 occurs for more than $|\Gamma|/2$ of the y values, then $\Psi(x_1y) = \Psi(x_2y)$ for at least $|\Gamma|/2$ ordered pairs $(x_1y, x_2y) \in \Gamma \times \Gamma$. Since Γ is a group, it follows that $x_1y \neq x_2y$ and $x_1y \neq x_1y'$ for $y \neq y'$. Consequently, at least $|\Gamma|/2$ values of y satisfy $x_1y \in \Gamma_*$, implying that $|\Gamma_*| \geq |\Gamma|/2$, which contradicts (1).

Thus, for at least $|\Gamma|/2$ of the y values, either item 1 in Lemma 12 occurs (where $\Psi(x_1y) \neq \Psi(x_1) * \Psi(y)$) or item 2 occurs (where $\Psi(x_2y) \neq \Psi(x_2) * \Psi(y)$).

Since this holds for each pair $\{x, y\}$, and we have at least $(\epsilon/24)|\Gamma|$ such disjoint pairs, it follows that

$$\Pr_{x,y}[\Psi(xy) \neq \Psi(x) * \Psi(y)] \geq \frac{(\epsilon/48)|\Gamma| \cdot |\Gamma|/2}{|\Gamma|^2} \geq \frac{\epsilon}{96}.$$

Therefore, with high probability, the tester rejects in steps 8-10.

Case II. $|\Gamma_1| > (1 - \epsilon/8)|\Gamma|$.

Let $\tilde{\Psi} : \Gamma \to G$ be any bijective function such that $\tilde{\Psi}(x) = \Psi(x)$ if $x \in \Gamma_1$. Define the binary operation $\bullet$ on G as follows:

$$a \bullet b = \tilde{\Psi}(\tilde{\Psi}^{-1}(a)\tilde{\Psi}^{-1}(b)).$$

By Lemma 5, we have the following:

▶ **Lemma 14.** *$(G, \bullet)$ is an abelian group.*

We now prove the following result.

▶ **Lemma 15.** *Let Y be the event $[x \in \Gamma_1, y \in \Gamma_1, xy \in \Gamma_1]$. Then*

$$\Pr_{x,y}[Y] \geq 1 - \frac{3}{8}\epsilon.$$

Proof. We have

$$\Pr_x[x \notin \Gamma_1] = \Pr_y[y \notin \Gamma_1] = \frac{|\Gamma_*|}{|\Gamma|} = \frac{|\Gamma| - |\Gamma_1|}{|\Gamma|} \leq \frac{\epsilon}{8}.$$

Since every group element appears exactly $|\Gamma|$ times in the Cayley table of Γ, it follows that

$$\Pr_{x,y}[xy \notin \Gamma_1] = \frac{|\Gamma_*| \cdot |\Gamma|}{|\Gamma|^2} \leq \frac{\epsilon}{8},$$

and the result follows from the union bound. ◀

If Y ocures, then $\Psi(xy) = \tilde{\Psi}(xy)$, and

$$\Psi(xy) = \tilde{\Psi}(xy) = \tilde{\Psi}(\tilde{\Psi}^{-1}(\tilde{\Psi}(x))\tilde{\Psi}^{-1}(\tilde{\Psi}(y))) = \tilde{\Psi}(x) \bullet \tilde{\Psi}(y).$$

Since $\tilde{\Psi}$ is bijective, $(G, \bullet)$ is abelian group, $(G, *)$ is ϵ-far from any abelian group, and by Lemma 15,

$$\begin{aligned}
\Pr_{x,y}[\Psi(xy) \neq \Psi(x) * \Psi(y)] &\geq \Pr_{x,y}[\Psi(xy) \neq \Psi(x) * \Psi(y)|Y] \Pr[Y] \\
&= \Pr_{x,y}[\tilde{\Psi}(x) \bullet \tilde{\Psi}(y) \neq \tilde{\Psi}(x) * \tilde{\Psi}(y)|Y] \Pr[Y] \\
&\geq (\Pr_{x,y}[\tilde{\Psi}(x) \bullet \tilde{\Psi}(y) \neq \tilde{\Psi}(x) * \tilde{\Psi}(y)] - \Pr[\neg Y]) \Pr[Y] \\
&= (\Pr_{a,b\sim G}[a \bullet b \neq a * b] - \Pr[\neg Y]) \Pr[Y] \\
&\geq (\epsilon - 3\epsilon/8)(1 - 3\epsilon/8) \geq \frac{\epsilon}{3}.
\end{aligned}$$

Thus, with high probability, the tester rejects in steps 8-10. This completes the proof of correctness for the tester.

