Pseudorandomness of Expander Walks via Fourier Analysis on Groups

Fernando Granha Jeronimo
University of Illinois Urbana-Champaign, IL, USA

Tushant Mittal
Stanford University, CA, USA

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

Abstract

A long line of work has studied the pseudorandomness properties of walks on expander graphs. A central goal is to measure how closely the distribution over n-length walks on an expander approximates the uniform distribution of n-independent elements. One approach to do so is to label the vertices of an expander with elements from an alphabet Σ, and study closeness of the mean of functions over Σ^n, under these two distributions. We say expander walks ε-fool a function if the expander walk mean is ε-close to the true mean. There has been a sequence of works studying this question for various functions, such as the XOR function, the AND function, etc. We show that:

- The class of symmetric functions is $O(|\Sigma|\lambda)$-fooled by expander walks over any generic λ-expander, and any alphabet Σ . This generalizes the result of Cohen, Peri, Ta-Shma [STOC'21] which analyzes it for $|\Sigma| = 2$, and exponentially improves the previous bound of $O(|\Sigma|^{O(|\Sigma|)}\lambda)$, by Golowich and Vadhan [CCC'22]. Moreover, if the expander is a Cayley graph over $\mathbb{Z}_{|\Sigma|}$, we get a further improved bound of $O(\sqrt{|\Sigma|}\lambda)$.

Morever, when Σ is a finite group G, we show the following for functions over G^n:

- The class of symmetric class functions is $O\left(\frac{\sqrt{|G|}}{D}\lambda\right)$-fooled by expander walks over "structured" λ-expanders, if G is D-quasirandom.
- We show a lower bound of $\Omega(\lambda)$ for symmetric functions for any finite group G (even for "structured" λ-expanders).
- We study the Fourier spectrum of a class of non-symmetric functions arising from *word maps*, and show that they are exponentially fooled by expander walks.

Our proof employs Fourier analysis over general groups, which contrasts with earlier works that have studied either the case of $\mathbb{Z}_2$ or $\mathbb{Z}$. This enables us to get quantitatively better bounds even for unstructured sets.

2012 ACM Subject Classification Theory of computation → Pseudorandomness and derandomization

Keywords and phrases Expander graphs, pseudorandomness

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2025.49

Category RANDOM

Related Version *Full version*: https://www.arxiv.org/abs/2507.14445

Funding *Tushant Mittal*: Research supported by NSF grants CCF-2143246 and CCF-2133154.
Sourya Roy: Research supported by the Old Gold Summer Fellowship from The University of Iowa.

1 Introduction

Expander graphs are fundamental pseudorandom objects with a vast range of applications in computer science and mathematics [13, 26, 17]. These graphs combine two opposing properties of being well-connected yet sparse. In many ways, they exhibit behavior that

is surprisingly close to truly random, thereby being used to replace randomness and yield several explicit constructions. For instance, explicit codes approaching the random guarantees of the Gilbert–Varshamov [7, 27] bound [24] or the generalized Singleton [23, 21] bound can be constructed using expanders [16]. Moreover, expanders can be used to construct a variety of pseudorandom generators [14, 12].

Walks on expander graphs not only mix fast, but they are an important derandomization tool for the Chernoff bound [8, 6], the hitting set property [1, 25], etc. These tasks can be phrased in a more general and unified way as how well expander walks fool a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$. In this setting, the vertices, V_X, of an expander graph X, are labelled with bits $\{0,1\}$ and instead of evaluating f under the uniform distribution on n bits, we evaluate it under the distribution on $\{0,1\}^n$ induced by taking a random walk on X of length n. To quantify the error incurred in this process of replacing true randomness by expander walks, it is convenient to define $\mathcal{E}_X(f)$ as:

$$\mathcal{E}_X(f) \;=\; \left|\mathbb{E}_{s\sim V_X^n}\left[f(s)\right] - \mathbb{E}_{s\sim \mathrm{RW}_n}\left[f(s)\right]\right| .$$

In this language, by choosing f to be the AND function on n bits, we recover the expander hitting set property application. The choice of f as a (suitable) threshold function on n bits leads to the expander Chernoff bound. The choice of f as the XOR function on n bits (and a carefully constructed X) leads to the breakthrough code construction of Ta-Shma [24].

Using this unified perspective, Cohen, Peri, and Ta-Shma [4] developed a systematic framework to analyze expander random walks and obtain bounds on $\mathcal{E}_X(f)$. Their framework is based on Fourier analysis and exploits the fact that any Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ can be expressed in the Fourier basis as a linear combination of characters, which are XOR functions in this case. They obtained bounds on $\mathcal{E}_X(f)$ in terms of the spectral expansion λ of the (normalized) adjacency matrix of X.

A series of works [10, 3, 9] have since extended the [4] framework to functions of the form $f\colon \Sigma^n \to \mathbb{C}$, where Σ is a finite alphabet. These works study *symmetric functions* – functions that are invariant under any permutation of the input coordinates – and functions computed by restricted circuit classes such as AC^0. Golowich and Vadhan [10] get the following bound for symmetric functions:

$$|\mathcal{E}_X(f)| \;\leq\; (|\Sigma|^{O(|\Sigma|)} \cdot \lambda).$$

They asked whether such an exponential dependence on $|\Sigma|$ is optimal. In this work, we improve this bound to $O(|\Sigma| \cdot \lambda)$ by viewing a function $f : \Sigma^n \to \mathbb{C}$ as a function $f : \mathbb{Z}_{|\Sigma|}^n \to \mathbb{C}$ which enables us to use a Fourier basis. More interestingly, this change of perspective motivates us to consider graphs that can utilize this algebraic structure, such as Cayley graphs over $\mathbb{Z}_{|\Sigma|}$. This idea helps us get a bound of $O(\sqrt{|\Sigma|} \cdot \lambda)$ for Cayley expanders, further improving upon our bound of $O(|\Sigma| \cdot \lambda)$ for arbitrary expanders.

