# Derandomized Non-Abelian Homomorphism Testing in Low Soundness Regime

Tushant Mittal[*] Sourya Roy[†]

We give a randomness-efficient homomorphism test in the low soundness regime for functions, $f : G \to \mathbb{U}_t$, from an arbitrary finite group $G$ to $t \times t$ unitary matrices. We show that if such a function passes a derandomized Blum–Luby–Rubinfeld (BLR) test (using small-bias sets), then (i) it correlates with a function arising from a genuine homomorphism, and (ii) it has a non-trivial Fourier mass on a low-dimensional irreducible representation.

In the full randomness regime, such a test for matrix-valued functions on finite groups implicitly appears in the works of Gowers and Hatami [Sbornik: Mathematics '17], and Moore and Russell [SIAM Journal on Discrete Mathematics '15]. Thus, our work can be seen as a near-optimal derandomization of their results. Our key technical contribution is a "degree-2 expander mixing lemma" that shows that Gowers' $U^2$ norm can be efficiently estimated by restricting it to a small-bias subset. Another corollary is a "derandomized" version of a useful lemma due to Babai, Nikolov, and Pyber [SODA'08].

## 1 Introduction

An important problem in theoretical computer science is to efficiently test if a function $f : G \to H$ is correlated with some homomorphism between groups $G$ and $H$. Such tests are widely used in constructions of *probabilistically checkable proofs* (PCPs), hardness of approximation, locally testable codes, and many other areas of computer science. Recently, there has been an interest in studying such tests for non-abelian groups. For example, in quantum complexity, *entanglement testing* [NV17] involves homomorphism testing over the (non-Abelian) Pauli group, which played an important role in the proof of MIP*=RE [JNV$^+$21]. Additionally, such non-Abelian tests have been used for constructions of better PCPs [BK21], and hardness of approximation results [BKM22].

The famous three-query randomized Blum–Luby–Rubinfield [BLR90] (BLR) test is as follows: pick two uniformly random group elements $x, y \in G$ and check if the homomorphism property holds for this pair, namely, if $f(x)f(y) = f(xy)$. This simple local test surprisingly sheds light on a global property of the function: if a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ passes the test with non-trivial probability, then the function must have a non-trivial correlation with some homomorphism.

[*] University of Chicago. tushant@uchicago.edu. Supported by NSF grant CCF-2326685.

[†] The University of Iowa. sourya-roy@uiowa.edu.

This test can be used for any pair of groups $G, H$ (assuming that one can sample from $G$), and requires $2\log|G|$ random bits. A randomness-efficient version of the test that has been studied is the *derandomized BLR test* wherein $x$ is uniformly sampled from $G$ as before, but $y$ is chosen from a sparse pseudorandom set $S \subseteq G$. If $S$ is constant-sized, then the randomness is reduced to $\log|G| + O(1)$, which is almost optimal.

The study of such derandomized linearity (and low-degree) tests has found significant applications, particularly in the development of Probabilistically Checkable Proofs (PCPs). For example, the derandomization results in [BSVW03] have enabled the construction of PCPs and Locally Testable Codes of nearly linear size. Additionally, derandomized parallel execution [ST00, HW03] of the BLR test has facilitated the creation of PCPs with low amortized costs. We extend this study of derandomized tests and investigate the question,

*Given a function $f : G \to H$ that passes the derandomized BLR test with probability $\delta$, what can one conclude about the function $f$?*

An ideal conclusion would be that the function $f$ is close to a true homomorphism $\varphi$ in some metric, i.e., $\|f - \varphi\| \le \theta(\delta)$. This is achievable in the "99%-regime", when the test passing probability, $\delta$, is close to 1. This is also called the *unique-decoding regime*, as there is a unique homomorphism, $\varphi$, near the given function, $f$. The unique homomorphism can often be constructed via a *majority decoding procedure*. There are many results in this setting [BCH+95, Far00, BP18] including derandomized ones [SW04]. In particular, for any finite group $G$ and an arbitrary (not necessarily finite) group $H$, [Far00] constructs a homomorphism close in Hamming metric to the given function $f$, if the test passing probability is $\ge 10/11$.

However, the situation is significantly more complex in the low-soundness or "1%-regime", wherein the function performs barely better than a random function, i.e., the test passing probability is $\frac{1}{|H|} + \delta$. Firstly, one cannot always hope to find a homomorphism close in the Hamming metric. A folklore counterexample due to Coppersmith (also in [BOCLR07]) gives a function $f : \mathbb{Z}_{3^k} \to \mathbb{Z}_{3^{k-1}}$ that passes the test with probability $2/9$ but it is far away from every homomorphism in the Hamming metric. More interestingly, for some pair of groups $G, H$, the only homomorphism from $G \to H$ might be the trivial one. In this case, we might not be able to conclude that $f$ is close to the trivial homomorphism but still deduce something about the global structure of $f$. To do so, however, we need to have a better understanding of how the set of functions from $G$ to $H$, relates to the set of homomorphisms. For instance, Fourier analysis yields that any function $f : \mathbb{Z}_2^n \to \mathbb{C}$ can be expressed as a linear combination of homomorphisms. In general, *representation theory* gives a similar relation for the more general setting of functions $f : G \to \mathbb{U}_t$, where $G$ is any finite group, and $\mathbb{U}_t$ is the group of $t \times t$ unitary matrices. This setting is, therefore, a natural starting point to start investigating the general question of derandomized testing for non-abelian groups. Moreover, this setting (which we work with throughout our paper) has interesting connections to quantum linearity testing!

### 1.1 Our Setup: Matrix-valued functions

We will work with functions from an arbitrary finite group $G$ to the group of $t \times t$ unitary matrices, $f : G \to \mathbb{U}_t$, and will use the following inner product to measure correlation, i.e., $\langle f, g\rangle_{\text{tr}} = \mathbb{E}_{x\sim G}[\text{tr}(g^*(x)f(x))]$. We wish to design a randomness-efficient variant of BLR such that if a function $f : G \to \mathbb{U}_t$ passes such a test, then the function $f$ correlates with a homomorphism, or a functions arising from a homomorphism.

This setting has been studied in prior works [MR15, NV17, GH17], most importantly in the context of quantum low-degree tests. The results of [MR15] and [GH17] are particularly relevant to our result, and we will discuss them in detail shortly. The other result by Natarajan and Vidick [NV17] gives a BLR-like test for homomorphism testing of functions, $f : \mathcal{P}^n \to \mathbb{U}_t$ where $\mathcal{P}^n$ is the $n$-fold tensor product of the *Pauli group* (also known as the *Weyl-Heisenberg* group). This was initially developed for entanglement testing [NV17], and later became a crucial component in the $\text{MIP}^* = \text{RE}$ proof [JNV+21].

While our setting encompasses their setup and has identical notions of correlation, our results do not directly apply to the quantum linearity test. This is because their test works with a specific presentation of the Pauli group due to additional constraints related to quantum measurements. Nevertheless, there might be interesting connections between our results and those in quantum homomorphism testing.

Before we state our results, we very briefly define some relevant concepts and discuss the challenges associated with this setting. See Section 2 for detailed definitions.

A *group representation* is a pair $(\rho, V)$ where $\rho : G \to \mathbb{U}_V$ is a homomorphism from the group $G$ to the group of unitary operators on the complex Hilbert space $V$. If Vis idendified with $\mathbb{C}^t$, we use the notation, $\mathbb{U}_t$. Every finite group $G$ has a finite set of *irreducible representations* (irreps) $\widehat{G}$, which are the building blocks of complex-valued functions on $G$. In the case of Abelian groups, all the irreducible representations are one-dimensional and given by the Fourier characters. These characters also form an orthogonal basis for the space of complex-valued functions. For general finite groups, the orthogonal basis is given by the set of matrix coefficients of irreps, i.e., $\left\{\rho(x)_{i,j} \mid \rho \in \widehat{G}\ i, j \leq \dim(\rho)\right\}$. Just as in the Abelian case, we use $\hat{f}(\rho) = \mathbb{E}_x[f(x)\rho(x)]$ to represent the coefficient corresponding to irrep $\rho$, which is now a matrix. Such a basis also exists for matrix-valued functions, $f : G \to \mathbb{C}^{t\times t}$, which is a collection of $t^2$ scalar functions.

#### 1.1.1 Challenges with this general setting

This general setting has three key differences with the original setting of BLR $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$: (i) $G$ is an arbitrary (not necessarily Abelian) finite group, (ii) $H$ is continuous and not discrete, and (iii) the test passing probability is low (low-soundness regime). While each of these generalizations presents its own challenges, these are compounded when they are all together. In order to clearly illustrate the issues, let us focus only on the case of complex-valued functions, $f : G \to \mathbb{U}_1 \subseteq \mathbb{C}$. The entire discussion is relevant when the functions are matrix-valued, but this special case captures all the difficulties.

**Hamming norm is unsuitable** Since the codomain is continuous, the Hamming norm is inappropriate as it is sensitive to small perturbations. For example, let $G$ be a finite group such that the only homomorphism to $\mathbb{U}_1$ is the trivial one. These groups exist and are known as *quasirandom groups*. If $f(x)$ is set to $e^{-i\varepsilon}$ for half of the inputs from $G$ and $e^{-2i\varepsilon}$ for the rest, the BLR test passes with probability roughly $\frac{1}{8}$. But $f$ has a normalized Hamming distance of 1 from the closest homomorphism, i.e., the trivial homomorphism. However, $f$ is actually close to the trivial homomorphism in $L^2$-distance, $\|f - g\|^2 = \mathbb{E}_x[|f(x) - g(x)|^2]$. This suggests why previous works [GH17, BFL03, MR15] in this setting have used the $L^2$-norm.