Time Complexity. The time complexity of the tester is as follows. By Lemma 8, time complexity of **Random-Generators** is $\tilde{O}(\sqrt{|G|})$. Computing $\Psi(\alpha)$ requires time at most

$$\sum_{i=1}^{t} \lceil \log k_i \rceil \leq 2t + \log(k_1 k_2 \cdots k_t) \leq 3 \log |G|.$$

Therefore, the time complexity of steps 6-7 is $\tilde{O}(\sqrt{|G|})$. By Lemma 6, operations in Γ take time $\tilde{O}(\log^2 |G|)$, so the time complexity of steps 8-10 is $\tilde{O}(1/\epsilon)$. Thus, the overall time complexity of the tester is $\tilde{O}(\sqrt{|G|} + 1/\epsilon)$.

6 Testing Subclasses of Abelian Groups

In this section, we prove.

▶ **Theorem 16.** *Let $\mathcal{G}$ be a subclass of abelian groups that is closed under isomorphism. Suppose there exists an algorithm $\mathcal{A}$ that can decide if any abelian group of the form $G' = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ belongs to $\mathcal{G}$ in time T. Then, there exists a tester for $\mathcal{G}$ that runs in time $T + \tilde{O}(\sqrt{|G|} + 1/\epsilon)$ and makes $\tilde{O}(\sqrt{|G|} + 1/\epsilon)$ queries.*

In particular, we have

▶ **Theorem 17.** *There exist testers for abelian groups of rank at most k, abelian p-groups, vector spaces, and cyclic groups over $\mathbb{Z}_p$ that run in time $O(\sqrt{|G|} + 1/\epsilon)$.*

Proof. The tester follows the same structure as the tester for abelian groups in Algorithm 2, with an additional two steps before step 6. These additional steps are:

1. Finding a basis for $\Gamma := \Gamma(K, L)$ to determine the abelian group $G' = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ that is isomorphic to Γ.
2. Verifying whether $G' \in \mathcal{G}$ using algorithm $\mathcal{A}$. If $G' \notin \mathcal{G}$, then the tester rejects.

The basis can be found using the algorithm from Lemma 7.

If Γ is isomorphic to G' and $G' \in \mathcal{G}$, it follows that $\Gamma \in \mathcal{G}$. We now revisit the proof of Theorem 11 to show that if $\Gamma \in \mathcal{G}$, then the tester in Algorithm 2 is a tester for $\mathcal{G}$.

Completeness. If $(G, *)$ is an abelian group in $\mathcal{G}$, then all the arguments from the completeness proof for the abelian group remain valid. Consequently, the algorithm does not reject in the steps 7 and 9.

Since $\Gamma \in \mathcal{G}$, the additional verification step 2 also does not reject, and the tester accepts.

Soundness. Suppose $(G, *)$ is ϵ-far from any abelian group in $\mathcal{G}$.

First, Lemma 12 still applies. The sets Γ_1 and Γ_* are defined in the same way. Consequently, Lemma 13 holds as well. If $|\Gamma_*| \geq |\Gamma|/8$, then $(G, *)$ is not an abelian group and, therefore, is not in $\mathcal{G}$. In that case, with high probability, the algorithm rejects in steps 6-7. Thus, we can assume

$$|\Gamma_*| \leq |\Gamma|/8.$$

Since Case I follows exactly as before, we proceed with Case II, where $|\Gamma_1| > (1 - \epsilon/8)|\Gamma|$.

Let $\tilde{\Psi} : \Gamma \to G$ be any bijective function such that $\tilde{\Psi}(x) = \Psi(x)$ for $x \in \Gamma_1$. Define a binary operation $\bullet$ on G as follows:

$$a \bullet b = \tilde{\Psi}(\tilde{\Psi}^{-1}(a)\tilde{\Psi}^{-1}(b)).$$

The following lemma replaces Lemma 14.