Functions over Groups

More broadly, the above suggests investigating functions over general finite groups (instead of just $\mathbb{Z}_{|\Sigma|}$) and considering expanders with a compatible algebraic structure. This opens up interesting directions to study:

1. What novel classes of functions $f : G^n \to \mathbb{C}$ can we study that utilize the group operation, or have richer symmetries coming from the group? For instance, *class functions*, i.e., functions that satisfy $f(x) = f(gxg^{-1})$ for every $x, g \in G$.
2. Can one obtain stronger bounds on $\mathcal{E}_X(f)$ for such function classes when the expander X has algebraic structure?
3. How can one utilize the pseudorandomness properties of the group itself, such as *quasirandomness*?

While these questions are very natural in their own right, studying functions over general groups has been fruitful in the context of complexity theory. For instance, the famed Barrington's theorem [2] effectively reinterprets a Boolean function as a function over the permutation group. More recently, [15] showed that one can obtain improved expanders by studying pseudorandomness for functions over the permutation group.

1.1 Our Results

We initiate a study of this general setup and make progress in answering these questions. We (i) give a general lemma about the pseudorandomness for matrix-valued functions (over arbitrary expanders), which is needed to work with Fourier decompositions of non-abelian groups, (ii) analyze specific function classes of symmetric functions and *word functions* over a group G, and (iii) we study symmetric *class functions* over structured expanders, and show that the quasirandomness of the group G synergizes with the randomness of the expander X to yield improved bounds, and finally, (iv) we prove a lower bound for the fooling of symmetric functions even over such structured expanders.

1.1.1 Pseudorandomness of generic expanders

We begin by considering an abstract problem about expander walks. Let X be an expander and consider a set of k matrix-valued mean-zero functions:

$$\left\{f_j : X \to \mathbb{C}^{d_j \times d_j} \mid j \in [k]\right\}, \quad \max_x \|f_j(x)\|_{\mathrm{op}} \leq 1.$$

Given an ordered subset $\mathcal{S} = \{i_1 < i_2 < \cdots < i_{k-1} < i_k\}$ of indices, we wish to study the expression,

$$\mathcal{E}_{X,\mathcal{S}}\left(f_1 \otimes \cdots \otimes f_k\right) \;:=\; \left\|\mathbb{E}_{\vec{x} \sim \mathsf{RW}_n}[f_1(x_{i_1}) \otimes \cdots \otimes f_k(x_{i_k})]\right\|_{\mathrm{op}}$$

Note that the above expression is identically 0 if X is a complete graph (with self-loops) as the functions, f_i, have zero mean. The goal is to show that above quantity is small when we have a λ-expander. Analyzing special cases of such quantity is at the heart of several past works [4, 15, 20] that studied pseudorandomness of expander walks. For the setting of matrix-valued functions, the result of [15] gives the following bound on the expression:

▶ **Theorem 1** ([15]). *Let X be any λ-expander and $\{f_1, \ldots, f_k\}$ be a collection of mean-zero normalized matrix-valued functions for $k \geq 2$. Then for any k-sized subset of indices, $\mathcal{S}$,*

$$\mathcal{E}_{X,\mathcal{S}}\left(f_1 \otimes \cdots \otimes f_k\right) \;\leq\; (2\lambda)^{\lfloor \frac{k}{2} \rfloor}.$$

The above result is agnostic to the set $\mathcal{S}$ and gives a general worst-case bound. But this is too pessimistic when $\mathcal{S}$ has large gaps. For instance, if $\mathcal{S} = \{1, 4, 9\}$, the above result gives a bound of λ which is far from the optimal (could be as small as λ^8). We prove a result that takes the structure of $\mathcal{S}$ into account and gives an improved guarantee when $\mathcal{S}$ has large gaps.

▶ **Theorem 2** (Matrix-Valued Fooling, Theorem 19). *Let X be any λ-expander and $\{f_1, \ldots, f_k\}$ be a collection of mean-zero matrix-valued functions for $k \geq 2$. Then for any k-sized subset of indices, $\mathcal{S}$,*

$$\mathcal{E}_{X,\mathcal{S}}\left(f_1 \otimes \cdots \otimes f_k\right) \;\leq\; \lambda^{\eta(\mathcal{S})} \;\leq\; (4\lambda)^{\lfloor \frac{k}{2} \rfloor}.$$

where $\eta(\mathcal{S})$ is an explicit function.

The above bound is an improvement (over Theorem 1) when $\mathcal{S}$ has large gaps. Theorem 2 generalizes the result of [4], who achieved the same improvement over the result of Ta-Shma [24] for $\{\pm 1\}$-valued functions. This quantitative improvement was crucially used by [4] to prove their result about fooling functions over $\{0,1\}^n$, and we use it similarly to prove it for functions over an arbitrary alphabet, Σ^n.

The above theorem connects with fooling functions via Fourier analysis. Let G be a group, and $f : G^n \to \mathbb{C}$ be any function. Consider a labeling[1] map, $\varphi : X \to G$. Then, $f \circ \varphi : X^n \to \mathbb{C}$, and the term we wish to bound is:

$$\mathcal{E}_X(f) \;:=\; \left| \mathop{\mathbb{E}}_{\vec{x}\sim \mathsf{RW}_n} \left[f\big(\varphi(x_1), \ldots, \varphi(x_n)\big) \right] - \mathop{\mathbb{E}}_{\vec{x}\sim \mathrm{Unif}_n} \left[f\big(\varphi(x_1), \ldots, \varphi(x_n)\big) \right] \right| .$$

Furthermore, since f is a function on a product group, G^n, we can apply the general Fourier transform to express f as a linear combination of matrix-valued tensor functions[2]. These tensor functions (when composed with φ) can be analyzed using Theorem 2. This can be seen as a generalization of the Fourier analytic approach of [4], who study symmetric functions over $\mathbb{Z}_2^n$. As a first application, we use our generalization from $\mathbb{Z}_2^n$ to $\mathbb{Z}_{|\Sigma|}^n$, to prove Theorem 3. Additionally, the ability to work with a general Fourier basis is utilized for other results where the function uses group structure for a given (potentially non-Abelian) group G, such as for *group products* (Theorem 5), and our general lower bound (Theorem 9).

