# A General Framework for Low Soundness Homomorphism Testing

**Tushant Mittal**
Stanford University, CA, USA

**Sourya Roy**
University of Iowa, Iowa City, IA, USA

## Abstract

We introduce a general framework to design and analyze algorithms for the problem of testing homomorphisms between finite groups in the low-soundness regime.

In this regime, we give the first constant-query tests for various families of groups. These include tests for: (i) homomorphisms between arbitrary cyclic groups, (ii) homomorphisms between any finite group and $\mathbb{Z}_p$, (iii) automorphisms of dihedral and symmetric groups, (iv) inner automorphisms of non-abelian finite simple groups and extraspecial groups, and (v) testing linear characters of $\mathrm{GL}_n(\mathbb{F}_q)$, and finite-dimensional Lie algebras over $\mathbb{F}_q$. We also recover the result of Kiwi [TCS'03] for testing homomorphisms between $\mathbb{F}_q^n$ and $\mathbb{F}_q$.

Prior to this work, such tests were only known for abelian groups with a constant maximal order (such as $\mathbb{F}_q^n$). No tests were known for non-abelian groups.

As an additional corollary, our framework gives combinatorial list decoding bounds for cyclic groups with list size dependence of $O(\varepsilon^{-2})$ (for agreement parameter $\varepsilon$). This improves upon the currently best-known bound of $O(\varepsilon^{-105})$ due to Dinur, Grigorescu, Kopparty, and Sudan [STOC'08], and Guo and Sudan [RANDOM'14].

**2012 ACM Subject Classification** Theory of computation → Error-correcting codes

**Keywords and phrases** Property Testing, Coding Theory

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2026.103

**Related Version** *Full Version*: `https://arxiv.org/abs/2509.05871`

**Funding** *Tushant Mittal*: T.M. is a postdoctoral fellow supported by the NSF grants CCF-2143246 and CCF-2133154.
*Sourya Roy*: S.R. was partially supported by the Old Gold Summer Fellowship from The University of Iowa.

**Acknowledgements** We sincerely thank the reviewer for their helpful comments and careful reading of our manuscript.

## 1 Introduction

The problem of *homomorphism testing* has been extensively studied in the theoretical computer science literature [2, 6, 17, 23, 15]. A primary motivation for studying this question is its relevance to the theory of *probabilistically checkable proofs* [4, 5] and *locally testable codes*. Additionally, there has been an interest in studying such tests in quantum complexity, for example, *entanglement testing* [20] involves homomorphism testing which played an important role in the proof of MIP$^*$=RE [16].

In this work, we study this homomorphism testing problem in the context of general finite groups. To make the discussion precise, we begin by formally describing the setup. Let $G$ and $H$ be two finite groups. Denote by $\mathrm{Hom}(G, H)$, the set of all homomorphisms from $G$ to $H$, i.e., a function such that, $f(xy) = f(x) \cdot f(y)$ for each $x, y \in G$.

▶ **Definition 1.** $\mathrm{Hom}(G,H)$ *is* $(k,\delta,\varepsilon)$*-testable if there exists an algorithm (test) that, given oracle access to a function* $f : G \to H$*, makes* $k$ *queries to it, and satisfies the following:*

- *(Completeness) If* $f$ *is a homomorphism, the test passes with probability* 1*.*
- *(Soundness) If test passes with probability* $\delta$ *(over the choice of queries), then there exists a homomorphism* $\varphi$ *such that* $\mathrm{agr}(f,\varphi) := \Pr_{x\sim G}[f(x)=\varphi(x)] \geq \varepsilon(\delta)$*.*

As an example, the famous Blum–Luby–Rubinfield [6] (BLR) test samples a random pair $x, y \sim G$ and checks if $f(x)\cdot f(y) = f(xy)$. This test shows that $\mathrm{Hom}(\mathbb{F}_2^n, \mathbb{F}_2)$, also known as the *Hadamard code*, is $(3,\delta,\delta)$-testable. We are interested in identifying finite groups, $(G,H)$, for which the set $\mathrm{Hom}(G,H)$ is testable and designing such tests.

### High Soundness Regime

It is much easier to construct a test that only guarantees soundness when a function passes the test with a probability much larger than the test passing probability of a random function. This regime is known as the high soundness or the unique decoding regime, as there is often a unique homomorphism that agrees with the input function. There are many results in this regime and in particular, Ben Or-Coppersmith-Luby-Rubinfeld [3], showed that $\mathrm{Hom}(G,H)$ is $(3,\delta,1-\frac{\delta}{2})$-testable for $\delta > \frac{7}{9}$ for any finite groups $G, H$. Moreover, the test is the same as the BLR test.

### Low Soundness Regime

It is significantly more difficult to design and analyze tests in the low soundness (*list decoding*) setting when the test passing probability can be arbitrarily small, and the function has a tiny agreement with many homomorphisms. As a sharp contrast to the result of [3], the only known cases for which the BLR test has been analyzed in this low soundness setting are: (i) $(\mathbb{F}_p^n, \mathbb{F}_p)$ for some prime $p$, by Håstad and Wigderson [15], and (ii) $(\mathbb{F}_p^n, \mathbb{F}_p^m)$ by Samrodnitsky[1] [23] which can be generalized to the setting of $G = \mathbb{Z}_p^{n_1} \oplus \cdots \oplus \mathbb{Z}_{p^r}^{n_r}$, where $r = O(1)$.

### Issues with BLR

The high-soundness result of [3] cannot be hoped to generalized to the low soundness setting, as they also give the following counterexample: for any $r \geq 3$, there exists a function $f : \mathbb{Z}_{3^r} \to \mathbb{Z}_{3^{r-1}}$ that passes the BLR test with probability $\frac{7}{9}$ but agrees with any homomorphism at most $3^{-(r-1)}$-fraction of points. This demonstrates that BLR fails catastrophically, even for cyclic groups, in the low-soundness regime.

Moreover, even in cases for which BLR works, it is not always known to yield the best agreement guarantee. For instance, [15] showed that the BLR test for $(\mathbb{F}_p^n, \mathbb{F}_p)$ achieves an agreement guarantee of $\varepsilon(\delta) = \frac{1+\delta}{p}$. Hence, even when the function passes with probability 1, the guarantee is small for large $p$. This was remedied by Kiwi [17] by giving a different test[2] which showed that $\mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q)$ is $(3,\delta,\delta)$-testable.

The above discussion shows that new tests and techniques must be devised to handle new families of groups and/or obtain optimal parameters. Additionally, it is desirable to have tests that can provide an improved soundness guarantee by using more queries.

---

[1] For $p = 2$, this setting is equivalent to the Freiman-Rusza conjecture for which improved bounds were proven in the breakthrough works of [24, 11].

[2] Grigorescu, Kopparty and Sudan [13], and Gopalan [10] gave an alternate Fourier analytic proof of Kiwi's result.

## 1.1 Our Contribution

We take a first step towards this by defining a general testing framework and using it to get testability results for a variety of groups. In particular, we give the first tests for classes of non-abelian groups in the low-soundness setting. Our meta-test is the following. Let $G, H$ be finite groups, $k$ be an integer, and let $\mathcal{D}_k$ be a distribution on $G^k$.

**$\mathsf{Test}_k(G, H, \mathcal{D}_k)$**

- Sample $(x_1, \ldots, x_k) \sim \mathcal{D}_k \subseteq G^k$.
- Return 1 if and only if there exists[3] a homomorphism (or automorphism) $\varphi$ such that $f(x_i) = \varphi(x_i)$ for $i \in [k]$.