▶ **Lemma 18.** *$(G, \bullet)$ is an abelian group that is isomorphic to Γ.*
In particular, $(G, *)$ is ϵ-far from $(G, \bullet)$.

Proof. The lemma follows from Lemma 5.

Since Γ is in $\mathcal{G}$, we have that $(G, \bullet)$ is in $\mathcal{G}$. Since $(G, *)$ is ϵ-far from any group in $\mathcal{G}$ we have that $(G, *)$ is ϵ-far from $(G, \bullet)$. ◀

Now, Lemma 15 and all the associated arguments also hold in this setting. The only difference is that we now derive

$$\Pr_{a,b \sim G}[a \bullet b \neq a * b] \geq \epsilon$$

because, by Lemma 18, $(G, *)$ is ϵ-far from $(G, \bullet)$. ◀

7 Lower Bounds

In this section, we present lower bounds for testing subclasses of abelian groups.

Bshouty [3] proved the following two lower bounds.

▶ **Lemma 19.** *Let $\mathcal{G}$ be the set of all groups that are isomorphic to either $H_1 = \mathbb{Z}_{2^2}^m$ or $H_2 = \mathbb{Z}_{2^2}^{m-1} \times \mathbb{Z}_2^2$. Any algorithm that, with probability at least 2/3, determines whether $G \in \mathcal{G}$ is isomorphic to H_1 or H_2 must access the elements of G and its Cayley table at least $\Omega(|G|^{1/4})$ times.*

▶ **Lemma 20.** *Let $\mathcal{G}$ be the set of all groups that are isomorphic to either $H_1 = \mathbb{Z}_2^{m-1}$ or $H_2 = \mathbb{Z}_2^m$. Any algorithm that, for $G \in \mathcal{G}$ of unknown size, decides with probability at least 2/3 whether G is isomorphic to H_1 or H_2 must access an oracle that selects uniformly random elements of G and access the Cayley table of G at least $\Omega(|G|^{1/2})$ times.*

In [9], Gall and Yushida proved the following result.

▶ **Lemma 21.** *For any two non-isomorphic groups G and H, G is 1/23-far from H.*

We now give the lower bounds for testers.

▶ **Theorem 22.** *Let $\mathcal{G}$ be the set of all abelian groups isomorphic to $H_1 = \mathbb{Z}_{2^2}^m$. Then, in the FS-model, any tester for $\mathcal{G}$ with $\epsilon < 1/23$ must run in time $\Omega(|G|^{1/4})$.*

Proof. Let $\mathcal{T}$ be a tester for $\mathcal{G}$ that runs in time t. Define the set of groups $\mathcal{G}'$ to be all groups that are isomorphic to either $H_1 = \mathbb{Z}_{2^2}^m$ or $H_2 = \mathbb{Z}_{2^2}^{m-1} \times \mathbb{Z}_2^2$. Given $G \in \mathcal{G}'$, we run the tester $\mathcal{T}$ on G with $\epsilon < 1/23$. If G is isomorphic to H_1, the tester accepts with probability at least 2/3. If G is isomorphic to H_2, then since, by Lemma 21, H_2 is 1/23-far from G, the tester rejects with probability at least 2/3. Thus, the tester $\mathcal{T}$ can distinguish between $G \in \mathcal{G}'$ that are isomorphic to H_1 and those that are isomorphic to H_2. By Lemma 19, it must run in time $\Omega(|G|^{1/4})$. ◀

We now prove the following lower bound.

▶ **Theorem 23.** *Let $\mathcal{G}$ be the set of all abelian groups of even rank. Then, in the PS-model, any tester for $\mathcal{G}$ with $\epsilon < 1/23$ must run in time $\Omega(\sqrt{|G|})$.*

Proof. Suppose there exists a tester $\mathcal{T}$ for $\mathcal{G}$ that runs in time $T(|G|)$. Consider the set of groups $\mathcal{G}'$ that are isomorphic to either $H_1' = \mathbb{Z}_2^{2m}$ or $H_2' = \mathbb{Z}_2^{2m-1}$. Given G that is either isomorphic to H_1' or H_2', we run the tester $\mathcal{T}$. If the tester accepts, then G is isomorphic to H_1'. This is because H_1' is of even rank, while H_2' is 1/23-far from any group of size 2^{2m-1} with even rank. For the same reason, if the tester rejects, G is isomorphic to H_2'.