**Need to look at larger representations** For abelian groups $G$, every function $f : G \to \mathbb{C}$ can be expressed as a linear combination of homomorphisms from $G \to \mathbb{C}$. This is no longer true when $G$ is non-abelian. As we have seen in the preliminaries, we need to rely on homomorphisms $\rho : G \to \mathbb{U}_t$ for $t$ potentially as large as $\sqrt{|G|}$, even though the original function maps to scalars. Thus, it is not immediate how to formalize the statement "$f$ correlates with the homomorphism $\rho$," as $f : G \to \mathbb{C}$ whereas, $\rho : G \to \mathbb{U}_t$ for $t > 1$. There have been two non-equivalent solutions to this in prior work,

1. Clip[1] a representation – Let $g_\rho : G \to \mathbb{C}$ be defined as $g_\rho(x) = V\rho(x)U^*$ for a homomorphism $\rho$, and $V, U \in \mathbb{C}^{1\times t}$. One can now check if $f$ correlates with $g_\rho$. This is the route taken by Gowers and Hatami [GH17].
2. Large Fourier Mass – If the representation $\rho$ is irreducible, one can look at how much of the function can be explained by the Fourier basis elements corresponding to $\rho$, i.e., $\{\rho_{i,j}\}_{i,j}$. Note that these elements are no longer homomorphisms (unlike for Abelian groups), but $\|\hat{f}(\rho)\|_{HS}$ being large is another way to formalize $f$ being correlated with $\rho$, as $\|f\|^2 = \sum_\rho \dim(\rho)\|\hat{f}(\rho)\|_{HS}^2$ by Parseval's. This approach is followed by [MR15].

**Representation sizes depend on test-passing probability** Ideally, we would want to show the correlation of the function with a representation $\rho$ of dimension 1. But the above discussion shows why that is too much to ask for. Nevertheless, one might still want to bound the dimension of these representations, the intuition being that the smaller the dimension, the closer $f$ is to being a true homomorphism. We will see that this can be done but this dimension must depend on the test passing probability $\delta$. Such a dependence is unavoidable, as the following counterexample illustrates. Let $\Gamma$ be a non-abelian group containing an irrep of dimension $d \simeq \mathrm{poly}(|\Gamma|)$, say $\rho$. Consider the group $G = \mathbb{Z}_2^n \times \Gamma$ and its irrep, $\psi = \mathrm{triv} \otimes \rho$. The function $f(x) = \psi(x)_{1,1}$ passes the randomized BLR test if either of the query points is in the kernel of this irrep. Since $\mathbb{Z}_2^n$ lies in the kernel, the test passes with probability at least $\frac{1}{|\Gamma|}$. However, by construction, $f$ is entirely supported on a $d$-dimensional irrep, $\psi$.

[1] For functions $f : G \to \mathbb{U}_t$ for $t > 1$, the representations that need to be considered could be of dimension $t' < t$ as well. We still refer to it as "clipping".

### 1.1.2 Known Results

As previously mentioned, despite the outlined challenges, researchers have achieved intriguing results in this matrix-valued function setting that we are interested in. Specifically, Moore and Russell [MR15] as well as Gowers and Hatmai [GH17] explored the homomorphism testing problem for functions from any finite group $G$ to $\mathbb{U}_t$. It is important to note that their studies did not explicitly focus on this question from a testing perspective. Nevertheless, their findings can be easily adapted into a BLR-type linearity testing framework. Additionally, when translated into homomorphism testing terminology, their approaches correspond to the same Hilbert-Schmidt version of the BLR test that we employ. Below, we summarize the homomorphism testing results derived from these two studies.

**Theorem 1.1** (Tests from [GH17, MR15]). *Let $G$ be any finite group, and $f : G \to \mathbb{U}_t$ be a unitary matrix-valued function. Assume that the function $f$ passes the BLR test with probability $\delta$. Then,*

1. *(Correlation with clipped representation [GH17]) : There is a representation, $\pi : G \to \mathbb{U}_{t'}$ and two matrices, $V, U \in \mathbb{C}^{t \times t'}$, such that $f$ correlates with the function, $g_\pi = V\pi(x)U^* : G \to \mathbb{U}_t$ :*
$$\left\langle f, g_\pi \right\rangle_{\mathrm{tr}} \geq \frac{\delta^2}{4} \cdot t$$
*Moreover, the representation has bounded dimension, $\delta^2 t \leq t' = \dim(\pi) \leq \frac{2t}{\delta^2}$.*
2. *(Fourier Mass on a low-dimensional irreducible representation [MR15]) : There exists an irrep $\rho \in \widehat{G}$ such that $\dim(\rho) < \frac{2t}{\delta^2}$ and $\|\widehat{f}(\rho)\|_{\mathrm{HS}}^2 \geq \frac{\delta^2}{2}$.*

**Remark 1.2.** Note that the representation, $\pi$, in part 1 of the theorem is not guaranteed to be irreducible, but the second one is.

## 1.2 Our Results

The main contribution of this work is to give a derandomized BLR like homomorphism test in the low soundness regime for the general setup of functions from an arbitrary finite group $G \to \mathbb{U}_t$. Prior to this work, the only known derandomized test in the 1%-regime is that of [BSVW03] for the case when $G = \mathbb{Z}_p^n$ and $H = \mathbb{Z}_p$.

Our key derandomization tool is *small–bias sets*, which are those that "fool" irreducible representations. Formally, a set $S \subseteq G$ is $\varepsilon$-biased if for every non-trivial irreducible representation $\rho$, we have $\|\mathbb{E}_{s\sim S}[\rho(s)]\|_{\mathrm{op}} \leq \varepsilon$. Here, the operator norm is the largest singular value of the operator. In the Abelian case, the irreducible representations are *characters*, and thus, this definition is a generalization of the usual one of *fooling* non-trivial characters [NN93, AGHP92]. We have the following derandomization of a result of Alon–Roichman [AR94],

**Theorem 1.3** ([WX08, Thm 5.1]). *For every finite group $G$ and any constant $\varepsilon > 0$, there exists a deterministic $\mathrm{poly}(|G|)$-time algorithm that outputs an $\varepsilon$-biased set $S \subseteq G$ of size $|S| \leq O\left(\frac{\log|G|}{\varepsilon^2}\right)$.*

While this bound is tight over Abelian groups, we can do much better for other groups. Particularly for all *finite simple groups* we now have explicit constant-sized small-biased sets due to a long line of work [KN06, Kas07, Lub11]. These can also be made near-optimal using the amplification machinery in [JMRW22].

**Theorem 1.4** ([KN06, Kas07, Lub11, JMRW22])**.** *For every finite simple group* $G$ *and any* $\varepsilon > 0$*, there exists a deterministic* $\mathrm{poly}(1/\varepsilon)$*-time algorithm that outputs an* $\varepsilon$*-biased set* $S \subseteq G$ *of size* $|S| \leq O\big(\varepsilon^{-(2+o(1))}\big)$.

**Result 1: Derandomized Homomorphism Testing** We analyze the following derandomized variant of BLR. Here, the parameter $\gamma$ allows for a relaxed version of this test that makes the test robust to small noise, which can be useful as $\mathbb{U}_t$ is a continuous group.

**Derandomized BLR**$_\gamma(G, S, f)$:

1. Sample $x \sim G, y \sim S$.
2. If $\|f(xy) - f(x) \cdot f(y)\|_{HS}^2 \leq \gamma t$, output *Pass*. Else, output *Fail*.

Setting $\gamma = 0$ recovers the usual derandomized version of the BLR test that has been used in previous derandomizations of homomorphism tests [BSVW03, SW04]. The following table compares our derandomized test with other tests.

| Work | Setting ($f : G \to H$) | Conclusion | Randomness |
|---|---|---|---|
| | High Soundness | | |
| [BLR90] | $G = \mathbb{Z}_2^n$, $H = \mathbb{Z}_2$ | Hamming | $2 \log \lvert G \rvert$ |
| [BOCLR07] | $G, H$ any finite groups | Hamming | $2 \log \lvert G \rvert$ |
| [SW04] | $G, H$ any finite groups | Hamming | $(1 + o(1)) \log \lvert G \rvert$ |
| | Low Soundness | | |
| [BCH+95] | $G = \mathbb{Z}_2^n$, $H = \mathbb{Z}_2$ | Hamming | $2 \log \lvert G \rvert$ |
| [Kiw03] | $G = \mathbb{Z}_p^n$, $H = \mathbb{Z}_p$ | Hamming | $(2 + o(1)) \log \lvert G \rvert$ |
| [BSVW03] | $G = \mathbb{Z}_p^n$, $H = \mathbb{Z}_p$ | Hamming | $(1 + o(1)) \log \lvert G \rvert$ |
| [Sam07, San12, GGMT23] | $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$ | Hamming | $2 \log \lvert G \rvert$ |
| [BFL03] | $G$ finite abelian, $H = \mathbb{U}_1$ | Correlation | $2 \log \lvert G \rvert$ |
| [MR15] | $G$ any finite group, $H = \mathbb{U}_t$ | Correlation | $2 \log \lvert G \rvert$ |
| [GH17] | $G$ any finite group, $H = \mathbb{U}_t$ | Hilbert-Schmidt | $2 \log \lvert G \rvert$ |
| Our Result | $G$ any finite group, $H = \mathbb{U}_t$ | Hilbert-Schmidt | $(1 + o(1)) \log \lvert G \rvert$ |
| Our Result | $G$ any finite group, $H = \mathbb{U}_t$ | Correlation | $(1 + o(1)) \log \lvert G \rvert$ |

Figure 1: A summary of prior works on homomorphism testing

**Theorem 1.5** (Informal version of Theorem 4.4)**.** *Let* $G$ *be any finite group, and* $f : G \to \mathbb{U}_t$ *be a unitary matrix-valued function. Let* $S \subseteq G$ *be an* $\varepsilon$*-biased set. Assume that the function* $f$ *passes the derandomized BLR test with probability* $\delta > \sqrt{\varepsilon}$*. Then,*

1. *(Correlation with clipped representation): There is a representation,* $\pi : G \longrightarrow \mathbb{U}_{t'}$ *and two matrices,* $V, U \in \mathbb{C}^{t\times t'}$, *such that for* $g_\pi = V\pi(x)U^* : G \longrightarrow \mathbb{U}_t$, $f$ *correlates with* $g_\pi$,

   $$\left\langle f, g_\pi \right\rangle_{tr} \ \geq \ \tfrac{\delta^2-\varepsilon}{4} \cdot t$$

   *Moreover, the representation has bounded dimension,* $(\delta^2 - \varepsilon)t \leq t' = \dim(\pi) \leq \frac{2t}{\delta^2-\varepsilon}$.