We explain the framework in Section 1.2, but briefly summarize its salient features:

- **Defining the Distribution $\mathcal{D}_k$** – A key feature of the framework is that this distribution naturally emerges from an (approximating) expression for the soundness, i.e., $\max_{\varphi \in \mathrm{Hom}(G,H)} \mathrm{agr}(f, \varphi)$. The BLR test uses the uniform distribution over $\{(x_1, x_2, x_3) \mid x_1 x_2 x_3 = 1\}$ as $\mathcal{D}_k$, regardless of the groups $G, H$. In contrast, our distribution takes into account the group-theoretic data. In the special case of $(\mathbb{F}_2^n, \mathbb{F}_2)$, our distribution coincides with the one in BLR, but for other groups, they are quite different. For example, in the case of cyclic groups, our distribution (roughly) weighs elements based on their order and is not uniform. This difference intuitively explains why BLR fails for cyclic groups, but our test works.
- **Distance Approximation and List Decoding** – Our analysis works by giving an exact expression for the $k^{\text{th}}$-moment, $\sum_\varphi \mathrm{agr}\,(f, \varphi)^k$. This can be seen as a "degree-$k$ variant" of the general Johnson bound (which is for $k = 2$). Such an expression not only yields a soundness guarantee but also implies a bound on (i) the number of "large-agreement homomorphisms", i.e., combinatorial list size bounds for homomorphism codes, and (ii) the largest possible agreement that gives a tight control on the distance of the input function $f$ to the property of being a homomorphism. This task of distance approximation was introduced in [22], where they show that approximating distance implies *tolerant tests*.
- **Avoiding Fourier Analysis** – Our technique works entirely in the "physical space" by reducing the soundness analysis to the computation of certain group-theoretic constants. For some classes of groups (such as finite simple groups), these constants have been studied in the literature. This is helpful when the target group $H$ does not embed easily into $\mathbb{C}$, and one cannot directly rely on Fourier analysis.
- **Query vs Soundness Tradeoff** – The above test works for any (large enough) number of queries $k$, and the analysis shows that the test guarantee improves exponentially with the number of queries, $\varepsilon(\delta) \approx \delta^{\frac{1}{k}}$, giving us a smooth tradeoff between query complexity and the soundness guarantee.

### 1.1.1 Homomorphism Testing

We now summarize our results for homomorphism testing over various classes of finite abelian groups. To the best of our knowledge, all the tests here are novel except for the 3-query test for $\mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q)$ due to [17].

[3] For almost all the groups we study, there is a simple and efficient way to check this.

▶ **Theorem 2** (Summary of Homomorphism Testing). *For each pair of groups $G, H$ as listed in Table 1, and correspondingly allowed integers $k$, $\mathrm{Hom}(G,H)$ is $(k, \delta, \varepsilon(\delta))$-testable. The test is $\mathsf{Test}_k(G, H, \mathcal{D}_k)$, for an explicitly defined distribution $\mathcal{D}_k$ on $G^k$. Additionally, we also get an upper bound of $\max_\varphi \mathrm{agr}(f,\varphi) \leq O(\delta^{\frac{1}{k}})$, for any appropriate $k$ as in the table.*

**Table 1** A summary of our results on homomorphism testing.

| Result | $G$ | $H$ | Query | Soundness $[\varepsilon(\delta)]$ |
|---|---|---|---|---|
| Theorem 27 | $\mathbb{F}_q^n$ | $\mathbb{F}_q$ | Odd $k \geq 3$ | $\frac{1}{q} - O(\frac{1}{q^n}) + (\frac{q-1}{q}) \cdot \left(\frac{q\delta - 1}{q-1}\right)^{\frac{1}{k-2}}$ |
| [17] | $\mathbb{F}_q^n$ | $\mathbb{F}_q$ | $k = 3$ | |
| Theorem 20 | $\mathbb{Z}_n$ | $\mathbb{Z}_m$ | Any $k \geq 4$ | $\left(\zeta(2)^2 \cdot \delta\right)^{\frac{1}{k-3}}$ |
| Theorem 30 | $\mathbb{F}_q$ | $\mathbb{F}_q^n$ | Any $k \geq 2$ | $\frac{q-1}{q} \cdot \delta^{\frac{1}{k-1}}$ |
| Theorem 15 | $\mathbb{Z}_{p^r}$ | Abelian group of $p$-rank $\leq t$ | Any $k \geq t+2$ | $\left(\frac{(p-1)^2}{p^2} \cdot \delta\right)^{\frac{1}{k-t-1}}$ |

Note: The $p$-rank of an Abelian group is the number of cyclic groups of order a power of $p$ in its decomposition, see Fact 7.

### Combinatorial List Decoding

While the focus of our work is not list decoding, our technique yields stronger bounds than currently known for some groups. This is because our analysis gives bounds on $\sum_\varphi \mathrm{agr}(f,\varphi)^k$, and the list size then immediately follows.

The work of Dinur, Grigorescu, Kopparty, and Sudan [8], and later Guo and Sudan [14] gave a list size bound of $O\left(\varepsilon^{-105}\right)$ that works for every pair of abelian groups (and in fact "supersolvable" groups). However, their bound does not improve even when $H$ is cyclic. We prove a much better bound of $\varepsilon^{-2}$ for cyclic groups of prime power and $\varepsilon^{-3}$ for general cyclic groups.

▶ **Theorem 3** (List Decoding for Cyclic groups). *Let $G = \mathbb{Z}_{p^r}$ and $H = \mathbb{Z}_{p^s}$ be cyclic groups. Let $f : G \to H$ be any function. Then the following holds:*

$$\left|\{\varphi \in \mathrm{Hom}(G,H) \ : \ \mathrm{agr}(f,\varphi) \ \geq \ \varepsilon\}\right| \ \leq \ \left(\frac{p}{p-1}\right) \cdot \frac{1}{\varepsilon^2}.$$

*In general, we get a list size bound of $2\varepsilon^{-(t+1)}$ when $H$ is an abelian group of $p$-rank $t \geq 1$. Additionally, for any integers $n, m \geq 1$, we get the following list size bound:*

$$\left|\{\varphi \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \ : \ \mathrm{agr}(f,\varphi) \ \geq \ \varepsilon\}\right| \ \leq \ \frac{\zeta(2)^2}{\varepsilon^3},$$

*where $\zeta(2) = \frac{\pi^2}{6}$, is the Riemmann-Zeta function.*

## 1.1.2 Automorphism Testing over Non-Abelian Groups

A very important class of homomorphisms arises from automorphisms of groups. Our next set of results concern testing automorphisms and inner automorphisms over various families for finite non-abelian groups. We quickly recall the relevant definitions,

$$\begin{aligned} \mathrm{Aut}(G) \ &= \ \{\varphi \in \mathrm{Hom}(G,G) \mid \varphi \text{ is bijective}\}, \\ \mathrm{Inn}(G) \ &= \ \{\varphi_g, \ g \in G \mid \varphi_g(x) = gxg^{-1}\} \ \subseteq \ \mathrm{Aut}(G). \end{aligned}$$

The set of inner automorphisms is easier to work with as the maps are very explicit. Moreover, for many groups, the inner automorphisms capture most of the automorphisms. For example, for the symmetric group $\mathrm{Sym}_n$, all the automorphisms are inner ([25]) (for $n \neq 6$). The following theorem consolidates all our automorphism testing results.

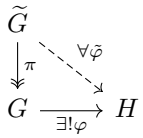
▶ **Theorem 4** (Automorphism Testing (Summary of Theorems 31 and 32)). *The following results hold by using* $\mathsf{Test}_k(G, G, \mathcal{D}_k)$ *for an explicitly defined distribution* $\mathcal{D}_k$ *on* $G^k$ :

- *For the family of dihedral groups,* $D_{2p}$ *(p prime),* $\mathrm{Aut}(D_{2p})$ *is* $\left(k,\, \delta,\, \frac{1}{2}\delta^{\frac{1}{k-2}}\right)$*-testable for every* $k \geq 3$.
- *For the family of symmetric groups,* $\mathrm{Aut}(\mathrm{Sym}_n) = \mathrm{Inn}(\mathrm{Sym}_n)$ *is* $\left(k,\, \delta,\, \delta^{\frac{1}{k-2}} - o_n(1)\right)$*-testable for every* $k \geq 3$*, and* $n \neq 6$.
- *For every non-abelian finite simple group* $G$, $\mathrm{Inn}(G)$ *is* $\left(k,\, \delta,\, \delta^{\frac{1}{k-2}} - o_{|G|}(1)\right)$*-testable for every* $k \geq 4$.
- *For any extraspecial group* $G$ *of order* $p^r$, $\mathrm{Inn}(G)$ *is* $\left(k,\, \delta,\, \delta^{\frac{1}{k-r}} - o_p(1)\right)$*-testable for every* $k \geq r+1$*. In particular, for the family of Heisenberg groups* $(H_p)$ *(the group of* $3 \times 3$ *unitrianguar matrices over* $\mathbb{F}_p$*),* $\mathrm{Inn}(H_p)$ *is* $\left(k,\, \delta,\, \delta^{\frac{1}{k-3}} - o_p(1)\right)$*-testable for any* $k \geq 4$.