1.1.2 Fooling symmetric functions and word functions

We analyze the fooling of symmetric functions, ie functions $f : \Sigma^n \to \mathbb{C}$ that is invariant under permuting the input coordinates, for any finite alphabet Σ.

▶ **Theorem 3** (Fooling symmetric functions, Theorem 32). *Let f be any symmetric function, $f : \Sigma^n \to \mathbb{C}$ where Σ is any finite set. Let X be a λ-expander such that $\lambda < \frac{1}{16e|\Sigma|}$. Then for any unbiased labelling of X with Σ,*

$$|\mathcal{E}_X(f)| \;\leq\; (32e\lambda|\Sigma|) \cdot \|f\|_2 \quad .$$

Moreover, if $\|f\|_2 = o_n(1)$ – for example, the weight indicator function which satisfies $\|f\|_2 = n^{-1/4}$ – one obtains a vanishing decay.

This improves the previous best bound of $(|\Sigma|^{O(|\Sigma|)} \cdot \lambda)$ due to Golowich and Vadhan [10]. Our analysis relies on using a Fourier basis for such functions that can be obtained by viewing Σ instead as $\mathbb{Z}_\Sigma$, and then applying Theorem 2. However, our proof is agnostic to this specific choice of group and can instead work with a Fourier basis over any group (of size $|\Sigma|$) by using Theorem 2.

Word Functions and Group Products

Going beyond symmetric functions, we analyze "non-commutative" monomial functions, which we call *word* functions.

---

[1] We only work with unbiased labelings, i.e., those that induce the uniform distribution on G.

[2] Theorem 2 enables the possibility of working with orthonormal bases other than the Fourier basis. Any reasonably "flat" orthonormal basis where the basis elements satisfy certain pointwise bound and contains the invariant vector (i.e., the all 1 vector) can be used.

▶ **Definition 4** (Monomial word function). *For an ordered subset $\mathcal{S} \subseteq [n]$, a monomial word is a map, $w_{\mathcal{S}} : G^n \to G$, defined as $w_{\mathcal{S}} = \prod_{s\in S} g_s^{e_s}$ where $e_S \in \{\pm 1\}$. A function $f : G^n \to \mathbb{C}$ is a monomial word function of degree k, if $f = h(w_{\mathcal{S}}(g_1, \cdots, g_n))$ for some $\mathcal{S}$ of size k and a function $h : G \to \mathbb{C}$.*

We give a complete characterization of the Fourier spectrum of *monomial word functions*, and show that these have Fourier support on the highest level and thus are analogs of the PARITY function over $\mathbb{Z}_2^n$. Moreover, this support is sparse (see Lemma 34), and this enables us to use Theorem 2. We thus deduce that such functions are exponentially fooled by expander walks.

▶ **Theorem 5** (Fooling word functions, Theorem 35). *Let $f : G^n \to \mathbb{C}$ be a word function of degree k corresponding to a set $\mathcal{S}$. Then for any expander X with an unbiased G-labelling,*

$$|\mathcal{E}_X(f)| \;\le\; \lambda^{\eta(\mathcal{S})} \cdot |G|^{\frac{k}{2}} \cdot \|f\|_2 \;\le\; (2\lambda)^{\lfloor \frac{k}{2} \rfloor} \cdot |G|^{\frac{k}{2}} \cdot \|f\|_2.$$

One important case of this class of functions is the group product functions, namely, Boolean valued functions f that take $x_1, \ldots, x_k \in G$ as input and output 1 if and only if the product is equal to some target element $t \in G$. Fooling group product functions is a crucial component in the construction of some pseudorandom generators for branching programs, e.g., [18, 5].

We sharpen Theorem 5 for group product functions by removing the dependence on $|G|$ in the error bound while achieving the same exponential decay in terms of expansion.

▶ **Theorem 6** (Fooling Group Products, Theorem 37). *Let G be any finite group, $t \in G$, and $f(\vec{x}) = \mathbb{1}_{\{x_1 \cdots x_k = t\}}$ be a group product. Then for any expander X with an unbiased G-labelling,*

$$|\mathcal{E}_X(f)| \;\le\; (2\lambda)^{k/2}\,.$$

1.1.3 Pseudorandomness of structured expanders

The above results hold for generic expanders, but since our function is defined on a group, it is natural to consider "structured" expanders that gel well with the group. In the case of Abelian groups, these are just *Cayley graphs*, using which we obtain a further improvement to Theorem 3.

▶ **Theorem 7** (Abelian Groups, Corollary 27 and Proposition 42). *Let G be an Abelian group and X be a Cayley graph on G and let $\{\chi_j \mid j \in [k]\}$ be a set of non-trivial characters of G. Then for any ordered subset $\mathcal{S}$ of size k,*

$$\mathcal{E}_{X,\mathcal{S}}(\chi_1 \otimes \cdots \otimes \chi_k) \;\le\; \lambda^{\eta(\mathcal{S})} \cdot \mathbb{1}_{\{\chi_1 \cdots \chi_k = \mathrm{triv}\}}\,.$$

As a consequence, for every symmetric function $f : \Sigma^n \to \mathbb{C}$ and Cayley expander X,

$$\left|\mathcal{E}_X(f)\right| \;\le\; O\Big(\sqrt{|\Sigma|} \cdot \lambda\Big) \cdot \|f\|_2\,.$$

For $G = \mathbb{Z}_2$, this result says that the odd degree characters are perfectly fooled, and thus, every odd function $f : \mathbb{Z}_2^n \to \mathbb{C}$ is perfectly fooled by such a structured expander. This already illustrates the improvement over generic expanders.