2. *(Fourier Mass on a low-dimensional irreducible representation): There exists an irrep* $\rho \in \widehat{G}$ *such that* $\dim(\rho) < \frac{2t}{\delta^2-\varepsilon}$ *and* $\|\widehat{f}(\rho)\|_{HS}^2 \geq \frac{\delta^2-\varepsilon}{2}$.

*Moreover, if one uses the* $\gamma$*-robust BLR test, the same conclusions hold with* $\delta$ *replaced by* $\delta - (\gamma/2)$.

Using the small-bias set construction from Theorem 1.3, we get a test that uses $\log|G| + \log|S| = \log|G| + O(\log\log|G|) = (1 + o(1))\log|G|$-random bits. For special families of groups like the class of *finite simple groups*, we can use Theorem 1.4 to further reduce the randomness to $\log|G| + O(1)$, which is almost optimal.

**Result 2: Derandomized BNP Lemma** The "BNP lemma" is a very useful observation due to Babai, Nikolov, Pyber [BNP08], and Gowers [Gow08]. This lemma gives an improvement over Cauchy–Schwarz for *quasirandom groups*, i.e., groups with no small non-trivial irreps, and has been used to analyze mixing in progressions [BHR22], product-free sets [Gow08], and hardness of approximation [BKM22], to name a few. In its most general form, it says that for functions $f, g : G \longrightarrow M$ that map to $t \times t$-matrices, we have,

$$\|f * g\|^2 = \mathop{\mathbb{E}}_{s\sim G}\left[\|(f * g)(s)\|_{HS}^2\right] \ \leq \ \frac{1}{D}\,\|f\|_2^2\|g\|_2^2$$

We show that such a bound holds even when the average is over a small-bias set $S \subseteq G$, which could be of constant size for some groups!

**Lemma 1.6** (Derandomized Matrix BNP)**.** *Let* $G$ *be a group such that the dimension of the smallest non-trivial irrep is* $D$ *and let* $S \subseteq G$ *be an* $\varepsilon$*-biased set. Let* $f, g : G \longrightarrow M_t(\mathbb{C})$ *be mean-zero functions. Then,*

$$\mathop{\mathbb{E}}_{s\sim S}\left[\|(f * g)(s)\|_{HS}^2\right] \ \leq \ \left(\frac{1}{D} + \varepsilon\right)\|f\|_2^2\|g\|_2^2$$

*The usual BNP lemma can be recovered by setting* $S = G$*, and thus,* $\varepsilon = 0$.

## 1.3 Technical Overview

Our main conceptual contribution is to initiate the study of the non-abelian generalization of two key notions in the analysis of Boolean functions: (i) *spectral norm* of a function and (ii) *spectral positivity*.

**Spectral norm and its non-abelian analog** The $\ell_1$-norm of the Fourier transform of a function is known as its *spectral norm*. Spectral norm has emerged as an important quantity for the analysis of Boolean functions, i.e., functions over $\mathbb{Z}_2^n$. In particular, functions with low spectral norm have a lot of structure [STV17]: they admit small decision trees, parity decision trees, they are easily learnable, etc.

One of the conceptual contributions of this paper is studying the non-abelian analog of this norm from the perspective of pseudorandomness. A first generalization one can think of would be a similar $\ell_1$ norm of the Fourier coefficients. However, it turns out that the appropriate generalization of the spectral norm is the *Fourier algebra norm*. This was suggested earlier by Sanders [San21], who used it to generalize the quantitative idempotent theorem. This norm has multiple equivalent definitions, but our key idea is to use the following harmonic analytic reformulation due to Sanders [San21] (attributed to [Eym64]),

$$\|f\|_A = \min_{(\pi,V)} \left\{ \|u\| \cdot \|v\| \;\middle|\; f(x) = \langle u, \pi(x) v \rangle \right\}$$

where $(\pi, V)$ is a representation of $G$ and $u, v \in V$. [2]

It is well-known that any function, $f$, on an Abelian group is $\varepsilon\|\hat{f}\|_1$-fooled by any $\varepsilon$-biased set. We show that this neatly generalizes to any finite group by replacing the spectral norm with Fourier algebra norm, any function, $f$, on a finite group is $\varepsilon\|f\|_A$-fooled by any $\varepsilon$-biased set.

**Spectral Positivity and its non-abelian analog** A function over an Abelian group $G$, $f : G \to \mathbb{C}$, is spectrally non-negative of $\hat{f}(\chi) \geq 0$ for every character $\chi$. This notion played a key role in the recent breakthrough by Kelley and Meka [KM23] on 3-AP free sets.

This naturally generalizes to the finite group setting wherein a *positive-definite functions* is a function $f$ such that $\hat{f}(\rho)$ is positive semi-definite for every irreducible representation $\rho$. The important observation is that such functions have small algebra norm, $\|f\|_A = f(1)$. We use this observation to prove that small–bias sets can be used to approximate the $U^2$-norm.

### 1.3.1 Proof Overview

Denote $\tilde{f}(x) = f(x^{-1})^*$, and recall the following two norms for functions $f : G \to \mathbb{U}_t$,

$$(U^2\text{-norm}) \quad \|f\|_{U^2} = \|f * \tilde{f}\|^2 = \mathop{\mathbb{E}}_{x\sim G}\left[\|(f * \tilde{f})(x)\|_{HS}^2\right]$$

$$(\text{Algebra norm}) \quad \|f\|_A = \min_{(\pi,V)} \left\{ \|u\| \cdot \|v\| \;\middle|\; f(x) = \langle u, \pi(x) v \rangle \right\}$$

We now give a quick summary of the key steps involved in the proof:

1. (Lemma 3.1) Small–bias sets fool functions with a small algebra norm.
2. (Lemma 5.1) Let $f, g : G \to \mathbb{U}_t$ be any functions. Then, the function, $x \mapsto \|(f * g)(x)\|_{HS}^2$ has a small Fourier algebra norm.

[2] The Fourier inversion theorem gives one such an expression for $f$ by using the *regular representation*; although it might not be the one that minimizes the algebra norm, and hence one minimizes over such expressions.

3. The above two lemmas imply a degree-2 EML. This immediately yields our result on the derandomized BNP lemma (Lemma 1.6). We expect that this degree-2 EML will have uses beyond this work, and we explain this below.

4. A special case of the above EML implies that small bias sets approximate $U^2$-norm (Corollary 1.7). Thus, the test passing probability of the derandomized test implies a large $U^2$-norm of the function. Combining this with the inverse theorem of Gowers-Hatami [GH17] gives us the first part of Theorem 1.5.

5. The second part of Theorem 1.5 follows from the same large $U^2$-norm consequence implied by test passing. To achieve this, we adapt the proof strategy of the BNP lemma [BNP08] to our setup, which relies on basic non-abelian harmonic analysis.

**Degree-2 EML** Our key technical contribution is a degree-2 variant of the celebrated *expander mixing lemma* (EML). Recall that EML characterizes spectral expansion. When applied to the Cayley graph $\mathrm{Cay}(G, S)$, we get that $S$ is an $\varepsilon$-biased set if and only if the EML holds,

$$\left| \mathop{\mathbb{E}}_{s\sim S}[(f * g)(s)] - \mathop{\mathbb{E}}_{s\sim G}[(f * g)(s)] \right| \leq \varepsilon \|f\|_2 \, \|g\|_2, \quad \text{(EML)}\,.$$

We prove that such sets also satisfy a degree-2 variant of the above inequality,

$$\left| \mathop{\mathbb{E}}_{s\sim S}\left[\|(f * g)(s)\|^2\right] - \mathop{\mathbb{E}}_{s\sim G}\left[\|(f * g)(s)\|^2\right] \right| \leq \varepsilon \|f\|_2^2 \, \|g\|_2^2, \quad \text{(Our degree-2 EML)}\,.$$

Using it for the special case of where $g(x) = \tilde{f}(x) = f(x^{-1})^*$, we get that small bias sets approximate $U^2$-norm.

**Corollary 1.7** (Small bias sets approximate $U^2$-norm)**.** *For $f : G \to \mathbb{U}_t$ such that $\|f\| = 1$,*

$$\left| \mathop{\mathbb{E}}_{s\sim S}\left[\|(f * \tilde{f})(s)\|^2\right] - \|f\|_{U^2} \right| \leq \varepsilon \|f\|_2^4\,.$$

*Thus, the $U^2$-norm of a function $f$ can be $\varepsilon$-estimated by querying $f * \tilde{f}$ on an $\varepsilon$-biased set $S$.*

## 1.4 Related Work

**High soundness regime** Blum–Luby–Rubinfield [BLR90] analyzed linearity tests for functions of the form $f : \mathbb{Z}_2^n \to \{\pm 1\}$. This was extended to the setting $f : G \to H$ where both are arbitrary finite groups, by Ben-Or, Coppersmith, Luby, and Rubinfeld [BOCLR07]. This result was derandomized by Shpilka and Wigderson [SW04]. Going beyond finite groups, Farah [Far00], and later, Badora and Przebieracz [BP18], give homomorphism tests for any *amenable group* $G$, and any group $H$, equipped with an invariant metric.