*Additionally, we also get an upper bound of* $\max_\varphi \mathrm{agr}\,(f, \varphi) \leq O(\delta^{\frac{1}{k}})$*, for any group* $G$ *and* $k$ *as above, except the dihedral group.*

### 1.1.3 Lifting Homomorphism Tests

We give a general method to extend results for testability of known $\mathrm{Hom}(G, H)$ to those of $\mathrm{Hom}(\widetilde{G}, H)$ in cases when $\mathrm{Hom}(\widetilde{G}, H)$ factors through $\mathrm{Hom}(G, H)$.




For instance, when $H$ is abelian, every homomorphism from $G$ to $H$ factors through an "abelianization" of $G$, which is defined as $G/[G, G]$ where $[G, G]$ is the subgroup generated by $\langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$. This also works when we have a more general structure like a *Lie algebra*. We quickly define the notion of a character over a Lie algebra.

#### Lie algebra characters

A finite-dimensional Lie algebra, $\mathfrak{g}$, is a finite-dimensional vector space over a field $\mathbb{F}$ with a Lie bracket $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ which is a bilinear map such that

$$[x, x] = 0 \quad \text{and} \quad [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0, \quad \forall\, x, y, z \in \mathfrak{g}.$$

A *linear character* of a Lie algebra is a linear map $\varphi : \mathfrak{g} \to \mathbb{F}$ such that $f([x, y]) = 0$ for every $x, y \in \mathfrak{g}$. Therefore, it is a linear map between vector spaces subject to an additional constraint. For example, let $\mathfrak{gl}_n(q) = \mathbb{F}_q^{n \times n}$, the vector space of $n \times n$-matrices. The bracket is defined as $[x, y] := xy - yx$, where the multiplication is matrix multiplication. A character of $\mathfrak{gl}_n$ is a linear map with the property that $f(xy) = f(yx)$ for every pair of matrices $x, y$.

Character testing has also been studied in the literature [1, 19, 21, 12, 18] for general groups (and more general representations). However, to the best of our knowledge, all known results work in the $L^2$-metric, i.e., the soundness guarantee is in terms of $\|f(x) - \varphi\|_2^2$. Our result gives the first character testing results for non-abelian groups in the Hamming metric.

▶ **Theorem 5** (Lifting results). *For the groups/Lie algebras mentioned in Table 2, one can obtain testing results by lifting from their base code. Moreover, the queries and soundness guarantees are identical to those of the base code.*

**Table 2** A summary of our lifting results.

| Result | $G$ | $H$ | Base Code |
|---|---|---|---|
| Theorem 34 | Any finite group<br>Any Lie Algebra over $\mathbb{F}_p$ | $\mathbb{F}_p$ | $\mathrm{Hom}(\mathbb{F}_p^n, \mathbb{F}_p)$ |
| Theorem 33 | $\mathrm{GL}_n(q),\ q \neq 2$ | $\mathbb{F}_q^*$ | $\mathrm{Hom}(\mathbb{Z}_{q-1}, \mathbb{Z}_{q-1})$ |
| Theorem 35 | $\mathfrak{gl}_n(q)$ | $\mathbb{F}_q$ | $\mathrm{Hom}(\mathbb{Z}_q, \mathbb{Z}_q)$ |

Note: For the first result, $n$ is the $p$-rank of $G$, i.e., the $p$-rank of its abelianization, or the rank of the Lie algebra.

▶ Remark 6. In coding theory terms, the lifted homomorphism code (up to permutation) is the base code tensored with the repetition code of length $m = (|\ker(\pi)|)$. Thus, one could alternatively design a test from this perspective, or appeal to results on local testability of tensor codes such as [9]. However, our approach yields the result easily by allowing us to mechanically reuse the analysis of the base code.

## 1.2 Technical Overview

For a function $f$ and a homomorphism $\varphi$, let $\mathrm{agr}(f, \varphi)$ be the agreement between these functions, i.e., the fraction of inputs on which they agree. We wish to estimate $\max_\varphi \mathrm{agr}(f, \varphi)$. To do this, we will define a distribution $\mathcal{F}$ on $\mathrm{Hom}(G, H)$. Clearly,

$$\max_{\varphi \in \mathrm{Hom}(G,H)} \mathrm{agr}(f, \varphi) \ \geq \ \mathop{\mathbb{E}}_{\varphi \sim \mathcal{F}}[\mathrm{agr}(f, \varphi)] \ . \tag{1}$$

For this approximation to be useful, the distribution must have a large mass on homomorphisms that agree significantly with $f$. A natural choice for such a distribution is $\Pr[\varphi] \propto \mathrm{agr}(f, \varphi)^k$ for some positive integer $k$. Note that this is general and agnostic to the choice of groups (or even the fact that the code is a homomorphism code).

This expectation then becomes:

$$\mathop{\mathbb{E}}_{\varphi \sim \mathcal{F}}[\mathrm{agr}(f, \varphi)] \ = \ \frac{\sum_\varphi \mathrm{agr}(f, \varphi)^{k+1}}{\sum_\varphi \mathrm{agr}(f, \varphi)^k} \ .$$

The next step is to estimate this expectation via a test that queries $f$ at only a few points. We do this by reinterpreting the expression for the $k^{\text{th}}$ powers algebraically, using the knowledge that the code is a homomorphism code. The key point of the framework is that after this reinterpretation, the definition of a test pops quite intuitively, such that

$$\sum_{\varphi \in \mathrm{Hom}(G,H)} \mathrm{agr}(f, \varphi)^k \ \propto \ \Pr[f \ \text{passes} \ \mathsf{Test}_k]. \tag{2}$$

Once we have this, the main testing result is a simple calculation. We now explain our algebraic reinterpretation of this expression and the test that emerges from it. The key to our method is the following evaluation map[4].

[4] We thank MO user *t3suji* whose comment on [7] was the inspiration for us to study this map.

### The evaluation map

One important way in which this framework utilizes the structure of $\mathrm{Hom}(G, H)$, is that for any fixed tuple $\vec{x} = (x_1, \ldots, x_k) \in G^k$, there is a naturally associated evaluation map,

$$\Gamma_{\vec{x}} : \mathrm{Hom}(G, H) \to H^k,\ \Gamma_{\vec{x}}(\varphi) = (\varphi(x_1), \ldots, \varphi(x_k)).$$

While this map could be defined for any subset of functions (and not necessarily homomorphisms), for the set of homomorphisms, the map is $N$-to-one on its image, where $N = |\ker(\Gamma_{\vec{x}})|$. This crucial property immediately implies that,

$$\sum_{\varphi} \mathrm{agr}(f, \varphi)^k \ = \ \mathop{\mathbb{E}}_{\vec{x} \sim G^k} \left[ \mathbb{1}_{f(\vec{x}) \in \mathrm{Im}(\Gamma_{\vec{x}})} \cdot |\ker(\Gamma_{\vec{x}})| \right].$$

The right-hand side can now be interpreted as a test wherein a tuple is sampled with a weight $\propto |\ker \Gamma_{\vec{x}}|$, and the indicator $\mathbb{1}_{f(\vec{x}) \in \mathrm{Im}(\Gamma_{\vec{x}})}$ tests if there exists a homomorphism $\varphi$ with which $f$ agrees on the entire tuple $\vec{x}$. This test trivially passes if $\mathrm{Im}(\Gamma_{\vec{x}}) = H^k$ and thus we exclude such tuples. The final test is then,

**$\mathsf{Test}_k(G, H)$**

- Sample $(x_1, \ldots, x_k) \propto |\ker \Gamma_{\vec{x}}|$ subject to $\mathrm{Im}(\Gamma_{\vec{x}}) \neq H^k$.
- If $(f(x_1), \ldots, f(x_k)) \in \mathrm{Im}(\Gamma_{\vec{x}})$: return 1; otherwise: return 0.

### Analyzing and adjusting the test

The above recipe works as it is for a given pair of groups if the following hold:

1. Our approximation, i.e., Equation (1), is not too weak, and
2. The test we have defined indeed approximates $\sum_{\varphi} \mathrm{agr}\,(f, \varphi)^k$ well.

Among the cases we analyze, this happens for cyclic (and cyclic-like) groups, and our results in Section 3 directly use this test. However, for $\mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q)$, the first condition does not hold. This is remedied by using a shifted variant of $\mathrm{agr}(f, \varphi)$. Moreover, verifying the second point, i.e., checking if Equation (2) holds can be difficult in general, and another trick we employ is to define the test on a subset of all $k$-tuples that makes the analysis more manageable. We wish to emphasize that $\mathsf{Test}_k(G, H)$ gives a starting point from which to derive a test for a general pair of groups.