To generalize this to general non-abelian groups, we need to restrict to *class functions*, i.e., functions such that $f(gxg^{-1}) = f(x)$ for every $x, g \in G$. Note that for Abelian groups, every function is a class function, as the condition is trivially true due to commutativity. Moreover, we will need a stronger notion of a "pseudo Cayley graph" for which we omit the formal definition here (see Definition 21). The key property of these graphs is that their eigenvectors are given by the Fourier basis functions.

Tighter Bound for Quasirandom Groups

An often seen phenomenon is that one gets better pseudorandomness properties for groups that are *highly non-abelian*. One way to quantify this is the notion of a *D-quasirandom groups* introduced in a seminal work by Gowers [11] which is a group in which the smallest (non-trivial) irreducible representation (see Definition 13) has dimension D. Abelian groups are 1-quasirandom, whereas on the other extreme, there are matrix groups that are $|G|^{\frac{1}{3}}$-quasirandom (see [11]). We show that such a gain does indeed occur in our setting as well.

▶ **Theorem 8** (General Groups, Corollary 27 and Proposition 42)**.** *Let G be a D-quasirandom group and let X be a "pseudo Cayley" graph on G. Let $\{\chi_j \mid j \in [k]\}$ be a set of non-trivial characters of G, normalized by their dimension. Then for any ordered subset $\mathcal{S}$ of size k,*

$$\mathcal{E}_{X,\mathcal{S}}(\chi_1 \otimes \cdots \otimes \chi_k) \;\leq\; \lambda^{\eta(\mathcal{S})} \cdot \langle \chi_{\text{triv}},\, \chi_1 \cdots \chi_k \rangle.$$

As a consequence, for every symmetric class function $f : G^n \to \mathbb{C}$,

$$\left|\mathcal{E}_X(f)\right| \;\leq\; O\left(\frac{\sqrt{|G|}}{D} \cdot \lambda\right) \cdot \|f\|_2.$$

Apart from the quasirandomness factor, the key improvement from Theorem 2 here is the extra factor of $\langle \chi_{\text{triv}},\, \chi_1 \cdots \chi_k \rangle$. This counts the fractional dimension of the trivial irrep inside the tensor representation $\rho_1 \otimes \cdots \otimes \rho_k$. This quantity is much smaller than one, for instance, when $k = 2$, it is at most $\frac{1}{D^2}$. Moreover, this quantity can be computed explicitly using basic representation theory, which yields a more precise upper bound.

1.1.4 Lower Bounds

We show that our dependence on λ in the bound of $|\mathcal{E}_X(f)|$ in Theorem 3 cannot be improved in general, no matter the choice of group G. Let, $A \subseteq G$ and $t \in [n]$. We define a symmetric boolean function $\text{Th}_{A,t}$ as :

$$\text{Th}_{A,t}(\vec{x}) = 1 \quad \text{if} \;\; |\{i \mid x_i \in A\}| \geq t; \;\; 0 \;\; \text{otherwise.}$$

▶ **Theorem 9** (Lower Bound for any group)**.** *Let G be any finite group, and $A \subseteq G$ be any subset such that $\frac{|A|}{|G|} = \frac{1}{2}$. There exists an λ-expander X such that for every n large enough,*

$$\left|\mathcal{E}_X\left(\text{Th}_{A,\frac{n+1-\sqrt{n}}{2}}\right)\right| \;\geq\; \Omega(\lambda).$$

This lower bound holds even when X is a "pseudo Cayley graph" (as in Theorem 8) on G.

This lower bound places a limitation on how much the quasirandomness of the group or the algebraic structure of the expander can be leveraged in terms of the pseudorandomness of expander walks with respect to symmetric functions.

Regardless of how "far" from Abelian the group G is, a lower bound of $\Omega(\lambda)$ still persists. This lower bound rules out the possibility of an upper bound of, say, $\frac{\lambda}{D}$ for a D-quasirandom group in Theorem 3. More importantly, it shows that even if one uses an expander with such Cayley-like algebraic structure, one cannot improve the linear dependence on λ.

We stress that proving this lower bound for general finite groups is substantially more challenging than for the $\mathbb{Z}_2^k$ case [3]. In general, this requires the function and the graph to "interact" in a non-trivial way, but now, in the presence of (possibly) higher-dimensional representations, this is substantially more delicate to achieve (see Section 1.2).

1.2 Proof techniques

A generalized "Ignore First Step" Trick

To prove our first main result (Theorem 2), we generalize the technique of [20] (also, subsequently used in [19]) that introduced a trick that they called "Ignore First Step" Trick. We generalize this in two significant ways. We first extend it to the setup of general matrix-valued functions. More importantly, we perform a finer analysis to obtain a dependence on λ that takes into account the subset of indices $\mathcal{S}$. This is necessary to yield a bound of $\lambda^{\eta(\mathcal{S})}$ as opposed to $\lambda^{\lfloor k/2 \rfloor}$ (even for scalar-valued functions) that would be implied by [20].