**Low soundness regime** Bellare, Coppersmith, Håstad, Kiwi, and Sudan [BCH+95] analyzed linearity tests for functions of the form $f : \mathbb{Z}_2^n \to \{\pm 1\}$ in this low-soundness regime. This was extended to the setting of $\mathbb{Z}_p^n \to \mathbb{Z}_p$ by Håstad and Wigderson [HW03]. This result was derandomized using $\varepsilon$-biased sets by Ben-Sasson, Sudan, Vadhan, and Wigderson [BSVW03]. For the same setting, Kiwi [Kiw03] analyzed a variant of the BLR test that uses a lot more randomness but gives an improved correlation. Samorodnitsky [Sam07] studied a completely different setup where $H$ is large and not a subset of $\mathbb{C}$. He showed that if a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, passes the test with probability $\delta$, then it has an exponentially small agreement with a homomorphism. Improving the agreement to polynomial in $\delta$ is equivalent to the polynomial Freiman–Rusza (PFR) conjecture which was finally settled recently [San12, GGMT23].

## 2 Preliminaries

Throughout the work, we will assume that $G$ is a finite group, and all vector spaces are finite-dimensional over $\mathbb{C}$. We work with vector spaces of matrix-valued functions, and unless mentioned otherwise, these spaces are equipped with the expectation inner product, $\langle f, g\rangle = \mathbb{E}_x[\langle f(x), g(x)\rangle_{\mathrm{tr}}]$. We use $\mathbb{U}_t$ to denote the group of $t \times t$ unitary matrices, and $M_t(\mathbb{C})$ to denote the set of $t \times t$ complex matrices.

### 2.1 Group Representations and small-bias sets

For finite groups, every representation can be made unitary, and thus, we can restrict to studying these. Let $V$ be a complex Hilbert space and denote by $U_V$, the unitary group of operators acting on $V$.

**Definition 2.1** (Unitary Group Representation)**.** For a group $G$, a unitary representation is a pair $(\rho, V)$ where $\rho : G \to U_V$ is a group homomorphism, i.e., for every $x, y \in G$, we have $\rho(xy) = \rho(x)\rho(y)$. A representation is *irreducible* if the only subspaces of $V$ that are invariant under the action of $\rho(G)$ are the empty space, $\{0\}$, and the entire space, $V$. For a representation $(\rho, V)$, will use $d_\rho$ to denote $\dim(V)$.

We use $\widehat{G}$ to denote the set of all irreducible representations (*irreps*) of a group $G$. Every group has a special irreducible representation called the *trivial representation*, $(\rho_{\mathrm{triv}}, \mathbb{C})$, where $\rho(g) = 1$ for every group element $g \in G$. The following is a fundamental result that states that every representation decomposes as a finite sum of irreducible ones.

**Theorem 2.2** (Maschke)**.** *Let $G$ be a finite group and let $(\pi, V)$ be any representation of $G$. Then, $V = \oplus_i V_{\rho_i}$, i.e., it decomposes as a direct sum of irreducible representations $\{\rho_i\}_i$. Explicitly, there exists a unitary transformation $U_\pi$ such that $U_\pi \pi U_\pi^*$ is block-diagonal with each block being $\rho_i$.*

**Small–bias sets** Small bias sets over Abelian groups were introduced in the pioneering work of Naor and Naor [NN93], and are a fundamental derandomization tool that has been widely used across domains like complexity theory, coding theory, learning theory, graph theory, etc. See the excellent surveys [HH24, HLW06] for references and details. Apart from the wealth of applications arising from expanders, $\varepsilon$-biased sets for non-abelian groups have also recently found applications in constructions of near-optimal expanders and quantum expanders [JMRW22], constructions of *unitary designs* [OSP23].

**Definition 2.3** (δ-fooled)**.** A function $f : G \to M_t(\mathbb{C})$ is δ-fooled by a set $S \subseteq G$ if,

$$\left\| \mathop{\mathbb{E}}_{x\sim G}[f(x)] - \mathop{\mathbb{E}}_{x\sim S}[f(x)] \right\|_{op} \leq \delta.$$

Small–bias sets are those that fool all non-trivial irreducible representations. In the abelian case, the irreducible representations are *characters*, and thus, this definition is a generalization of the usual one of *fooling* non-trivial characters [NN90, AGHP92].

**Definition 2.4** (ε-Biased Set)**.** Let $\varepsilon \in [0, 1)$. We say that a multiset $S \subseteq G$ is ε-biased if for every irreducible representation ρ, ρ is ε-fooled by S, i.e., $\|\mathbb{E}_{s\sim S}[\rho(s)]\|_{op} \leq \varepsilon$. Here, the operator norm is the largest singular value of the operator

The notion of small bias is closely linked to graph expansion, in particular, a symmetric subset $S \subseteq G$ is an ε-biased set if and only if the $\mathrm{Cay}(G, S)$ is an ε-spectral expander, i.e., the adjacency matrix has second largest eigenvalue ε.

## 2.2 Matrix–valued functions and $U^2$-norm

Denote by $L^2_t(\mathbb{C}) = \{f : G \to M_t(\mathbb{C})\}$, the space of $t \times t$ matrix-valued functions equipped with the trace expectation inner product,

$$\langle f, g\rangle = \mathop{\mathbb{E}}_{x\sim G}[\langle f(x), g(x)\rangle_{tr}] = \mathop{\mathbb{E}}_{x\sim G}\left[\mathrm{Tr}\big(g(x)^* f(x)\big)\right] \tag{1}$$

The induced norm is $\|f\|^2 = \mathbb{E}_{x\sim G}[\|f(x)\|^2_{HS}]$. For a function f, we denote its *adjoint* by $\tilde{f}(x) := f(x^{-1})^*$. The operation of convolution generalizes as,

$$(f * g)(x) := \mathbb{E}_{y\sim G}\left[f(xy^{-1})g(y)\right] = \mathbb{E}_{y\sim G}\left[\tilde{f}(y)^* g(yx)\right].$$

**Definition 2.5** (Matrix Fourier Coefficient)**.** For any irrep ρ, we have $\widehat{f}(\rho) := \mathbb{E}_x\left[f(x) \otimes \rho(x)\right]$. We denote the coefficient of the trivial irrep as $\mu(f) := \widehat{f}(\rho_{triv})$.

**Fact 2.6.** *The following identities hold for the matrix Fourier transform,*

1. **(Parseval's identity)** $\|f\|^2 = \mathbb{E}_x\left[\|f(x)\|^2_{HS}\right] = \sum_{\rho\in\widehat{G}} d_\rho \|\widehat{f}(\rho)\|^2_{HS}$
2. **(Convolution identity)** $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$
3. **($U^2$ norm)** $\|f\|_{U^2} = \|\tilde{f} * f\|^2 = \sum_\rho d_\rho \left\|\widehat{f}(\rho)\widehat{f}(\rho)^*\right\|^2_{HS} = \sum_\rho d_\rho \left\|\widehat{f}(\rho)^*\widehat{f}(\rho)\right\|^2_{HS}$

*Proof.* These facts are simple extensions of the scalar-valued functions and were considered in [BFL03, MR15, GH17]. Since the last one is perhaps atypical, we provide a quick proof.

$$\|f\|_{U^2} := \mathop{\mathbb{E}}_{xy^{-1}=wz^{-1}}\left[\mathrm{Tr}\big(\, f(x)f(y)^* f(z)f(w)^* \,\big)\right]$$

$$
\begin{aligned}
&= \mathop{\mathbb{E}}_{t=xy^{-1}=wz^{-1}}[\langle f(x)f(y)^*, f(w)f(z)^* \rangle] \\
&= \mathop{\mathbb{E}}_{t=xy^{-1}=wz^{-1}}\Big[\Big\langle f(x)\tilde{f}(y^{-1}), f(w)\tilde{f}(z^{-1}) \Big\rangle\Big] \\
&= \mathop{\mathbb{E}}_{t}\Big[\Big\langle (f * \tilde{f})(t), (f * \tilde{f})(t) \Big\rangle\Big] = \|f * \tilde{f}\|^2
\end{aligned}
$$

The second equality follows from Parseval's and convolution identity once one observes that,

$$
\widehat{\tilde{f}}(\rho) = \mathop{\mathbb{E}}_{x}\Big[f(x^{-1})^* \otimes \rho(x)\Big] = \mathop{\mathbb{E}}_{x}\Big[f(x)^* \otimes \rho(x^{-1})\Big] = \mathop{\mathbb{E}}_{x}[f(x)^* \otimes \rho(x)^*] = \hat{f}(\rho)^* \qquad \blacksquare
$$

### 2.3 Fourier algebra norm and positive definite functions

Let $f : G \to \mathbb{C}$ be any function and let $T_f$ be the convolution by f operator, $T_f(g) = f * g$. More explicitly, $T_f(x, y) = \frac{1}{|G|} f(x^{-1}y)$ is a $|G| \times |G|$ matrix.

**Definition 2.7** (Fourier algebra norm)**.** The *algebra norm* of $f : G \to \mathbb{C}$ has the following equivalent definitions,

i. $\|f\|_A = \sup\big\{\langle f, g\rangle \;\big|\; \|T_g\|_{op} \leq 1\big\}$.

ii. $\|f\|_A = \|T_f\|_{tr} = \sum_i \sigma_i(T_f)$ where $\{\sigma_i\}$ are the singular values of $T_f$.

iii. $\|f\|_A = \min_{(\pi,V)}\big\{\, \|u\| \cdot \|v\| \;\big|\; f(x) = \langle u, \pi(x)\, v\rangle \,\big\}$ where $(\pi, V)$ is a representation of G and $u, v \in V$.

The equivalence of definitions (i) and (ii) can be found in [San11, Lem. 5.2] and also in [HHH22, Prop 3.11]. The proof of equivalence between (i) and (iii) is present in [San21, Lem. 2.2], attributed to Eymard [Eym64, Thèorém, Pg 218]. In particular, Sanders shows that the minimum is indeed attained for some representation $(\pi, V)$.