## 1.3 Outline

We start in Section 1.4 by summarizing basic definitions and some of the notation used throughout the paper. The general testing framework developed in Section 2 captures the core methodology that is used throughout the paper to prove our main results.

As our first application, we use the proposed framework in Section 3 to establish the testing and list decoding results for cyclic groups. In particular, in Section 3.1, we prove the testing result, Theorem 15, for $G = \mathbb{Z}_{p^r}$ and $H =$ abelian group of bounded $p$-rank; here, we also prove the list decoding theorem, Theorem 16. In Section 3.2, we generalize to the case when $G$ and $H$ are arbitrary cyclic groups.

We focus on vector spaces in Section 4. The main result of this section is Theorem 27 that allows us to test functions from $\mathbb{F}_q^n \to \mathbb{F}_q$. In the same section, we also derive a testing result (Theorem 30) for $\mathrm{Hom}(\mathbb{F}_q, \mathbb{F}_q^n)$.

In Section 5 and Section 6, we consider the non-abelian setting. Section 5 focuses on testing for closeness to an automorphism or an inner automorphism. We look at dihedral groups (Theorem 31), symmetric group, quasirandom groups, and more generally, finite simple groups (Theorem 32). Finally, in Section 6, we prove a general lifting theorem. This allows us to prove our character testing results (Theorems 33 and 35), and other lifted results Theorem 34.

## 1.4 Prelims

▶ **Fact 7** (*p*-components of Abelian groups). *Every finite abelian group decomposes into* $G = \oplus_p G_p$ *where* $G_p = \oplus_i \mathbb{Z}_{p^{b_i}}$ *is the p-component of* $G$*. The p-rank of* $G$ *is the number of summands in* $G_p$*. Moreover,* $\mathrm{Hom}(G,H) \cong \oplus_p \mathrm{Hom}(G_p, H_p)$.

▶ **Fact 8** (Cyclic Homomorphisms). *Let* $G = \mathbb{Z}_{p^r}$ *and* $H$ *be any abelian group with a p-component* $\oplus_i \mathbb{Z}_{p^{b_i}}$*. Then,* $\mathrm{Hom}(G,H) = \oplus_i \mathbb{Z}_{p^{\min(r,b_i)}}$*, and thus,* $|\mathrm{Hom}(G,H)| \le |H|$.

**Proof.** Any homomorphism $\varphi : \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^b}$, is determined by $\varphi(1)$ which must have order $p^{a_\varphi} \le p^{\min(r,b)}$. For a given order $p^j$, the number of elements with order at most $j$ is $p^j$ and thus $\mathrm{Hom}(G,H) = \mathbb{Z}_p^{\min(r,b)}$. ◀

**Notation.** Let $f : G \to H$ be a function. For any $\vec{x} = (x_1, \ldots, x_k) \in G^k$, we use the shorthand: $f(\vec{x}) := (f(x_1), \ldots, f(x_k))$.

## 2 A General Test

For any, $\vec{x} \in G^k$, we define the following evaluation map:

$$\Gamma_{\vec{x}} : \mathrm{Hom}(G,H) \to H^k \ : \ \Gamma_{\vec{x}}(\varphi) = (\varphi(x_1), \ldots, \varphi(x_k)) \ .$$

Because $H$ is an abelian group, the set $\mathrm{Hom}(G,H)$ is an abelian group under pointwise multiplication. Moreover, the maps $\{\Gamma_{\vec{x}}\}_{\vec{x}}$ are homomorphisms. We make the following important definitions that we will use throughout:

$$\mathsf{H}_{\vec{x}} := \mathrm{Im}(\Gamma_{\vec{x}}) \leqslant H^k, \quad \mathcal{G}_k := \left\{\vec{x} \in G^k \mid \mathsf{H}_{\vec{x}} \neq H^k\right\}, \quad \eta_k = \frac{|\mathcal{G}_k|}{|G^k|} \ .$$

▶ **Lemma 9** (Rewriting the agreement). *Let* $G, H$ *be finite abelian groups, and let* $f : G \to H$ *be any function.*

$$\sum_{\varphi \in \mathrm{Hom}(G,H)} \mathrm{agr}\left(f,\varphi\right)^k \ = \ \eta_k \cdot \mathop{\mathbb{E}}_{\vec{x} \sim \mathcal{G}_k}\left[\mathbb{1}_{f(\vec{x}) \in \mathsf{H}_{\vec{x}}} |\ker(\Gamma_{\vec{x}})|\right] + (1-\eta_k) \cdot \frac{|\mathrm{Hom}(G,H)|}{|H^k|} \ .$$

**Proof.** See the full version for the proof. ◀

### General Test

Motivated by the non-constant term in the expression, we define the distribution on $\mathcal{G}_k$ which samples $x \propto |\ker(\Gamma_{\vec{x}})|$, i.e.,

$$\mathcal{D}_{\ker}(\vec{x}) \ := \ \frac{|\ker(\Gamma_{\vec{x}})|}{\sum_{\vec{x} \in \mathcal{G}_k} |\ker(\Gamma_{\vec{x}})|} \ .$$

Test_$\ker_k(G, H)$

- Sample $\vec{x} \sim \mathcal{D}_{\ker}$, i.e., $\vec{x} \in \mathcal{G}_k \propto |\ker(\Gamma_{\vec{x}})|$.
- If $f(\vec{x}) \in \mathsf{H}_{\vec{x}}$: return 1; otherwise: return 0.

▶ **Corollary 10** (Test passing Probability). *Let $f : G \to H$ and $\delta_k$ be the probability that $f$ passes the* Test_$\ker_k(G, H)$. *Then,*

$$\delta_k \;=\; \frac{\mathbb{E}_{\vec{x}\sim\mathcal{G}_k}[\mathbb{1}_{f(\vec{x})\in H_x}|\ker(\Gamma_{\vec{x}})|]}{\mathbb{E}_{\vec{x}\sim\mathcal{G}_k}[|\ker(\Gamma_{\vec{x}})|]} \quad .$$

*And therefore,*

$$\sum_{\varphi} \operatorname{agr}(f,\varphi)^k \;=\; \delta_k \cdot \eta_k \cdot \mathop{\mathbb{E}}_{\vec{x}\sim\mathcal{G}_k}[|\ker(\Gamma_{\vec{x}})|] \;+\; (1-\eta_k)\cdot\frac{\mathrm{Hom}(G,H)}{|H|^k}.$$

The following claim merely gives an alternate way to compute the term on the RHS of the above equation, i.e., the expected kernel size.

▷ Claim 11. For any finite groups $G, H$, and $k \geq 1$, we have

$$\gamma_k \;:=\; \sum_{\vec{x}\in G^k} |\ker(\Gamma_{\vec{x}})| \;=\; \sum_{\varphi\in\mathrm{Hom}(G,H)} |\ker(\varphi)|^k.$$

Proof. See the full version for the proof. ◁

### Summarizing the expressions

We now summarize the expressions we need for ready reference in our proofs.

$$\max_{\varphi} \operatorname{agr}(f,\varphi) \;\geq\; \frac{\sum_{\varphi}\operatorname{agr}(f,\varphi)^{k+1}}{\sum_{\varphi}\operatorname{agr}(f,\varphi)^{k}} \tag{3}$$

$$\sum_{\varphi} \operatorname{agr}(f,\varphi)^k \;=\; \mathop{\mathbb{E}}_{\vec{x}\sim G^k}\left[\mathbb{1}_{f(\vec{x})\in\mathsf{H}_{\vec{x}}}|\ker(\Gamma_{\vec{x}})|\right] \tag{4}$$

$$\;=\; \eta_k \cdot \mathop{\mathbb{E}}_{\vec{x}\sim\mathcal{G}_k}\left[\mathbb{1}_{f(\vec{x})\in\mathsf{H}_x}|\ker(\Gamma_{\vec{x}})|\right] + (1-\eta_k)\cdot\frac{|\mathrm{Hom}(G,H)|}{|H^k|} \tag{5}$$

$$\;=\; \delta_k \cdot \frac{\gamma_k}{|G|^k} + (1-\eta_k)\cdot\frac{|\mathrm{Hom}(G,H)|}{|H^k|}. \tag{6}$$

# 3 Cyclic Groups

## 3.1 Cyclic groups of prime power order to abelian groups of small rank

We will first start with both the domain being a cyclic group of prime power order. For such groups, the expression from Corollary 10 can be further simplified, as $\eta_k = 1$.