By Lemma 20, for $n = 2^{2m}$, we have $T(n) = \Omega(\sqrt{n})$. ◀

It follows from [7] that any tester for abelian groups or their subclasses must make at least $\Omega(1/\epsilon)$ queries. This also follows from the fact that if we take any group and modify an $\epsilon < 1/46$ fraction of the entries of its Cayley table, chosen uniformly at random, to different values, we obtain a magma H that is ϵ-far from every group. At least $\Omega(1/\epsilon)$ queries are required to identify one of these modified entries.

References

1 Noga Amir, Oded Goldreich, and Guy N. Rothblum. Doubly sub-linear interactive proofs of proximity. *Electron. Colloquium Comput. Complex.*, TR24-143, 2024. URL: https://eccc.weizmann.ac.il/report/2024/143.

2 Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. Syst. Sci.*, 47(3):549–595, 1993. doi:10.1016/0022-0000(93)90044-W.

3 Nader H. Bshouty. Sublinear time algorithms for abelian group isomorphism and basis construction. In Jakub Kozik and Alexander Wolff, editors, *SOFSEM 2026: Theory and Practice of Computer Science - 51st International Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM 2026, Kraków, Poland, February 9-13, 2026, Proceedings*, volume 16448 of *Lecture Notes in Computer Science*, pages 31–45. Springer, 2026. doi:10.1007/978-3-032-17801-5_3.

4 Artur Czumaj and Christian Sohler. Sublinear-time algorithms. *Bull. EATCS*, 89:23–47, 2006.

5 Funda Ergün, Sampath Kannan, Ravi Kumar, Ronitt Rubinfeld, and Mahesh Viswanathan. Spot-checkers. *J. Comput. Syst. Sci.*, 60(3):717–751, 2000. doi:10.1006/JCSS.1999.1692.

6 Shai Evra, Shay Gadot, Ohad Klein, and Ilan Komargodski. Verifying groups in linear time. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, pages 2131–2147. IEEE, 2024. doi:10.1109/FOCS61266.2024.00126.

7 Eldar Fischer. A basic lower bound for property testing. *CoRR*, abs/2403.04999, 2024. doi:10.48550/arXiv.2403.04999.

8 Katalin Friedl, Gábor Ivanyos, and Miklos Santha. Efficient testing of groups. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 157–166, 2005. doi:10.1145/1060590.1060614.

9 François Le Gall and Yuichi Yoshida. Property testing for cyclic groups and beyond. *J. Comb. Optim.*, 26(4):636–654, 2013. doi:10.1007/S10878-011-9445-8.

10 Oded Goldreich, editor. *Property Testing - Current Research and Surveys*, volume 6390 of *Lecture Notes in Computer Science*. Springer, 2010. doi:10.1007/978-3-642-16367-8.

11 Oded Goldreich. *Introduction to Property Testing*. Cambridge University Press, 2017. doi:10.1017/9781108135252.

12 Oded Goldreich and Laliv Tauber. On testing group properties. *Electron. Colloquium Comput. Complex.*, TR23-214, 2023. URL: https://eccc.weizmann.ac.il/report/2023/214.

13 Erich L. Kaltofen and Gilles Villard. On the complexity of computing determinants. *Comput. Complex.*, 13(3-4):91–130, 2005. doi:10.1007/S00037-004-0185-3.

14 Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, 1979. doi:10.1137/0208040.

15 Igor Pak. Testing commutativity of a group and the power of randomization. *LMS J. Comput. Math.*, 15:38–43, 2012. doi:10.1112/S1461157012000046.

16 Sridhar Rajagopalan and Leonard J. Schulman. Verification of identities. *SIAM J. Comput.*, 29(4):1155–1163, 2000. doi:10.1137/S0097539797325387.

17 Dana Ron. Property testing: A learning theory perspective. *Foundations and Trends in Machine Learning*, 1(3):307–402, 2008. doi:10.1561/2200000004.

18 Dana Ron. Algorithmic and analysis techniques in property testing. *Foundations and Trends in Theoretical Computer Science*, 5(2):73–205, 2009. doi:10.1561/0400000029.

19 Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. Comput.*, 25(2):252–271, 1996. doi:10.1137/S0097539793255151.