**Abelian Case** When the group is abelian, the algebra norm coincides with the *spectral norm*, i.e., $\|f\|_A = \|\,\hat{f}\,\|_1$. This can be seen by observing that $T_f$ is a diagonal matrix (in the Fourier basis) with the Fourier coefficients on the diagonal. Therefore, the algebra norm is a generalization of the spectral norm to the non-Abelian setting.

**Definition 2.8** (Positive definite functions)**.** Let G be a finite group. A function $f : G \to \mathbb{C}$, is said to be positive definite if the convolution operator, $T_f$, is positive semi-definite.

The following simple observation states that positive definite functions have a small algebra norm. We will crucially use this later to bound the algebra norm of a function.

**Observation 2.9.** If a function f is positive-definite, then $\|f\|_A = f(1)$.

*Proof.* Since $T_f$ is positive semi-definite, $\|f\|_A = \|T_f\|_{tr} = tr(T_f) = f(1)$ as $T_f(x, y) = \frac{f(x^{-1}y)}{|G|}$. $\blacksquare$

## 3 Small-bias sets “fool” small norm functions

In the Boolean setting, properties of low spectral norm function have been well-studied [KM93, STV17]. Green and Sanders [GS08] showed that functions with low spectral norm can be expressed as a ±1 combination of characteristic functions of cosets. Sanders [San11] generalized it to non-abelian groups with spectral norm replaced by the algebra norm.

This suggests that the algebra norm is indeed the right generalization of the spectral norm, and one might investigate other properties of functions with low algebra/spectral norm. In this section, we make yet another connection by showing that small-bias sets fool functions with small algebra norm; again generalizing the Abelian case.

**Boolean Cube** Let $f : \mathbb{Z}_2^n \to \mathbb{C}$, be any function and let $S$ be an $\varepsilon$-biased set. Then,

$$\begin{aligned} \left|\mathop{\mathbb{E}}_{h\sim S}[f(h)] - \mathop{\mathbb{E}}_{h\sim G}[f(h)]\right| &= \left|\sum_{\chi} \hat{f}(\chi)\Big(\mathop{\mathbb{E}}_{h\sim S}[\chi(h)] - \mathop{\mathbb{E}}_{h\sim G}[\chi(h)]\Big)\right| \\ &\leq \max_{\chi}\left|\mathop{\mathbb{E}}_{h\sim S}[\chi(h)] - \mathop{\mathbb{E}}_{h\sim G}[\chi(h)]\right| \cdot \sum_{\chi\neq 0}\left|\hat{f}(\chi)\right| \\ &\leq \varepsilon \cdot \|f - \mu(f)\|_A \end{aligned}$$

Moreover, this is tight due to a result of [DETT10, Prop. 2.7], which says that any function that is fooled by all $\varepsilon$-biased sets must be sandwiched by low spectral norm functions.

**General finite groups** We now generalize the above result for finite groups. The key here is to use the harmonic analytic definition of the spectral norm which makes the proof surprisingly simple.

**Lemma 3.1.** *Let $f : G \to \mathbb{C}$, be a function and $S \subseteq G$ be any $\varepsilon$-biased set,. Then,*

$$\left| \mathop{\mathbb{E}}_{x\sim S}[f(x)] - \mathop{\mathbb{E}}_{x\sim G}[f(x)] \right| \leq \varepsilon \cdot \|f\|_A \ .$$

*Proof.* From Definition 2.7, we get that there is a representation, $(\pi, V)$, representation of $G$ such that $f(x) = \langle u, \pi(x)v\rangle$ for some $u, v \in V$. Moreover, $\|u\|\|v\| \leq \|f\|_A$. Using Maschke’s theorem (Theorem 2.2), we have $\pi = \rho_{\text{triv}}^{\oplus c} \oplus_i \rho_i$ where $c$ denotes the multiplicity of the trivial representation and $\rho_i$ are all non-trivial irreducible representations (possibly with repetitions). Let $U_\pi$ be the unitary transformation that block-diagonalizes $\pi$. Then, $U_\pi v = v_{\text{triv}} \oplus v_i$ and similarly $U_\pi u = u_{\text{triv}} \oplus u_i$. Thus, we have,

$$\begin{aligned} \langle u, \pi(x)\, v\rangle = \langle U_\pi u, U_\pi\, \pi(x)\, v\rangle = \langle U_\pi u, (U_\pi \pi(x) U_\pi^*)\, U_\pi v\rangle \\ = \langle u_{\text{triv}} \oplus_i u_i, v_{\text{triv}} \oplus_i (\rho_i v_i)\rangle \\ = \langle u_{\text{triv}}, v_{\text{triv}}\rangle + \sum_i \langle u_i, \rho_i(x)\, v_i\rangle \end{aligned}$$

Now, $\langle u_{\text{triv}}, v_{\text{triv}}\rangle$ is a constant and is the same for both terms. Therefore,

$$\begin{aligned}
\mathop{\mathbb{E}}_{x\sim S}[f(x)] - \mathop{\mathbb{E}}_{x\sim G}[f(x)] &= \sum_i \left\langle u_i, \mathop{\mathbb{E}}_{x\sim S}[\rho_i(x)] - \mathop{\mathbb{E}}_{x\sim G}[\rho_i(x)]\, v_i \right\rangle \\
\left|\mathop{\mathbb{E}}_{x\sim S}[f(x)] - \mathop{\mathbb{E}}_{x\sim G}[f(x)]\right| &\le \sum_i \|u_i\|_2 \cdot \left\|\mathop{\mathbb{E}}_{x\sim S}[\rho_i(x)] - \mathop{\mathbb{E}}_{x\sim G}[\rho_i(x)]\right\|_{\mathrm{op}} \|v_i\|_2 && \text{(From Cauchy–Schwarz)} \\
&\le \varepsilon \sum_i \|u_i\|_2 \|v_i\|_2 && \text{($S$ is an $\varepsilon$-bias set)} \\
&\le \varepsilon \cdot \sqrt{\sum_i \|u_i\|_2^2}\sqrt{\sum_i \|v_i\|_2^2} && \text{( Cauchy–Schwarz)} \\
&= \varepsilon \cdot \|u - u_{\mathrm{triv}}\|_2 \|v - v_{\mathrm{triv}}\|_2 && \text{($U_\pi$ is unitary)} \quad \blacksquare
\end{aligned}$$

**Corollary 3.2** (PD functions are fooled)**.** *If* $f : G \to \mathbb{C}$ *is a positive-definite function, then* $\|f\|_A = f(1) \le \|f\|_\infty$*. Therefore, if* $\|f\|_\infty \le 1$*, then* $f$ *is* $\varepsilon$*-fooled by every* $\varepsilon$*-biased set.*

*Proof.* Since, $f$ is positive definite, $T_f$ is PSD and thus, $\|f\|_A = \|T_f\|_{\mathrm{tr}} = \mathrm{Tr}(T_f) = f(1) \le 1$. ■

## 3.1 $U^2$ norm and algebra norm

Let $f : G \to M_t(\mathbb{C})$ be a function, then $\|f\|_{U^2} = \mathbb{E}_{y\sim G}[\psi(y)]$ where,

$$\psi(y) = \left\|(\tilde{f} * f)(y)\right\|_{\mathrm{HS}}^2 = \left\|\mathop{\mathbb{E}}_{x\sim G}[f(x)^* f(xy)]\right\|_{\mathrm{HS}}^2 .$$

Therefore, if $\psi$ has small algebra norm then, $\|f\|_{U^2}$ can be approximated by averaging $\psi$ over an $\varepsilon$-biased set. We prove the algebra norm bound by proving that the function, $\psi$, is a positive-definite function.

**Lemma 3.3.** *For* $f : G \to M_t(\mathbb{C})$*, the function* $\psi(y) = \left\|(\tilde{f} * f)(y)\right\|_{\mathrm{HS}}^2$ *is positive-definite.*

*Proof.* To prove that $T_\psi$ is a PSD matrix, we wish to show that for any $\{c_a\}_{a\in G} \in \mathbb{C}^G$,

$$\sum_{a,b\in G} c_a \overline{c_b}\, \psi(a^{-1}b) \;\ge\; 0$$

The key observation is that, if we can write $\psi(a^{-1}b) = \mathbb{E}_{x,y\sim G}[\langle N_{x,y}(a), N_{x,y}(b)\rangle_{\mathrm{tr}}]$ for some $N_{x,y}$, then $\psi$ is positive-definite. We first show such a factorization of $\psi(a^{-1}b)$.

$$\begin{aligned}
\psi(a^{-1}b) &= \left\|\mathop{\mathbb{E}}_{x\sim G}\left[f(x)^* f(xa^{-1}b)\right]\right\|_{\mathrm{HS}}^2 \\
&= \left\|\mathop{\mathbb{E}}_{x\sim G}[f(xa)^* f(xb)]\right\|_{\mathrm{HS}}^2 \\
&= \left\langle \mathop{\mathbb{E}}_{x\sim G}[f(xa)^* f(xb)], \mathop{\mathbb{E}}_{y\sim G}[f(ya)^* f(yb)] \right\rangle_{\mathrm{tr}} \\
&= \mathop{\mathbb{E}}_{x,y\sim G}[\langle f(xa)^* f(xb), f(ya)^* f(yb)\rangle_{\mathrm{tr}}]
\end{aligned}$$

$$
\begin{aligned}
&= \mathop{\mathbb{E}}_{x,y\sim G}[\langle f(ya)f(xa)^*, f(yb)f(xb)^*\rangle_{\mathrm{tr}}] \\
&:= \mathop{\mathbb{E}}_{x,y\sim G}\left[\left\langle N_{x,y}(a), N_{x,y}(b)\right\rangle_{\mathrm{tr}}\right]
\end{aligned}
$$

The second last equality uses the cyclicity of trace. The result now follows,

$$
\begin{aligned}
\sum_{a,b\in G} c_a\overline{c_b}\,\psi(a^{-1}b) &= \sum_{a,b\in G} c_a\overline{c_b}\mathop{\mathbb{E}}_{x,y\sim G}\left[\left\langle N_{x,y}(a), N_{x,y}(b)\right\rangle_{\mathrm{tr}}\right] \\
&= \mathop{\mathbb{E}}_{x,y\sim G}\left[\left\langle \sum_{a\sim G} c_a N_{x,y}(a), \sum_{b\sim G} c_b N_{x,y}(b)\right\rangle_{\mathrm{tr}}\right] \\
&= \mathop{\mathbb{E}}_{x,y\sim G}\left[\left\|\sum_{a\sim G} c_a N_{x,y}(a)\right\|_{\mathrm{HS}}^2\right] \geq 0.
\end{aligned}
$$

■

**Remark 3.4.** One can also deduce this by coupling *Stinespring's dilation theorem* with the observation in [DCOT18] that $\tilde{f} * f$ is *completely positive*. This immediately yields that $\psi(y) = \langle VV^*, \pi(y)VV^*\pi(y)^*\rangle = \langle VV^*, \rho(y)VV^*\rangle$ for some representation $\rho$. We will use this idea in proving Lemma 5.1 which is a general version of the above lemma.