▶ **Observation 12.** *Let $G = \mathbb{Z}_{p^r}$ and $H$ be any abelian group. Then, for any $k \geq 2$, $\eta_k(G, H) = 1$ and thus, for any $f : G \to H$,*

$$\sum_{\varphi\in\mathrm{Hom}(G,H)} \operatorname{agr}(f,\varphi)^k \;=\; \delta_k(f)\cdot\frac{\gamma_k}{|G|^k} \quad .$$

**Proof.** See the full version for the proof. ◀

### Bounding $\gamma_k$

From the expression it is clear that the only quantity we need to analyze is $\gamma_k$ which we will do via Claim 11.

▶ **Lemma 13** (Cyclic to Abelian). *Let $G = \mathbb{Z}_{p^r}$ and $H$ any abelian group. Then,*

$$\gamma_k(G,H) \;=\; \big|\mathrm{Hom}(\mathbb{Z}_{p^r},H)\big| + (1-p^{-k})\sum_{a=1}^{r} p^{ak}\cdot\big|\mathrm{Hom}(\mathbb{Z}_{p^{r-a}},H)\big|.$$

**Proof.** See the full version for the proof. ◀

Note that due to Fact 7, any homomorphism maps $\mathbb{Z}_{p^r}$ only to a *p-group*. Since, $\gamma_k$ only concerns homomorphisms, it is only dependent on the $p$-component $H_p := \oplus_{i=1}^{t}\mathbb{Z}_{p^{b_i}}$. Here, $t$ is the $p$-rank of $H$. We now explicitly bound $\gamma_k$ for $k$ larger that the $p$-rank of $H$.

▶ **Corollary 14.** *Let $G = \mathbb{Z}_{p^r}$, and let $H$ be an abelian group of $p$-rank $t$, and let $k > t$. Then,*

$$(1-p^{-k})\cdot p^{kr} \;\le\; \gamma_k(G,H) \;\le\; \Big(\frac{p^{k-t}}{p^{k-t}-1}\Big)\cdot p^{kr}.$$

**Proof.** See the full version for the proof. ◀

We can now use the above calculation for $\gamma_k$ to deduce a testing result, and a (combinatorial) list decoding bound.

▶ **Theorem 15** (Testing prime power cyclic groups to Abelian groups of bounded rank). *Let $G = \mathbb{Z}_{p^r}$ be a cyclic group and $H$ be an abelian group of $p$-rank $t \ge 1$. Let $k \ge t+2$ be an integer, and let $f : G \to H$ be any function. Then if $f$ passes* Test_$\ker_k(G,H)$ *with probability $\delta_k$, then,*

$$\Big(\frac{(p-1)^2}{p^2}\cdot\delta_k\Big)^{\frac{1}{k-t-1}} \;\le\; \mathrm{agr}(f,\varphi) \;\le\; \Big(\frac{p^2}{p^2-1}\delta_k\Big)^{\frac{1}{k}}.$$

**Proof.** The upper bound directly follows from Observation 12 and Corollary 14. For the lower bound we use Equation (3) and Observation 12 to get,

$$\max_{\varphi}\mathrm{agr}(f,\varphi) \;\ge\; \frac{\sum_{\varphi}\mathrm{agr}(f,\varphi)^i}{\sum_{\varphi}\mathrm{agr}(f,\varphi)^{i-1}} \;\ge\; \frac{\delta_i\gamma_i}{|G|\delta_{i-1}\gamma_{i-1}}.$$

Multiplying this for $i \in [t+2,k]$, we get

$$\begin{aligned}
(\max_{\varphi}\mathrm{agr}(f,\varphi))^{k-t-1} &\ge \Big(\frac{1}{|G|}\Big)^{k-t}\cdot\frac{\delta_k\gamma_k}{\delta_{t+1}\gamma_{t+1}}\\
&\ge \Big(\frac{1}{|G|}\Big)^{k-t-1}\cdot\frac{\delta_k\gamma_k}{\gamma_{t+1}} && [\delta_{t+1}\le 1]\\
&\ge \delta_k\cdot\frac{(1-p^{-k})(p-1)}{p} && [\text{Using Corollary 14}]\\
&\ge \delta_k\cdot\frac{(p-1)^2}{p^2}
\end{aligned}$$

◀

Using the above bound we also immediately get a list decoding bound.

▶ **Theorem 16** (List Size Bound). *Let $G = \mathbb{Z}_{p^r}$ be a cyclic group and $H$ be an abelian group of $p$-rank $t \geq 1$. Let $f : G \to H$ be any function. Then the following holds:*

$$|\{\varphi \in \mathrm{Hom}(G,H) \ : \ \mathrm{agr}(f,\varphi) \ \geq \ \varepsilon\}| \ \leq \ \left(\frac{p}{p-1}\right) \cdot \frac{1}{\varepsilon^{t+1}}.$$

*In particular, we get a list size bound of $\frac{2}{\varepsilon^2}$ for homomorphisms between cyclic groups.*

**Proof.** Let $N = |\{\varphi \in \hom(G,H) \ : \ \mathrm{agr}(f,\varphi) \ \geq \ \varepsilon\}|$. Then,

$$\begin{aligned} N\varepsilon^{t+1} \ \leq \ \sum_{\varphi} \alpha_{\varphi}^{t+1} \ &= \ \frac{\delta_{t+1}\gamma_{t+1}}{|G|^{t+1}} \\ &\leq \ \frac{p}{p-1} \qquad \text{[Using Corollary 14].} \end{aligned}$$

◀

## 3.2 Arbitrary Cyclic groups

To handle general cyclic groups, we will use the decomposition of abelian groups into their $p$-components.

▶ **Lemma 17** (Reduction to p-groups). *Let $\varphi : G \to H$, and let $X = \oplus_p X_p$ for $X \in \{G, H\}$ be the decomposition of the groups into their $p$-components. Then, $\varphi = \oplus \varphi_p$ where $\varphi_p : G_p \to H_p$. Therefore,*

$$\begin{aligned} \gamma_k(G,H) \ &= \ \prod_p \gamma_k(G_p, H_p), \\ 1 - \eta_k(G,H) \ &= \ \prod_p (1 - \eta_k(G_p, H_p)). \end{aligned}$$

**Proof.** See the full version for the proof. ◀

▶ **Definition 18** (Riemann Zeta Function). *Define the Riemann zeta function using Euler's product formula as $\zeta(s) = \prod_p (1 - \frac{1}{p^s})^{-1}$ where the product runs over all primes.*

▶ **Proposition 19.** *Let $G, H$ be any cyclic groups and let $k \geq 3$. Denote by $\zeta()$, the Riemann zeta function. Then,*

$$|G|^k \ \leq \ \gamma_k(G,H) \ \leq \ |G|^k \cdot \zeta(k-1)^2.$$

**Proof.** See the full version for the proof. ◀

▶ **Theorem 20** (Testing $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$). *Let $G, H$ be any cyclic groups and $f : G \to H$ be any function. Let $k \geq 4$ be any integer. Then if $f$ passes* Test_$\ker_k(G,H)$ *with probability $\delta_k$, then there exists a homomorphism $\varphi \in \mathrm{Hom}(G,H)$ such that $\mathrm{agr}(f,\varphi) \ \geq \ \left(\zeta(2)^2 \cdot \delta_k\right)^{\frac{1}{k-3}}$.*

**Proof.** By Lemma 17, $\eta(G,H) = 1$ for any pair of cyclic groups, and thus, the expression from Observation 12 holds. Using it,

$$\max_{\varphi} \mathrm{agr}(f,\varphi) \ \geq \ \frac{\sum_{\varphi} \mathrm{agr}(f,\varphi)^i}{\sum_{\varphi} \mathrm{agr}(f,\varphi)^{i-1}} \ \geq \ \frac{\delta_i \gamma_i}{|G| \delta_{i-1} \gamma_{i-1}}.$$

Multiplying this for $i \in [4, k]$, we get

$$\begin{aligned}
(\max_{\varphi} \operatorname{agr}(f,\varphi))^{k-t-1} &\geq \left(\frac{1}{|G|}\right)^{k-t} \cdot \frac{\delta_k \gamma_k}{\delta_{t+1}\gamma_{t+1}} \\
&\geq \left(\frac{1}{|G|}\right)^{k-t-1} \cdot \frac{\delta_k \cdot \gamma_k}{\gamma_{t+1}} && [\delta_{t+1} \leq 1] \\
&\geq \delta_k \cdot \frac{(1-p^{-k})(p-1)}{p} && [\text{Using Corollary 14}] \\
&\geq \delta_k \cdot \frac{(p-1)^2}{p^2}\,. && \blacktriangleleft
\end{aligned}$$

# 4 Vector space over finite fields

Let, $\mathbb{F}_q$ be a finite field of order $q$. In this section, we will focus on functions between a $\mathbb{F}_q$-vector space and the finite field, $\mathbb{F}_q$.