We give a quick overview of this technique in the very special setup of $\{\pm 1\}$-valued functions that are all identical. We wish to analyze the term:

$$\mathop{\mathbb{E}}_{(x_1,\ldots,x_n)\sim \mathrm{RW}_n}[f_1(x_1)\cdots f_k(x_k)].$$

This corresponds to $\mathcal{S} = \{1,\ldots,k\}$. Let us start with $k = 2$. This case can be directly handled by the expander mixing lemma, which says that for a λ-spectral expander,

$$\left| \mathop{\mathbb{E}}_{(x_1,x_2)\sim \mathrm{RW}_2}[f(x_1)\, f(x_2)] \;-\; \left(\mathop{\mathbb{E}}_{x\sim \mathrm{RW}_1}[f(x)]\right)^2 \right| \;\leq\; \lambda \cdot \mathop{\mathbb{E}}_{x\sim \mathrm{RW}_1}\left[|f(x)|^2\right].$$

One interpretation of this lemma is that it reduces the analysis of the mean of the product function over 2-length walks to the analysis of the mean and variance of the function over a walk of length 1. The main idea behind the technique is to do such a reduction from a length k-walk to analyzing mean and variance over $(k-1)$-length walks.

We do not get into the details of this reduction but explain the trick used to bound such variance terms, the simplest case of which is when $k = 3$. For a vertex x, let $\mathrm{RW}_1(x)$ be the distribution of 1-length walks starting from x. The term we need to analyze is,

$$\mathop{\mathbb{E}}_{x\sim \mathrm{RW}_1}\left[\left|\mathop{\mathbb{E}}_{y\sim \mathrm{RW}_1(x)}[f(x)f(y)]\right|^2\right] \;=\; \mathop{\mathbb{E}}_{x\sim \mathrm{RW}_1}\left[|f(x)|^2 \mathop{\mathbb{E}}_{y,z\sim \mathrm{RW}_1(x)}\left[f(y)\overline{f(z)}\right]\right]$$

The key technical point is the following. The expression on the right formally depends on x but since $f(x)^2 = 1$, this dependence is virtual. More importantly, the distribution on y, z in this expression is the same as sampling y, z independently (of x) at distance 2 in the graph,

$$\mathop{\mathbb{E}}_{x\sim \mathrm{RW}_1}\left[\mathop{\mathbb{E}}_{y,z\sim \mathrm{RW}_1(x)}\left[f(y)\overline{f(z)}\right]\right] \;=\; \mathop{\mathbb{E}}_{(y,z)\sim \mathrm{RW}'_2}\left[f(y)\overline{f(z)}\right].$$

The right-hand side can now be analyzed by applying the above expander mixing lemma on the graph X^2. Thus, this trick gets rid of the first variable x, and reduces the variance of 2-length walks to the mean of 1-length walk (on the squared graph).

Our proof follows a similar approach, but there are two key complications. One, the functions we need to analyze are matrix-valued, and secondly, the above analysis does not utilize the gaps in the index set $\mathcal{S}$, and therefore would give a bound akin to [15, 24] which is too weak for our purposes.

Let $\mathcal{S} = (i_1, \cdots, i_k)$, and let $\Delta_j := i_{j+1} - i_j$ be the j^{th} gap. To bound the recurrence more tightly, we view the random walk as a sequence of k steps, where the j^{th} step is on the graph X^{Δ_j}. To implement this approach in the general setup of tensors of operator-valued functions, we introduce auxiliary functions such as,

$$g_j(\vec{x}) \;:=\; \mathrm{I}_{d_1} \otimes \cdots \otimes \mathrm{I}_{d_{j-1}} \otimes f_j(x_{i_j}) \otimes f_{j+1}(x_{i_{j+1}}) \cdots \otimes f_k(x_{i_k}),$$

that capture the intermediate state of this random process after j steps. This lets us utilize the large gaps, i.e., $|\Delta_j|$ in $\mathcal{S}$, to obtain a sharper bound ($\lambda^{\eta(\mathcal{S})}$ instead of $\lambda^{\lfloor \frac{k}{2} \rfloor}$).

Beyond Spectral Gap via structured graphs

The above technique is quite general and works beyond the setup of groups, thereby yielding a general result (Theorem 2). Moreover, it only uses the fact that X is an expander i.e., that it satisfies a spectral gap. While this leads to operator norm bounds, it is not amenable to analyzing trace norms, and one has to appeal to generic bounds such as $\|\mathsf{M}\|_{\mathrm{tr}} \leq \dim(\mathsf{M}) \cdot \|\mathsf{M}\|_{\mathrm{op}}$ which is suboptimal in many cases. The key insight behind our second main result (Theorem 8) is to use additional spectral information (eigenvectors) about the expander X, and not just its spectral gap. To do so, we define the notion of *pseudo Cayley graphs*.

Pseudo Cayley Graphs

These are graphs such that the characters of the group G are its eigenvectors. More precisely, there exists a labeling of its vertices, $\varphi : X \to G$, such that $\chi \circ \varphi$ is an eigenvector of the graph adjacency matrix A_X for every character χ of G. Note that this property is true for Cayley graphs over Abelian groups. Moreover, one can also build examples over non-Abelian groups (see Example 22).

To make use of the above structure, we use a key fact from representation theory, which says that the product of characters over any finite group G can be decomposed a linear sum,

$$\chi_\alpha(g) \cdot \chi_\beta(g) \;=\; \sum_\gamma c_\gamma^{\alpha,\beta} \cdot \chi_\gamma(g).$$

These coefficients are called Clebsch–Gordan coefficients for G. Therefore, our expression can be inductively unrolled by alternating the operations– (i) taking a step of the walk (which can be handled now that characters are eigenvectors), and (ii) decomposing the product of characters as a linear sum. This leads to a precise calculation of the mean over random walks (see Theorem 24) as opposed to an upper bound for the operator norm.