# 4 Derandomized Matrix Correlation Testing

In this section, we will focus on functions of the form, $f : G \to \mathbb{U}_t$. Let $S \subseteq G$ be an $\varepsilon$-biased set. We consider the following robust variant of the BLR test on group $G$ :

**BLR**$_\gamma(G, S, f)$:

1. Sample $x \sim G, y \sim S$.
2. If $\|f(xy) - f(x)\cdot f(y)\|_{\mathrm{HS}}^2 \leq \gamma t$, output *Pass*. Else, output *Fail*.

If $S = G$, i.e., in the full randomness regime, it can be easily shown that if a function passes the test, then it must have a large $U^2$-norm. Our key technical claim (Claim 4.2) is that if $S$ is a small–biased set, then, essentially, the same conclusion can be drawn from derandomized BLR test passing.

This lower bound on the $U^2$-norm can then be plugged into the result of Gowers and Hatami [**?**], who showed that if a matrix-valued function on a finite group has non-trivial $U^2$-norm then it must be close to some genuine representation. More specifically,

**Theorem 4.1** (Gowers–Hatami [GH17])**.** *Let $G$ be any finite group and let $f : G \to M_t(\mathbb{C})$ be a matrix-valued function such that $\|f(x)\|_{\mathrm{op}} \leq 1$ and $\|f\|_{U^2} \geq ct$, for some $c > 0$. Then there are $t' \in [\frac{c}{2-c}t, \frac{2-c}{c}t]$ and a function $g(x) := V\pi(x)U^*$ where $\pi$ is a $t'$ dimensional unitary representation, $U, V$ are $t \times t'$ dimensional partial unitary matrices, such that:*

$$
\mathbb{E}_{x\sim G}\left[\left\langle f(x), g(x)\right\rangle_{\mathrm{HS}}\right] \geq c^2/4
$$

We first prove the key derandomization claim which lets us move from the test passing probability of the derandomized test, to a claim about the $U^2$ norm over the entire group.

**Claim 4.2** (Derandomized Test also implies large $U^2$-norm). *Let $\gamma, \delta \geq 0$ and $f : G \longrightarrow \mathbb{U}_t$. If $f$ passes the $BLR_{2\gamma}(G, S, f)$ test with probability $\geq \delta$ then, then*

$$\|f\|_{U^2} \ \geq \ \left((\delta - \gamma)^2 - \varepsilon\right) \cdot t.$$

*Proof.* Let, $\Delta(x, y) := \|f(x)f(y) - f(xy)\|_{HS}^2$ and $\delta' = \delta - \gamma$. We have,

$$\mathbb{E}_{x\sim G, y\sim S}\left[\Delta(x, y)\right] \ = \ 2t - \ \mathbb{E}_{y\sim S}\left[\ \left\langle f(y), \tilde{f} * f(y)\right\rangle_{tr} + \left\langle \tilde{f} * f(y), f(y)\right\rangle_{tr}\right] \tag{2}$$

This follows directly by expanding $\Delta(x, y)$ and using the fact that $\|f\|^2 = t$. On the other hand, from the test-passing guarantee we have,

$$\begin{aligned}\mathop{\mathbb{E}}_{x\sim G, y\sim S}[\Delta(x, y)] \ &\leq \ \mathop{\Pr}_{x\sim G, y\sim S}[\Delta(x, y) > 2\gamma t] \cdot 2t + \mathop{\Pr}_{x\sim G, y\sim S}[\Delta(x, y) \leq 2\gamma t] \cdot 2\gamma t \\ &\leq 2t(1 - \delta) + 2\gamma t \\ &= \ 2(1 - \delta')t \end{aligned} \tag{3}$$

In the first inequality, we used the fact that $\max_{x,y}\{\Delta(x, y)\} \ \leq \ 2t$, and in the second inequality, we used test passing probability to upper bound $\Pr_{x\sim G, y\sim S}[\Delta(x, y) \ > \ 2\gamma t]$. Combining Eq. (2) and Eq. (3), we get:

$$\begin{aligned} 2\delta' t \ &\leq \ \mathbb{E}_{y\sim S}\left[\ \left\langle f(y), \tilde{f} * f(y)\right\rangle_{tr} + \left\langle \tilde{f} * f(y), f(y)\right\rangle_{tr}\right] \\ &\leq \ 2 \mathop{\mathbb{E}}_{y\sim S}\left[\|f(y)\|_{HS} \cdot \left\|\tilde{f} * f(y)\right\|_{HS}\right] && \text{(Cauchy–Schwarz)} \\ &= \ 2\sqrt{t} \cdot \mathop{\mathbb{E}}_{y\sim S}\left[\left\|\tilde{f} * f(y)\right\|_{HS}\right] && \text{(Using: } f \text{ is unitary-valued.)} \\ &\leq \ 2\sqrt{t} \cdot \left(\mathop{\mathbb{E}}_{y\sim S}\left[\left\|\tilde{f} * f(y)\right\|_{HS}^2\right]\right)^{\frac{1}{2}} && \text{(Cauchy–Schwarz)} \end{aligned}$$

Now we define $\psi(y) = \left\|\tilde{f} * f(y)\right\|_{HS}^2$. Observe that, $\|\psi\|_\infty \leq t$ and it is a positive-definite function by Lemma 3.3. This will allow us to deduce that the $U^2$-norm is large easily. From the computation before, we get,

$$\begin{aligned} \delta'^2 t \ &\leq \ \mathop{\mathbb{E}}_{y\sim S}[\psi(y)] \\ &\leq \ \mathop{\mathbb{E}}_{y\sim G}[\psi(y)] + \varepsilon\|\psi\|_A && \text{(By Lemma 3.1)} \\ &\leq \ \mathop{\mathbb{E}}_{y\sim G}[\psi(y)] + \varepsilon t && \text{(By Lemma 3.3 and Corollary 3.2)} \\ &= \ \mathop{\mathbb{E}}_{y\sim G}\left[\left\|\tilde{f} * f(y)\right\|_{HS}^2\right] + \varepsilon t \\ (\delta'^2 - \varepsilon)\, t \ &\leq \ \|f\|_{U^2} && \text{(By definition of } U^2\text{-norm )} \end{aligned}$$

■

To prove our main result, we need one more component that roughly says that the convolution of functions is mostly supported on low dimensional irreps. The proof is almost identical to the proof of the BNP lemma by Babai, Nikolov, and Pyber [BNP08].

**Claim 4.3.** *Let,* $f, g : G \to M_t(\mathbb{C})$ *and let* $T := \{\rho \in \widehat{G} : d_\rho \geq D\}$*, then the following holds:*

$$\sum_{\rho\in T} d_\rho \left\|\widehat{f * g}\right\|_{HS}^2 \;\leq\; \frac{1}{D}\, \|f\|_2^2\, \|g\|_2^2.$$

*In particular, if* $G$ *is a* $D$*-quasirandom group, then* $\left\|f * g - \mu(f * g)\right\| \leq \frac{1}{\sqrt{D}} \|f\|_2 \|g\|_2$.

*Proof.* From the convolution identity (Fact 2.6), we have:

$$\begin{aligned}
\sum_{\rho\in T} d_\rho \left\|\widehat{f * g}\right\|_{HS}^2 &= \sum_{\rho\in T} d_\rho \left\|\widehat{f}(\rho)\widehat{g}(\rho)\right\|_{HS}^2 && \text{(By convolution identity)}\\
&\leq \sum_{\rho\in T} d_\rho \left\|\widehat{f}(\rho)\right\|_{HS}^2 \left\|\widehat{g}(\rho)\right\|_{HS}^2 && \text{(Norm submultiplicativity)}\\
&\leq \frac{1}{D} \sum_{\rho\in T} d_\rho^2 \left\|\widehat{f}(\rho)\right\|_{HS}^2 \left\|\widehat{g}(\rho)\right\|_{HS}^2 && \text{(Using } d_\rho \geq D \text{ for } \rho \in T)\\
&\leq \frac{1}{D} \sum_{\rho} d_\rho \left\|\widehat{f}(\rho)\right\|_{HS}^2 \sum_{\rho} d_\rho \left\|\widehat{g}(\rho)\right\|_{HS}^2 \\
&= \frac{1}{D} \|f\|_2^2 \|g\|_2^2 && \text{(Parseval's identity)}
\end{aligned}$$

To see the final claim, apply the above to $T := \{\rho \in \widehat{G} : d_\rho \geq D\} = \{\rho \neq \text{triv}\}$ because the group $G$ is $D$-quasirandom. Using Parseval's identity (Fact 2.6) we obtain,

$$\|f * g - \mu(f * g)\|^2 = \sum_{\rho\neq \text{triv}} d_\rho \left\|\widehat{f * g}\right\|_{HS}^2 \leq \frac{1}{D} \|f\|_2^2 \|g\|_2^2. \qquad \blacksquare$$

**Theorem 4.4** (Deranomized Homomorphism Testing)**.** *Let* $G$ *be any finite group, and* $f : G \to \mathbb{U}_t$ *be a unitary matrix-valued function. Let* $S \subseteq G$ *be an* $\varepsilon$*-biased set. Assume that* $f$ *passes the* $BLR_{2\gamma}(G, S, f)$ *test with probability* $\geq \delta(\gamma)$ *for any chosen* $0 \leq \gamma \leq 1$*. Then for* $\eta = (\delta - \gamma)^2 - \varepsilon$*, the following holds,*

1. *There exists* $t' \in [\eta t, \frac{2}{\eta} t]$ *and a function* $g(x) := V\pi(x)U^*$ *where* $\pi$ *is a* $t'$ *dimensional unitary representation,* $U, V$ *are* $t \times t'$ *dimensional partial unitary matrices, such that:*

$$\mathbb{E}_x \left\langle f(x), g(x) \right\rangle_{HS} \geq \frac{\eta^2}{4} t$$

2. *for any integer* $D > 1$*,*

$$\max_{\rho\in\widehat{G}: d_\rho < D} \|\widehat{f}(\rho)\|_{HS}^2 \;\geq\; \eta - \frac{t}{D}$$

*In particular, there exists an irrep* $\rho$ *such that* $d_\rho < \frac{2t}{\eta}$ *such that* $\|\widehat{f}(\rho)\|_{HS}^2 \geq \frac{\eta}{2}$.