## 4.1 Vector space to Finite Field

Let, $G = \mathbb{F}_q^n$ and $H = \mathbb{F}_q$. Let $f : G \to H$ be an arbitrary function.

### A shifted variant of agreement

We first recall the expression for $\sum_{\varphi} \operatorname{agr}(f,\varphi)^k$ from Section 2.

$$\sum_{\varphi \in \operatorname{Hom}(G,H)} \operatorname{agr}(f,\varphi)^k \;=\; \delta_k \cdot \eta_k \cdot \mathop{\mathbb{E}}_{\vec{x}\sim\mathcal{G}_k}[|\ker(\Gamma_{\vec{x}})|] \;+\; (1-\eta_k) \cdot \frac{\operatorname{Hom}(G,H)}{|H|^k},$$

where $\delta_k$ is the test passing probability of the general test (that samples $\vec{x} \propto |\ker \Gamma_{\vec{x}}|$ and checks $\mathbb{1}_{f(\vec{x})\in \mathsf{H}_{\vec{x}}}$) given in Section 2. A key difference in the vector space case compared to the cyclic case is that $\eta_k \approx 0$. Therefore most of the contribution in $\sum_{\varphi\in\operatorname{Hom}(G,H)} \operatorname{agr}(f,\varphi)^k$ comes from the non-test part: $\operatorname{Hom}(G,H) \cdot H^{-k}$. This happens because any function has roughly $\frac{1}{q}$-agreement with many homomorphisms (at least $\frac{1}{2q}$-fraction of all homomorphisms). In particular, it is easy to see that if $f$ is a random function then it has $\frac{1}{q}$-agreement with almost all the homomorphisms. This suggests adjusting the definition of agreement, $\operatorname{agr}(f,\varphi)$, so that it measures the non-trivial advantage over the trivial agreement of $\frac{1}{q}$. To achieve this we define the following shifted variant of $\operatorname{agr}(f,\varphi)$.

**Shifted agreement:** $\widetilde{\operatorname{agr}}(f,\varphi) = \dfrac{q\operatorname{agr}(f,\varphi) - 1}{q-1}$

Accordingly, we will use the expression $\sum_{\varphi} \widetilde{\operatorname{agr}}(f,\varphi)^k$ instead of $\sum_{\varphi} \operatorname{agr}(f,\varphi)^k$ so that distribution concentrates on homomorphisms with non-trivial agreements. Fortunately, the former expression can be directly computed from the latter via binomial expansion.

### Refining the test

We need to address one more issue in this vector space setting. We cannot directly use the original generalized test that - samples $\vec{x}$ with probability $\propto |\ker \Gamma_{\vec{x}}|$ and checks $f(\vec{x}) \in \mathsf{H}_{\vec{x}}$. This is because even though this test uses length $k$-tuple, it can happen that sampled the tuple satisfy only linear relation involving $j$ (for some $j < k$) co-ordinates of the input and

all the rest of the co-ordinates are independent. If this happens, then the test essentially collapses to a $j$-th level test involving $j$-length tuple - as it essentially checks if $f$ satisfy that linear relation or not. In other words, the generalized test is a linear combination of such different tests associated with different levels. For a precise analysis, it is crucial to refine the initial test definition and isolate these different tests. To do this, we need to formalize this notion of *tuples satisfiying a linear relation involving $j$-coordinates*.

▶ **Definition 21** (A level-$j$ distribution). *We define $\mathcal{R}_j$ to be the set of tuples $\vec{x} \in G^k$ such that (1) there exist $\emptyset \neq S \subseteq [k]$ with $|S| = j$ such that $\sum_{\ell \in S} a_\ell x_\ell = 0$ for non-zero coefficients $\{a_\ell\}_{\ell \in S}$ and (2) vectors in $\vec{x}$ do not satisfy any other linear relation.*

Observe that the sets $\mathcal{R}_j$ for distinct $j$ are disjoint. Now we collect all the claims involving $\mathcal{R}_j$ and linear independence of tuples, that will be needed for our analysis. For any two quantities, $\mathsf{t}_1$ and $\mathsf{t}_2$ : we write $\mathsf{t}_1 \approx_\varepsilon \mathsf{t}_2$ if $|\mathsf{t}_1 - \mathsf{t}_2| = O(\varepsilon)$. Our first claim is the following:

▷ Claim 22. Let, $k \geq 1$ be any integer such that $k = O_n(1)$. Then it holds that,

1. $\Pr_{\vec{x} \sim G^k}[\mathrm{rank}(\vec{x}) = k] \approx_{q^{-2n}} \left(1 - \frac{q^k - 1}{q^n(q-1)}\right)$.
2. $\Pr_{\vec{x} \in G^k}[\vec{x} \in \mathcal{R}_j] \approx_{q^{-2n}} \binom{k}{j} \frac{(q-1)^{j-1}}{q^n}$.

Proof. See the full version for the proof. ◁

▷ Claim 23. Let, $1 \leq j \leq k$ be two integers. Then,

$$\mathop{\mathbb{E}}_{\vec{x} \sim G^k}\left[\mathbb{1}_{f(\vec{x}) \in \mathsf{H}_{\vec{x}}} | \vec{x} \in \mathcal{R}_j\right] \;=\; \mathop{\mathbb{E}}_{\vec{x} \sim G^j}\left[\mathbb{1}_{f(\vec{x}) \in \mathsf{H}_{\vec{x}}} | \vec{x} \in \mathcal{R}_j\right] .$$

Proof. See the full version for the proof. ◁

### Analyzing the key expression

Let us now examine the expression for $\sum_\varphi \mathrm{agr}\,(f, \varphi)^k$, from which the appropriate definition of the test becomes apparent.

▷ Claim 24. Let, $k \geq 1$ be any integer, and $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be any function. Then,

$$\sum_{\varphi} \mathrm{agr}\,(f, \varphi)^k \;\approx_{q^{-n}}\; \Pr_{\vec{x} \sim G^k}[\mathrm{rank}(\vec{x}) = k] \cdot q^{n-k} + q^{-(k-1)} \cdot \sum_{j=1}^{k} \binom{k}{j} (q-1)^{j-1} \delta_j(f) \;,$$

where $\delta_j(f) \;:=\; \mathbb{E}_{\vec{x} \sim G^j}[\mathbb{1}_{f(\vec{x}) \in \mathsf{H}_{\vec{x}}} | \vec{x} \in \mathcal{R}_j]$.

Proof. See the full version for the proof. ◁

### Defining the refined test

Inspired from Claim 24 we define a $k^{\text{th}}$ test such that the test passing probability of a function $f$ is $\delta_k(f)$ as above, i.e.,

$$\delta_k(f) := \mathop{\mathbb{E}}_{\vec{x} \in G^k}\left[\mathbb{1}_{f(\vec{x}) \in \mathsf{H}_{\vec{x}}} | \vec{x} \in \mathcal{R}_k\right].$$

**Test_VSpace$_k(f)$**

- Sample $(x_1, \ldots, x_k) \sim \mathcal{R}_k$.
- If $(f(x_1), \ldots, f(x_k)) \in \mathsf{H}_{\vec{x}}$: return 1; otherwise: return 0

Or equivalently,

- Sample $k-1$ independent vectors: $x_1, \ldots, x_{k-1}$.
- Sample $a_1, \ldots, a_{k-1} \sim \mathbb{F}_q \setminus \{0\}$ and set $x_k = \sum_i^{k-1} a_i x_i$
- If $f(x_k) = a_1 f(x_1) + a_2 f(x_2) + \cdots + a_{k-1} f(x_{k-1})$ : return 1; otherwise: return 0

### Analysis of the Test

We state a simple combinatorial fact that we will need.