Lower Bound

This precise calculation comes in handy not just to prove the sharper bound in Theorem 8, but also for the lower bound. The candidate hard function is a generalization of the Boolean threshold function which was used in the analysis of [4]. However, their construction of the graph is specific to $\mathbb{Z}_2$ and does not generalize to other groups (even $\mathbb{Z}_p$). Moreover, in Abelian groups the representations are 1-dimensional irreps and thus, $|\mathrm{tr}(\mathsf{M})| = \|\mathsf{M}\|_{\mathrm{op}} = \|\mathsf{M}\|_{\mathrm{tr}}$. However, in higher dimensions even if $\|\mathsf{M}\|_{\mathrm{op}} \geq \lambda$, the trace, $\mathrm{tr}(\mathsf{M})$ can be zero which is actually the quantity which we need to lower bound. To tackle this, we compute this trace exactly at level 2 (Corollary 45) and combine it with the precise computation of the mean for pseudo Cayley graphs (see Theorem 24).

2 Preliminaries

2.1 Random walks on expander graphs

Throughout the paper, $X = (V, E)$ will be a d-regular λ-expander graph. We write A_X to denote the degree normalized adjacency operator of X.

▶ **Definition 10** ((d,λ)-expander). *A graph d-regular graph $X = (V, E)$ is called (d, λ)-expander if $\max\{|\lambda_2|, |\lambda_N|\} \leq \lambda$ where $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_N$ are the eigenvalues of A_X.*

We write $x \sim y$ denote sampling of an edge, (x, y) from X. A key tool in analyzing expanders is the expander mixing lemma:

▶ **Lemma 11** (Expander mixing lemma). *Let X be a λ-spectral expander and $f,\ g : X \to \mathbb{C}^n$ be two vector-valued functions on the vertex set X. Let, $\mu_f = \mathbb{E}_{x\sim X}[f(x)]$ and $\|f\|_2^2 = \mathbb{E}[|f(x)|^2]$. Then we have:*

$$\left|\, \mathbb{E}_{x\sim y}[\langle f(x), g(y)\rangle] - \langle \mu_f, \mu_g\rangle \,\right| \ \leq\ \lambda \cdot \|f\|_2 \|g\|_2.$$

Random walk notation

We find it helpful to define a few shortands associated with random walks on $X = (V, E)$ to streamline our presentation. We list them below.

- We write $''\vec{x} \sim \mathrm{RW}_n''$ to denote uniform sampling of an $(n-1)$-step (or, n vertices long) random walk, $(x_1, x_2, \ldots, x_n) =: \vec{x}$ on X.
- Given, $x \in V$, the notation $''\vec{x} \sim \mathrm{RW}_n(x)''$ denotes uniform sampling of an $(n-1)$-step (or, n vertices long) random walk, $\vec{x}$ conditioned on $x_1 = x$.
- The expression "$x \sim^k y$" denotes sampling a pair, (x, y), of vertices from X that are at a distance of k.

▶ **Fact 12** (Distribution for a single). *Fix any $k \in [n]$. Then, the marginal distribution on x_k when $\vec{x} \sim \mathrm{RW}_n$ is uniform over X.*

2.2 The main quantity

Let G be any finite group and $X = (V, E)$ be an expander graph. A G-labeling (or, simply labeling), φ, of X is a map $\varphi : X \to G$. Given any such labeling φ, we say φ, is *unbiased* if

$$\Pr_{x\sim X}[\varphi(x) = g] = |G|^{-1} \text{ for all } g \in G$$

In this work, our focus is functions of the form $f : G^n \to \mathbb{C}$. We will always assume that the labelling is unbiased and use $f(x)$ to denote $f \circ \varphi$ to prevent clutter.

2.3 Inner products and norms

Let $\mathbb{C}^d$ be the d-dimensional complex inner product space equipped with the inner product. We denote by U_d the group of d-dimensional unitary matrices. Let $A, B \in \mathbb{C}^{d\times d}$ be two complex matrices. We have the following inner products and norms:

- $\langle u, v\rangle := \mathbb{E}_{i\sim[d]}[u_i v_i^*]$
- $\langle A, B\rangle_{\mathrm{HS}} := \mathrm{tr}(A^*B) = \mathrm{tr}(B^*A)$
- $\|A\|_{\mathrm{HS}}^2 = \mathrm{tr}(A^*A) = \sum_{i,j} |A_{i,j}|^2$
- $\|A\|_{\mathrm{tr}} = \mathrm{tr}(\sqrt{A^*A})$
- $\|A\|_{\mathrm{op}} = \sup_{\|x\|=1} \|Ax\|$ where $\|\cdot\|$ denotes the norm associated with $\mathbb{C}^d$.

2.4 Fourier Analysis on Finite Groups

We always use G to denote an arbitrary finite group (not necessarily abelian) unless specified otherwise. Denote by $L^2(G) = \{f : G \to \mathbb{C}\}$, the space of complex-valued functions equipped with the following inner product,

$$\langle f, g\rangle = \mathop{\mathbb{E}}_{x\sim G}\big[\big(g(x)^* f(x)\big)\big].$$

This induces the norm is $\|f\|^2 = \mathbb{E}_{x\sim G}\big[|f(x)|^2\big]$.

Group Representations

We will use the notion of a group representation[3]. *Weyl's unitary trick*, says that for a large family of groups (which includes all finite groups), every representation can be made unitary and thus, we can restrict to studying these.