*Proof.* From the test passing assumption and Claim 4.2, it follows that: $\|f\|_{U^2} \geq \eta t$. Now applying, Theorem 4.1 gives us the first claim. For the second claim, our starting point is the same:

$$\eta t \leq \|f\|_{U^2} = \|\tilde{f} * f\|^2 = \sum_{\rho\in\widehat{G}} d_\rho \left\|\widehat{\tilde{f} * f}\,(\rho)\right\|_{HS}^2$$

Now we divide $\widehat{G}$ into low and high dimensional irreps by taking $T := \{\rho \in \widehat{G} :\ d_\rho \geq D\}$. We have,

$$\begin{aligned}
\eta t \leq \sum_{\rho \in \widehat{G}} d_\rho \left\|\widehat{\tilde{f} * f}(\rho)\right\|_{HS}^2 &= \sum_{\rho \in \widehat{G} \setminus T} d_\rho \left\|\widehat{\tilde{f} * f}\,(\rho)\right\|_{HS}^2 + \sum_{\rho \in T} d_\rho \left\|\widehat{\tilde{f} * f}\,(\rho)\right\|_{HS}^2 \\
&\leq \sum_{\rho \in \widehat{G} \setminus T} d_\rho \left\|\widehat{\tilde{f} * f}\,(\rho)\right\|_{HS}^2 + \frac{\|\tilde{f}\|^2 \|f\|^2}{D}
\end{aligned}$$

In the inequality step above, we used Claim 4.3. As $f$ is unitary valued, $\|f\|^2 = \|\tilde{f}\|^2 = t$. It follows that: $\sum_{\rho \in \widehat{G} \setminus T} d_\rho \left\|\widehat{\tilde{f} * f}(\rho)\right\|_{HS}^2 \geq \eta t - t^2/D$. Finally, we have,

$$\begin{aligned}
\eta t - t^2/D &\leq \sum_{\rho \in \widehat{G} \setminus T} d_\rho \left\|\widehat{\tilde{f} * f}\,(\rho)\right\|_{HS}^2 \\
&= \sum_{\rho \in \widehat{G} \setminus T} d_\rho \left\|\widehat{f}(\rho)^* \widehat{f}(\rho)\right\|_{HS}^2 && \text{(Convolution identity, Fact 2.6)} \\
&\leq \sum_{\rho \in \widehat{G} \setminus T} d_\rho \|\widehat{f}(\rho)\|_{HS}^4 && \text{(Sub-Multiplicativity.)} \\
&\leq \max_{\rho \in \widehat{G} : d_\rho < D} \|\widehat{f}(\rho)\|_{HS}^2 \cdot \sum_{\rho} d_\rho \|\widehat{f}(\rho)\|_{HS}^2 && \text{(As, } d_\rho \leq D \text{ holds for any } \rho \in \widehat{G} \setminus T) \\
&= \max_{\rho \in \widehat{G} : d_\rho < D} \|\widehat{f}(\rho)\|_{HS}^2 \cdot \|f\|^2 && \text{(Parseval's identity, Fact 2.6)} \\
&= t \cdot \max_{\rho \in \widehat{G} : d_\rho < D} \|\widehat{f}(\rho)\|_{HS}^2 && (f \text{ is unitary, } \|f\|^2 = t) \qquad \blacksquare
\end{aligned}$$

## 5 Derandomized Mixing

The goal of this section is to prove a general "degree–2 mixing lemma" as explained in the introduction for the general case of matrix-valued functions. The assumption of the functions being mean-zero is without loss of generality and only for the sake of brevity.

**Lemma 1.6** (Derandomized Matrix BNP). *Let $G$ be a group such that the dimension of the smallest non-trivial irrep is $D$ and let $S \subseteq G$ be an $\varepsilon$-biased set. Let $f, g : G \longrightarrow M_t(\mathbb{C})$ be mean-zero functions. Then,*

$$\mathop{\mathbb{E}}_{s \sim S}\left[\|(f * g)(s)\|_{HS}^2\right] \leq \left(\frac{1}{D} + \varepsilon\right) \|f\|_2^2 \|g\|_2^2$$

*The usual BNP lemma can be recovered by setting $S = G$, and thus, $\varepsilon = 0$.*

To prove this derandomization, we first prove a more general version of Lemma 3.3, where instead of $\psi(y) = \left\|(\tilde{f} * f)(y)\right\|_{HS}^2$, we have $\psi(y) = \|(f * g)(y)\|_{HS}^2$. This is no longer positive definite as earlier, but we can use elementary representation theory to explicitly give a factorization of the form $\psi(y) = \langle u, \varphi(y) v\rangle$ and thereby compute the algebra norm. The representation $\varphi$ that will come up is defined as follows — let $V \subseteq L_t^2(G \times G)$ be the subspace $V = \operatorname{span}\left\{F(x, y) = f(y) f(x)^* \mid f \in L_t^2(G)\right\}$. Note that $V$ inherits the expectation trace inner product, i.e., $\langle F, H\rangle = \mathbb{E}_{x,y\sim G}[\langle F(x,y), H(x,y)\rangle_{\mathrm{tr}}]$. Then we can define the following representation of G,

$$(\varphi(a)\cdot F)(x,y) = F(xa, ya) = f(ya)f(xa)^*.$$

We are now ready to prove the generalization of Lemma 3.3.

**Lemma 5.1.** *Let* $f, h : G \to M_t(\mathbb{C})$ *and define* $\psi(y) = \|(h * f)(y)\|_{\mathrm{HS}}^2$. *Then,* $\|\psi\|_A \le \|f\|^2\|h\|^2$. *Morever, if the functions are unitary-valued, then* $\|\psi\|_A \le t$.

*Proof.* Let $F(x,y) = f(y)f(x)^*$ and similarly, $\tilde{H}(x,y) = \tilde{h}(y)\tilde{h}(x)^*$. Now,

$$\begin{aligned}
\psi(a) &= \left\| \mathop{\mathbb{E}}_{x\sim G}\left[h(x^{-1})f(xa)\right]\right\|^2 \\
&= \left\langle \mathop{\mathbb{E}}_{x\sim G}\left[\tilde{h}(x)^* f(xa)\right], \mathop{\mathbb{E}}_{y\sim G}\left[\tilde{h}(y)^* f(ya)\right]\right\rangle_{\mathrm{tr}} \\
&= \mathop{\mathbb{E}}_{x,y\sim G}\left[\left\langle \tilde{h}(x)^* f(xa), \tilde{h}(y)^* f(ya)\right\rangle_{\mathrm{tr}}\right] \\
&= \mathop{\mathbb{E}}_{x,y\sim G}\left[\left\langle \tilde{h}(y)\tilde{h}(x)^*, f(ya)f(xa)^*\right\rangle_{\mathrm{tr}}\right] \\
&= \mathop{\mathbb{E}}_{x,y\sim G}\left[\left\langle \widetilde{H}(x,y), \varphi(a)\, F(x,y)\right\rangle_{\mathrm{tr}}\right] \\
&= \left\langle \widetilde{H}, \varphi(a)\, F\right\rangle
\end{aligned}$$

By the definition of algebra norm Definition 2.7, we have $\|\psi\|_A \le \|H\|\cdot\|F\|$. Now,

$$\|F\|^2 = \mathop{\mathbb{E}}_{x,y}\left[\|f(y)f(x)^*\|_{\mathrm{HS}}^2\right] \le \mathop{\mathbb{E}}_{x,y}\left[\|f(y)\|_{\mathrm{HS}}^2\|f(x)^*\|_{\mathrm{HS}}^2\right] = \|f\|^4.$$

The inequality here follows from sub-multiplicativity. Similarly, $\|\widetilde{H}\| = \|h\|^2$. This proves the first claim. When the functions map to unitary matrices, $\widetilde{H}(x,y), F(x,y)$ are unitary and thus, $\|\widetilde{H}(x,y)\|_{\mathrm{HS}}^2 = \|F(x,y)\|_{\mathrm{HS}}^2 = t$ for every $x, y \in G$. We can thus avoid using sub-multiplicativity and directly obtain,

$$\|F\|^2 = \mathop{\mathbb{E}}_{x,y}\left[\|f(y)f(x)^*\|_{\mathrm{HS}}^2\right] = t = \|\widetilde{H}\|^2. \qquad \blacksquare$$

**Remark 5.2.** One can weaken the unitary assumption by requiring that f is "unitary on average", an assumption also used in [MR15]. This is because $\|F\| = \|\mathbb{E}_x[f(x)f(x)^*]\|_{\mathrm{HS}}$.