▶ **Fact 25** (Binomial Identity). *Let $0 \le j < k$ be any integers. Then,*

$$\sum_{i=j}^{k} (-1)^{k-i} \binom{k}{i} \binom{i}{j} \;=\; 0\,.$$

**Proof.** A direct corollary of the fact that $\binom{k}{i}\binom{i}{j} = \binom{k}{j}\binom{k-j}{i-j}$. ◀

▶ **Corollary 26.** *Let $k \ge 1$ be any integer.*

$$\sum_{\varphi} \widetilde{\mathrm{agr}}(f,\varphi)^k \;\approx_{q^{-n}}\; \frac{1}{q-1}(q\delta_k - 1).$$

**Proof.** See the full version for the proof. ◀

▶ **Theorem 27.** *Let $G = \mathbb{F}_q^n$ be a vector space and $H = \mathbb{F}_q$ for some finite field of order $q$. Let $k \ge 3$ be any odd integer. Then if $f$ passes* Test_VSpace$_k(f)$ *with probability $\delta_k > \frac{1}{q}$, then,*

$$\frac{1}{q} + \Big(\frac{q-1}{q}\Big)\Big(\frac{q\delta_k - 1}{q-1}\Big)^{\frac{1}{k-2}} \;\le\; \max_{\varphi} \mathrm{agr}(f,\varphi) \pm O(q^{-n}) \;\le\; \frac{1}{q} + \Big(\frac{q-1}{q}\Big)\Big(\frac{q\delta_k - 1}{q-1}\Big)^{\frac{1}{k}}.$$

**Proof.** The upper bound is a direct consequence of Corollary 26. For the lower bound, let $k \ge 3$ be an odd integer,

$$\max_{\varphi} \widetilde{\mathrm{agr}}(f,\alpha)^{k-2} \cdot \sum_{\varphi} \widetilde{\mathrm{agr}}(f,\varphi)^2 \;\ge\; \sum_{\varphi} \widetilde{\mathrm{agr}}(f,\alpha)^k \;\ge\; \frac{1}{q-1}(q\delta_k - 1)\,.$$

Here, the second inequality follows from Corollary 26 and the test passing assumption. Thus, there exists a homomorphism $\varphi$ such that

$$\Big(\frac{q \cdot \mathrm{agr}\,(f,\varphi) - 1}{q-1}\Big)^{k-2} \;\ge\; \frac{1}{q-1}(q\delta_k - 1)\,.$$ ◀

Since $k-2$ is odd, this implies that we can take the positive $(k-2)^{\text{th}}$-root on either side of the inequality and obtain our result.

## 4.2 Finite Field to Vector Space

Let, $\mathbb{F}_q$ be a finite field of order $q$. Let, $G = \mathbb{F}_q$ and $H = \mathbb{F}_q^n$. Let $f : G \to H$ be an arbitrary function. The set of homomorphisms, $\mathrm{Hom}(G, H)$, have the property that for every non-trivial homomorphism $\varphi$, $\ker(\varphi) = \{0\}$. This property implies that no two homomorphisms agree on any non-zero input $x$. We note a simple consequence of this below.

▶ **Observation 28.** *Let $k \geq 1$ and $\vec{x} \in \mathbb{F}_q^k \setminus \{\vec{0}\}$ be a non-zero vector. Then,* $\ker(\Gamma_{\vec{x}}) = \{\mathrm{triv}\}$.

**Proof.** Let $x_i \neq 0$ be any non-zero element in the tuple, $\vec{x}$. Then, for any non-trivial homomorphism $\varphi \in \mathrm{Hom}(\mathbb{F}_q, \mathbb{F}_q^n)$, $\varphi(x_i) \neq 0$ and thus $\varphi \notin \ker(\Gamma_{\vec{x}})$. ◀

Recall the general version of the test which samples $\vec{x} \in G^k \propto |\ker \Gamma_{\vec{x}}|$. This is problematic in our case as for $\vec{x} = 0$, we have $|\ker \Gamma_{\vec{0}}| = q^n$, but $\ker(\Gamma_{\vec{x}}) = 1$ for every other vector $\vec{x}$. We circumvent this issue by simply ignoring the 0 element in $G$ and working over $\widetilde{G} = \mathbb{F}_q^*$, the set of non-zero elements of $\mathbb{F}_q$. Accordingly, we will work with the fractional agreement of $f$ over $\tilde{G}$,

$$\widetilde{\mathrm{agr}}(f, \varphi) := \mathop{\mathbb{E}}_{x \sim \widetilde{G}}\left[\mathbb{1}_{f(x)=\varphi(x)}\right].$$

Using this modified agreement, $\widetilde{\mathrm{agr}}(f, \varphi)$, we have the following claim.

▶ **Lemma 29** (A variant of Lemma 9). *Let $f : G \to H$ to be any function. Then, for any $k \geq 1$,*

$$\sum_{\varphi \in \mathrm{Hom}(\mathbb{F}_q, \mathbb{F}_q^n)} \widetilde{\mathrm{agr}}(f, \varphi)^k \;=\; \mathop{\mathbb{E}}_{\vec{x} \sim \widetilde{G}^k}\left[\mathbb{1}_{f(\vec{x}) \in \mathsf{H}_{\vec{x}}}\right].$$

**Proof.** Identical to the proof of Lemma 9, after using Observation 28. ◀

The expression in Lemma 29 suggests the following simple test.

**Test_NonZero$_k(f)$**

- Sample $\vec{x} \sim \widetilde{G}^k$ uniformly.
- If $f(\vec{x}) \in \mathsf{H}_{\vec{x}}$: return 1; otherwise: return 0.
- Equivalently, the test passes only if $x_i^{-1} f(x_i) = x_j^{-1} f(x_j)$ for every $x_i, x_j$ in the sampled tuple $\vec{x}$.

▶ **Theorem 30.** *Let $G = \mathbb{F}_q$ some finite field of order $q$ and $H = \mathbb{F}_q^n$ be a vector space. Let, $k \geq 2$ be any integer. Then if $f : G \to H$ passes* Test_NonZero$_k(f)$ *with probability $\delta_k$, then,*

$$\left(1 - \frac{1}{q}\right) \cdot \delta_k^{\frac{1}{k-1}} \;\leq\; \max_{\varphi} \mathrm{agr}(f, \varphi) \;\leq\; \frac{1}{q} + \left(\frac{q-1}{q}\right) \cdot \delta_k^{\frac{1}{k}} \;.$$

**Proof.** From the definition of the shifted agreement, we have, for any $\varphi$

$$\mathrm{agr}\,(f, \varphi) \;\leq\; \frac{1}{q} + \frac{q-1}{q} \cdot \widetilde{\mathrm{agr}}(f, \varphi).$$

Since, $\max_\varphi \widetilde{\mathrm{agr}}(f, \varphi)^k \;\leq\; \sum_\varphi \widetilde{\mathrm{agr}}(f, \varphi)^k \;=\; \delta_k$, we get the upper bound. We have,

$$\max_{\varphi}\{\widetilde{\mathrm{agr}}(f, \varphi)^{k-1}\} \cdot \sum_{\varphi} \widetilde{\mathrm{agr}}(f, \varphi) \;\geq\; \sum_{\varphi} \widetilde{\mathrm{agr}}^k(f, \varphi) \;=\; \delta_k \;.$$

From Lemma 29 for $k = 1$, we get $\sum_\varphi \widetilde{\mathrm{agr}}_\varphi \leq 1$. Clearly, this quantity is greater than 0, as otherwise the above inequality forces $\delta_k = 0$ for which the theorem trivially holds. Thus, we have the inequality,

$$\widetilde{\mathrm{agr}}(f,\varphi) \;\geq\; \delta_k^{\frac{1}{k-1}}.$$

Finally, by rescaling we get or result:

$$\mathrm{agr}\,(f,\varphi) \;\geq\; \frac{|\tilde{G}|}{|G|}\cdot \widetilde{\mathrm{agr}}(f,\varphi) \;=\; \left(1-\frac{1}{q}\right)\cdot \delta_k^{\frac{1}{k-1}}. \qquad \blacktriangleleft$$

## 5 Automorphism testing for Non-Abelian groups

We mention the main results of this section below. Please see the full version for the remainder of the section.