▶ **Definition 13** (Irreducible Group Representation). *Let G be a finite group. A unitary representation of G is a group homomorphism $\rho : G \to \mathrm{U}_d$ for some d, i.e., $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ for every $g_1, g_2 \in G$. The character, $\chi_\rho : G \to \mathbb{C}$ associated with ρ is the function: $\chi_\rho = \mathrm{tr} \circ \rho$. Note, that characters are not necessarily homomorphisms. A representation is called irreducible (or irrep) if there exists no subspace of $V \subseteq \mathbb{C}^d$ such that $\rho(g)V \subseteq V$ for all $g \in G$. The set of irreps of G is denoted as $\widehat{G}$.*

When G is abelian, all irreducible representations are one-dimensional. Thus, in this case, the set of characters, and the set of irreps coincide. Moreover, for abelian G, the set of characters form an orthogonal basis of $\mathbb{C}[G]$. This does not hold for arbitrary finite groups G. Nevertheless, even for arbitary finite groups, the set characters do satisfy the orthogonality conditions.

▶ **Fact 14.** *Let, $\rho, \gamma \in \widehat{G}$ be two irreducible representations. Then,*

$$\langle \chi_\rho, \chi_\gamma \rangle = \begin{cases} d_\rho, & \text{if } \rho = \gamma, \\ 0, & \text{otherwise.} \end{cases}$$

Moreover, for any non-trivial representation ρ of any finite group G, $\mathbb{E}_{g \in G} \rho(g) = 0$.

2.5 Complex valued functions on groups

For every finite group G, the set of functions given by the matrix entries of the irreps, i.e., $\{\rho_{ij} \mid \rho \in \widehat{G}, i, j \in [d_\rho]\}$, form an orthogonal basis for the space of all functions, $L^2(G)$.

▶ **Definition 15** (Fourier Coefficient). *For any irrep ρ, we have $\widehat{f}(\rho) := \mathbb{E}_x\big[f(x) \cdot \rho(x)\big]$. The Fourier coefficient of the trivial irrep as $\mu(f) := \widehat{f}(\rho_{\mathrm{triv}})$.*

▶ **Fact 16.** *The following identities hold for the Fourier transform,*

1. **(Fourier inversion)** $f(x) = \sum_{\rho \in \widehat{G}} d_\rho \big\langle \widehat{f}(\rho), \rho(x) \big\rangle$.
2. **(Plancharel's identity)** $\|f\|^2 = \sum_{\rho \in \widehat{G}} d_\rho \|\widehat{f}(\rho)\|_{\mathrm{HS}}^2$.

Product Groups

In this paper, we will work with product groups. The following fact characterizes the irreducible representations of G^n in terms of irreps of G.

▶ **Fact 17.** *$\widehat{G^n} = \{\rho_1 \otimes \cdots \otimes \rho_n \mid \rho_i \in \widehat{G}\}$. We use $\vec{\rho}_T$ to represent $\rho_1 \otimes \cdots \otimes \rho_n$ such that $T = \{i \mid \rho_i \neq \mathrm{triv}\}$. Moreover, $|\vec{\rho}| := |T|$.*

▶ **Definition 18** (Degree Decomposition). *For $f : G^n \to \mathbb{C}$, we use f_k to denote the function corresponding to its k^{th}-level, i.e., $f_k(\vec{x}) = \sum_{\vec{\rho}, |\vec{\rho}| = k} d_{\vec{\rho}} \Big\langle \hat{f}(\vec{\rho}), \vec{\rho}(\vec{x}) \Big\rangle$. In the Boolean case ($\mathbb{Z}_2^n$), this is also referred to as the degree k component of f.*

[3] Additional background on representation theory of finite groups can be found in [22].

3 Expander Walks and Product functions

In this section, we will prove the main claim about the fooling of tensored product matrix-valued functions. This can be seen as the matrix-valued generalization of [4]. We will then apply it to our Fourier basis elements, i.e., irreps which are tensor product functions, to obtain our main result for general functions. To state our theorem, we will need a few pieces of notations borrowed from [4] that we describe below.

Notation

Let $\mathcal{S} = \{i_1 < i_2 < \cdots < i_{k-1} < i_k\}$ be an ordered subset of $\{1, 2, \ldots, n\}$. We define the following key quantities:

- $\mathcal{I}_k = \big\{\{1, k-1\} \subseteq I \subseteq [k-1] \mid \forall\, 1 < j < k-1,\ \{j, j+1\} \cap I \neq \emptyset\big\}$.
- $\Delta_j(\mathcal{S}) = i_{j+1} - i_j$.

In this section, we can state our main theorem that we prove in this section.

▶ **Theorem 19.** *Let, X be an λ-expander graph and let $\mathcal{S} = \{i_1 < i_2 < \cdots < i_{k-1} < i_k\}$ be an ordered subset of $[n]$. Let $\{f_j : X \to \mathsf{M}_{d_j}(\mathbb{C}) \mid j \in [k]\ \}$ be set of matrix valued functions such that $\mathbb{E}_{x\sim X}[f_j(x)] = 0$, and $\max_x \|f_j(x)\|_{\mathrm{op}} \leq 1$. Then,*

$$\left\|\mathbb{E}_{\vec{x}\in \mathrm{RW}_n}[f_1(x_{i_1}) \otimes \cdots \otimes f_k(x_{i_k})]\right\|_{\mathrm{op}} \leq \sum_{I\in\mathcal{I}(k)} \lambda^{\sum_{i\in I}\Delta_i(\mathcal{S})}.$$

Proof. See the full version of the paper for this proof. ◀

▶ **Corollary 20** (Operator version of [4])**.** *Let X be a λ expander and $\varphi : V(X) \to G$ be an unbiased labeling. Let $\mathcal{S} = \{i_i, \cdots, i_k\} \subseteq [n]$. Then for any set of non-trivial irreps $\{\rho_1, \ldots, \rho_k\}$ of G,*

$$\left\|\mathbb{E}_{\vec{x}\in \mathrm{RW}_n}[\rho_1(\varphi(x_{i_1})) \cdots \otimes \rho_k(\varphi(x_{i_k}))]\right\|_{\mathrm{op}} \leq \sum_{I\in\mathcal{I}_k} \lambda^{\sum_{j\in I}\Delta_j(\mathcal{S})}.$$

Proof. We only need to check that a non-trivial irrep satisfies the conditions of Theorem 19. The max operator norm is 1 as representations map to unitary matrices. The mean zero condition holds from the fact we work with unbiased labelings and from Fact 14. ◀

3.1 Walks on "structured" Cayley graphs

In this section, we will specialize our results and work with a class of Cayley-like graphs. These graphs generalize a very useful property of Cayley graphs over Abelian groups, namely that, its eigenvectors are characters. This knowledge of the graph eigenvectors will enable us to sharpen our computation of the random walk expectation.