**Lemma 1.6** (Derandomized Matrix BNP). *Let* G *be a group such that the dimension of the smallest non-trivial irrep is* D *and let* $S \subseteq G$ *be an* $\varepsilon$*-biased set. Let* $f, g : G \to M_t(\mathbb{C})$ *be mean-zero functions. Then,*

$$\mathop{\mathbb{E}}_{s\sim S}\left[\|(f * g)(s)\|_{\mathrm{HS}}^2\right] \le \left(\frac{1}{D} + \varepsilon\right)\|f\|_2^2\|g\|_2^2$$

*The usual BNP lemma can be recovered by setting* $S = G$, *and thus,* $\varepsilon = 0$.

*Proof.* From Lemma 5.1, we have that the function, $\psi(s) := \|(f * g)(s)\|_{HS}^2$ has algebra norm $\|f\|_2^2 \|g\|_2^2$ and therefore from Lemma 3.1 we have that averaging over $S$ is $\varepsilon$-close to true average. Thus,

$$\begin{aligned}\mathop{\mathbb{E}}_{s\sim S}\left[\|(f*g)(s)\|_{HS}^2\right] &\le \mathop{\mathbb{E}}_{s\sim G}\left[\|(f*g)(s)\|_{HS}^2\right] + \varepsilon\|f\|_2^2\|g\|_2^2 && \text{(Using Lemma 3.1)}\\ &\le \frac{1}{D}\|f\|_2^2\|g\|_2^2 + \varepsilon\|f\|_2^2\|g\|_2^2 && \text{(Using Claim 4.3)} \quad \blacksquare\end{aligned}$$

## Acknowledgements

We are grateful to Fernando Granha Jeronimo for several illuminating conversations in the early phase of this work and to Madhur Tulsiani for closely looking at the draft and providing several helpful suggestions.

## References

[AGHP92] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures & Algorithms*, 3(3):289–304, 1992. 5, 11

[AR94] Noga Alon and Yuval Roichman. Random Cayley Graphs and Expanders. 5(2):271–285, 1994. doi:10.1002/rsa.3240050203. 5

[BCH+95] 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. 2, 6, 9

[BFL03] László Babai, Katalin Friedl, and András Lukács. Near representations of finite groups, 2003. Manuscript. 4, 6, 11

[BHR22] Amey Bhangale, Prahladh Harsha, and Sourya Roy. Mixing of 3-term progressions in Quasirandom Groups. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, pages 20:1–20:9, 2022. arXiv:2109.12627, doi:10.4230/LIPIcs.ITCS.2022.20. 7

[BK21] 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. 1

[BKM22] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-CSPs: I. In *Proceedings of the 54th ACM Symposium on Theory of Computing*, 2022. doi:10.1145/3519935.3520028. 1, 7

[BLR90] 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. 1, 6, 9

[BNP08] László Babai, Nikolay Nikolov, and László Pyber. Product growth and mixing in finite groups. In *Proceedings of the 19th ACM-SIAM Symposium on Discrete Algorithms*, 2008. 7, 9, 16

[BOCLR07] 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. 2, 6, 9

[BP18] Roman Badora and Barbara Przebieracz. On approximate group homomorphisms. *Journal of Mathematical Analysis and Applications*, 462(1):505–520, 2018. doi:10.1016/j.jmaa.2018.02.017. 2, 9

[BSVW03] 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. 2, 5, 6, 10

[DCOT18] Marcus De Chiffre, Narutaka Ozawa, and Andreas Thom. Operator algebraic approach to inverse and stability theorems for amenable groups. *Mathematika*, 65(1):98–118, August 2018. arXiv:1706.04544, doi:10.1112/s0025579318000335. 15

[DETT10] Anindya De, Omid Etesami, Luca Trevisan, and Madhur Tulsiani. Improved pseudorandom generators for depth 2 circuits. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, 2010. doi:10.1007/978-3-642-15369-3_38. 13

[Eym64] P. Eymard. L’algébre de Fourier d’un groupe localement compact. *Bulletin de la Société Mathématique de France*, 92:181–236, 1964. doi:10.24033/bsmf.1607. 8, 12

[Far00] Ilijas Farah. Approximate homomorphisms II: Group homomorphisms. *Combinatorica*, 20(1):47–60, 2000. doi:10.1007/s004930070030. 2, 9

[GGMT23] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of marton, 2023. arXiv:2311.05762. 6, 10

[GH17] William Timothy Gowers and Omid Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12):1784, 2017. arXiv:1510.04085, doi:10.1070/SM8872. 3, 4, 5, 6, 9, 11, 15

[Gow08] W. T. Gowers. Quasirandom Groups. *Combinatorics, Probability and Computing*, 17(3):363–387, May 2008. arXiv:0710.3877, doi:10.1017/S0963548307008826. 7

[GS08] Benjamin Green and Tom Sanders. A quantitative version of the idempotent theorem in harmonic analysis. *Annals of Mathematics*, 168(3):1025–1054, November 2008. doi:10.4007/annals.2008.168.1025. 13

[HH24] Pooya Hatami and William Hoza. Paradigms for unconditional pseudorandom generators. *Foundations and Trends in Theoretical Computer Science*, 16(1-2):1–210, 2024. doi:10.1561/0400000109. 10

[HHH22] Lianna Hambardzumyan, Hamed Hatami, and Pooya Hatami. Dimension-free bounds and structural results in communication complexity. *Israel Journal of Mathematics*, 253(2):555–616, October 2022. doi:10.1007/s11856-022-2365-8. 12

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(04):439–562, 2006. doi:10.1090/S0273-0979-06-01126-8. 10

[HW03] 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. 2, 9

[JMRW22] Fernando Granha Jeronimo, Tushant Mittal, Sourya Roy, and Avi Wigderson. Almost Ramanujan Expanders from Arbitrary Expanders via Operator Amplification. In *Proceedings of the 63rd IEEE Symposium on Foundations of Computer Science*, 2022. arXiv:2209.07024, doi:10.1109/FOCS54457.2022.00043. 6, 11

[JNV$^+$21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *Commun. ACM*, 64(11):131–138, 2021. doi:10.1145/3485628. 1, 3

[Kas07] Martin Kassabov. Symmetric groups and expander graphs. *Inventiones mathematicae*, 170(2):327–354, November 2007. doi:10.1007/s00222-007-0065-y. 6

[Kiw03] 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. 6, 10

[KM93] Eyal Kushilevitz and Yishay Mansour. Learning decision trees using the fourier spectrum. *SIAM Journal on Computing*, 22(6):1331–1348, 1993. doi:10.1137/0222080. 13

[KM23] Z. Kelley and R. Meka. Strong bounds for 3-progressions. In *Proceedings of the 64th IEEE Symposium on Foundations of Computer Science*, pages 933–973, 2023. arXiv:2302.05537, doi:10.1109/FOCS57990.2023.00059. 8

[KN06] Martin Kassabov and Nikolay Nikolov. Universal lattices and Property τ. *Inventiones mathematicae*, 165(1):209–224, July 2006. arXiv:math/0502112, doi:10.1007/s00222-005-0498-0. 6

[Lub11] Alexander Lubotzky. Finite simple groups of Lie type as expanders. *Journal of the European Mathematical Society*, pages 1331–1341, 2011. doi:10.4171/JEMS/282. 6

[MR15] 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. arXiv:1009.6230, doi:10.1137/140958578. 3, 4, 5, 6, 11, 19

[NN90] J. Naor and M. Naor. Small-bias probability spaces: efficient constructions and applications. In *Proceedings of the 22nd ACM Symposium on Theory of Computing*, pages 213–223, 1990. doi:10.1137/0222053. 11

[NN93] J. Naor and M. Naor. Small-bias probability spaces: efficient constructions and applications. *SIAM Journal on Computing*, 22(4):838–856, 1993. doi:10.1137/0222053. 5, 10

[NV17] 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. 1, 3

[OSP23] Ryan O'Donnell, Rocco A. Servedio, and Pedro Paredes. Explicit orthogonal and unitary designs. In *Proceedings of the 64th IEEE Symposium on Foundations of Computer Science*, 2023. doi:10.1109/FOCS57990.2023.00073. 11

[Sam07] A. Samorodnitsky. Low-degree tests at large distances. In *Proceedings of the 39th ACM Symposium on Theory of Computing*, pages 506–515, 2007. 6, 10

[San11] Tom Sanders. A Quantitative Version of the Non-Abelian Idempotent Theorem. *Geometric and Functional Analysis*, 21(1):141–221, February 2011. doi:10.1007/s00039-010-0107-2. 12, 13

[San12] Tom Sanders. On the Bogolyubov-Ruzsa lemma. *Analysis & PDE*, 5(3), 2012. arXiv:1011.0107, doi:10.2140/apde.2012.5.627. 6, 10

[San21] Tom Sanders. Coset decision trees and the Fourier algebra. *Journal d'Analyse Mathématique*, 144(1):227–259, December 2021. doi:10.1007/s11854-021-0179-y. 8, 12

[ST00] Alex Samorodnitsky and Luca Trevisan. A PCP characterization of NP with optimal amortized query complexity. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, 2000. doi:10.1145/335305.335329. 2

[STV17] Amir Shpilka, Avishay Tal, and Ben Lee Volk. On the Structure of Boolean Functions with Small Spectral Norm. *Computational Complexity*, 26(1):229–273, March 2017. doi:10.1007/s00037-015-0110-y. 8, 13

[SW04] Amir Shpilka and Avi Wigderson. Derandomizing Homomorphism Testing in General Groups. In *Proceedings of the 36th ACM Symposium on Theory of Computing*, page 18, 2004. doi:10.1137/S009753970444658X. 2, 6, 9

[WX08] Avi Wigderson and David Xiao. Derandomizing the Ahlswede-Winter matrix-valued Chernoff bound using pessimistic estimators, and applications. *Theory of Computing*, 4(3):53–76, 2008. doi:10.4086/toc.2008.v004a003. 5