▶ **Theorem 31** (Testing $\mathrm{Aut}(D_{2p})$ )**.** *Let $G = D_{2p}$ be the dihedral group of order $2p$ for some prime $p > 3$. Let $k \geq 3$ be an integer, and $f : G \to G$ be any function. Then if $f$ passes* $\mathsf{Test\_Dihedral}_k$ *with probability $\delta_k(f)$, then there exists a automorphism $\varphi \in \mathrm{Aut}(G)$ such that $\mathrm{agr}(f,\varphi) \;\geq\; \frac{1}{2}\cdot\delta_k(f)^{\frac{1}{k-2}}$ .*

▶ **Theorem 32** (Restatement of Theorem 1.4)**.** *The following results hold using* $\mathsf{Test\_Inner}_k$ :

- *For any $n \neq 6$, $\mathrm{Aut}(\mathrm{Sym}_n)$ is $\left(k,\, \delta,\, \delta^{\frac{1}{k-2}} - o_n(1)\right)$-testable for every $k \geq 3$.*
- *For every non-abelian finite simple group $G$, $\mathrm{Inn}(G)$ is $\left(k,\, \delta,\, \delta^{\frac{1}{k-5}} - o_{|G|}(1)\right)$-testable for every $k \geq 6$.*
- *For any exstraspecial group $G$ of order $p^r$, $\mathrm{Inn}(G)$ is $\left(k,\, \delta,\, \delta^{\frac{1}{k-r}} - o_p(1)\right)$-testable for every $k \geq r+1$. In particular, for the family of Heisenberg groups over $\mathbb{F}_p$, $H_p$, $\mathrm{Inn}(H_p)$ is $\left(k,\, \delta,\, \delta^{\frac{1}{k-3}} - o_p(1)\right)$-testable for any $k \geq 4$.*
- *Alternatively, if $p = O(1)$ is fixed and $r \to \infty$, then we have that $\mathrm{Inn}(G)$ is $\left(k,\, \delta,\, \frac{1}{p}\delta^{\frac{1}{k-1}}\right)$-testable for every $k \geq 2$, and $r \geq 3$.*

*Additionally, we get an upper bound of $\max_\varphi \mathrm{agr}\,(f,\varphi) \leq 2\delta^{\frac{1}{k}}$, for any group $G$ and $k$ as above.*

## 6 Lifting Homomorphism Tests

We mention the main results of this section below. Please see the full version for the remainder of the section.

▶ **Theorem 33** (Character Testing for $\mathrm{GL}_n(q)$)**.** *Let $G = \mathrm{GL}_n(q)$ be the group of inverible $n \times n$ matrices over $\mathbb{F}_q$ for $q > 2, n \geq 2$. Let $f : G \to \mathbb{F}_q^*$ be any function and fix an integer $k \geq 4$. Then if $f$ passes* $\mathsf{Test}_k$ *with probability $\delta_k$, there exists a character $\varphi \in \mathrm{Hom}(\mathrm{GL}_n(q), \mathbb{F}_q^*)$ such that $\mathrm{agr}(f,\varphi) \;\geq\; \left(\zeta(2)^2\cdot\delta_k\right)^{\frac{1}{k-3}}$.*

▶ **Theorem 34.** *For any $k \geq 3$,* $\mathsf{Test\_LiftedVSpace}_k$ *is a $(k,\delta,\varepsilon(\delta))$ sound test for $\mathrm{Hom}(G,\mathbb{F}_p)$ for any finite group $G$ and prime $p$, and for $\mathrm{LieHom}(\mathfrak{g},\mathbb{F}_q)$ for any finite-dimensional Lie algebra, $\mathfrak{g}$, and prime power $q$.*

▶ **Theorem 35** (Character Testing for $\mathfrak{gl}_n(q)$)**.** *Let $q$ be a power of a prime $p$, and let $\mathfrak{g} = \mathfrak{gl}_n(q) = \mathbb{F}_q^{n\times n}$, be the space of $n \times n$-matrices. Let $k \geq 3$ be an integer. Let $f : \mathfrak{g} \to \mathbb{F}_q$ be any function. If $f$ passes $\mathsf{Test}_k(G, H, \mathcal{D}_k)$ with probability $\delta_k$, then,*

$$\max_{\varphi\in \mathrm{Hom}(\mathfrak{g},\mathbb{F}_q)} \mathrm{agr}(f,\varphi) \;\geq\; \left(\frac{(p-1)^2}{p^2}\cdot\delta_k\right)^{\frac{1}{k-1}}.$$

## References


1 László Babai, Katalin Friedl, and András Lukács. Near representations of finite groups, 2003. Manuscript.

2 M. Bellare, D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan. Linearity testing in characteristic two. In *Proceedings of the 36th IEEE Symposium on Foundations of Computer Science*, pages 432–441, 1995.

3 Michael Ben-Or, Don Coppersmith, Mike Luby, and Ronitt Rubinfeld. Non-Abelian homomorphism testing, and distributions close to their self-convolutions. *Random Structures & Algorithms*, 32(1):49–70, August 2007. doi:10.1002/rsa.20182.

4 Eli Ben-Sasson, Madhu Sudan, Salil P. Vadhan, and Avi Wigderson. Randomness-efficient low degree tests and short PCPs via $\varepsilon$-biased sets. In *Proceedings of the 35th ACM Symposium on Theory of Computing*, pages 612–621, 2003. doi:10.1145/780542.780631.

5 Amey Bhangale and Subhash Khot. Optimal inapproximability of satisfiable k-LIN over non-abelian groups. In *Proceedings of the 53rd ACM Symposium on Theory of Computing*, 2021. doi:10.1145/3406325.3451003.

6 M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proceedings of the 22nd ACM Symposium on Theory of Computing*, pages 73–83, 1990. doi:10.1145/100216.100225.

7 Robin Chapman. Image of a fixed element under a random endomorphism in an abelian group. MathOverflow, 2010. URL:https://mathoverflow.net/q/30378 (version: 2010-07-04).

8 Irit Dinur, Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Decodability of group homomorphisms beyond the Johnson bound. In *Proceedings of the 40th ACM Symposium on Theory of Computing*, pages 275–284, 2008. doi:10.1145/1374376.1374418.

9 Irit Dinur, Madhu Sudan, and Avi Wigderson. Robust local testability of tensor products of LDPC codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 304–315. Springer Berlin Heidelberg, 2006. doi:10.1007/11830924_29.

10 Parikshit Gopalan. A Fourier-Analytic Approach to Reed-Muller Decoding. *IEEE Trans. Inf. Theory*, 59(11):7747–7760, 2013. doi:10.1109/TIT.2013.2274007.

11 W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of marton, 2023. arXiv:2311.05762.

12 William Timothy Gowers and Omid Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784, 2017. doi:10.1070/SM8872.

13 Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Local decoding and testing for homomorphisms. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 375–385. Springer, 2006. doi:10.1007/11830924_35.

14 Alan Guo and Madhu Sudan. List Decoding Group Homomorphisms Between Supersolvable Groups. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, 2014. doi:10.4230/LIPIcs.APPROX-RANDOM.2014.737.

15 Johan Håstad and Avi Wigderson. Simple analysis of graph tests for linearity and PCP. *Random Structures & Algorithms*, 22(2):139–160, 2003. doi:10.1002/rsa.10068.

16 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *Commun. ACM*, 64(11):131–138, 2021. doi:10.1145/3485628.

17 M. Kiwi. Algebraic testing and weight distributions of codes. *Theoretical Computer Science*, 299(1):81–106, 2003. doi:10.1016/S0304-3975(02)00816-2.

**18** Tushant Mittal and Sourya Roy. Derandomized Non-Abelian Homomorphism Testing in Low Soundness Regime, 2024. doi:10.48550/arXiv.2405.18998.

**19** Cristopher Moore and Alexander Russell. Approximate representations, approximate homomorphisms, and low-dimensional embeddings of groups. *SIAM Journal on Discrete Mathematics*, 29(1):182–197, 2015. doi:10.1137/140958578.

**20** Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th ACM Symposium on Theory of Computing*, 2017. doi:10.1145/3055399.3055468.

**21** Kenta Oono and Yuichi Yoshida. Testing properties of functions on finite groups. *Random Structures & Algorithms*, 49(3):579–598, February 2016. doi:10.1002/rsa.20639.

**22** Michal Parnas, Dana Ron, and Ronitt Rubinfeld. Tolerant property testing and distance approximation. *Journal of Computer and System Sciences*, 72(6):1012–1042, 2006. doi:10.1016/J.JCSS.2006.03.002.

**23** A. Samorodnitsky. Low-degree tests at large distances. In *Proceedings of the 39th ACM Symposium on Theory of Computing*, 2007.

**24** Tom Sanders. On the Bogolyubov-Ruzsa lemma. *Analysis & PDE*, 5(3), 2012. doi:10.2140/apde.2012.5.627.

**25** Irving E. Segal. The automorphisms of the symmetric group. *Bull. Am. Math. Soc.*, 46:565, 1940. doi:10.1090/S0002-9904-1940-07261-1.