▶ **Definition 21** (Pseudo Cayley graph)**.** *A graph X is pseudo-Cayley with respect to G if there is an unbiased labeling $\varphi : X \to G$ such that for every Fourier basis element ρ_{ij}, the function, $\rho_{ij} \circ \varphi$, is an eigenvector of A_X with eigenvalue λ_ρ.*

When working with such graphs, we will implicitly use such a labeling and thus write $\chi(v)$ as a shorthand for $\chi \circ \varphi(v)$.

▶ **Example 22.** Let H, G be groups such that there exists a surjective homomorphism $\varphi : H \to G$. Then, the complete graph on H (without self-loops), i.e., $X = \mathrm{Cay}(H, H \setminus \{1\})$ is pseudo Cayley with respect to G, with φ as the labeling. In particular, one may take $H = G^r$ for any $r \geq 1$. Moreover, it inherits the eigenvalues of X.

3.1.1 Decay for walks on Pseudo Cayley graphs

We now prove a finer bound for the decay obtained by performing walks on such an X. The labeling function is just the identity map on G. which is an unbiased labeling. This improves Theorem 2 by providing an explicit description of the mean $\mathcal{E}_X(\vec{\rho})$ and not just a norm bound on it. This will be used to give better bounds for conjugacy-invariant function i.e., *class functions* in Section 5.1. We start with a key fact from representation theory.

▶ **Fact 23** (Decomposition of tensor representations). *Let, $\alpha, \beta \in \widehat{G}$ be two irreps of a finite group G. There exists a change of basis transformation $\mathsf{N}_{\alpha,\beta}$, and non-negative integer coefficients $\{c_\gamma^{\alpha,\beta} \mid \gamma \in \widehat{G}\}$ such that for any $g \in G$:*

$$\begin{aligned} \mathsf{N}_{\alpha,\beta}\big(\alpha(g) \otimes \beta(g)\big)\mathsf{N}_{\alpha,\beta}^* &= \oplus_{\gamma\in\widehat{G}} \gamma^{\oplus c_\gamma^{\alpha,\beta}}, \\ \chi_\alpha(g) \cdot \chi_\beta(g) &= \sum_\gamma c_\gamma^{\alpha,\beta} \cdot \chi_\gamma(g), \\ c_{\mathrm{triv}}^{\alpha,\beta} &= \mathbb{1}_{\{\alpha=\beta^*\}}. \end{aligned}$$

These coefficients are called Clebsch-Gordan coefficients for G.

The proof is an inductive unfolding of the expression by applying Fact 23 and then using that the characters are eigenvectors.

▶ **Theorem 24** (Precise Computation of Expectation). *Let X be a pseudo-Cayley graph with respect to G, with eigenvalues $\{\lambda_\alpha \mid \alpha \in \widehat{G}\}$. Let $\mathcal{S} = \{i_1, \ldots, i_k\}$ be any ordered subset of $[n]$, and $\{\rho_1, \ldots, \rho_k\}$ be non-trivial irreps of G and $\{\chi_i\}$ their associated characters. Then for any $k \geq 2$,*

$$\mathop{\mathbb{E}}_{\vec{x}\sim \mathrm{RW}_n}[\chi_1(x_{i_1}) \cdots \chi_k(x_{i_k}))] = \sum_{\gamma_1,\ldots,\gamma_{k-2}\in\widehat{G}} \prod_{i=1}^{k-1} \Big(c_{\gamma_{i-1}}^{\rho_i,\gamma_i} \lambda_{\gamma_i}^{\Delta_i(\mathcal{S})} \Big).$$

where $\gamma_0 = \mathrm{triv}, \gamma_{k-1} = \rho_k$ are fixed in the summation.

Proof. See the full version of the paper for this proof. ◀

We now derive two consequences from the above theorem that we will use later. We start with a simple one that we have already computed as the base case in our above proof. We write out separately as it we will utilize this case later. Moreover, it is conceptually important because it captures the operation of projecting to the space of G-invariants.

▶ **Corollary 25.** *Let X be any pseudo Cayley graph. and let $\vec{\rho}$ be such that $|\vec{\rho}| = 2$ where $\rho_i = \alpha$ and $\rho_j = \beta$ for $\alpha, \beta \in \widehat{G}$ and $1 \leq i < j \leq n$. Then,*

$$\begin{aligned} \mathcal{E}_X(\vec{\rho}) &= 0 \qquad \text{if } \alpha \neq \beta^*, \\ \mathcal{E}_X(\vec{\rho}) &= \lambda_\alpha(X)^{j-i} \cdot \mathop{\mathbb{E}}_{g\sim G}[\alpha \otimes \alpha^*(g)] =: \lambda_\alpha^{j-i} \cdot \mathsf{M}_\alpha. \end{aligned}$$

Here, M_α is a $d_\alpha^2 \times d_\alpha^2$ matrix with $\mathrm{tr}(\mathsf{M}_\alpha) = 1$.

Proof. This is the same computation as in the proof for the base case of $k = 2$ but now utilizing the matrix decomposition of $\alpha \otimes \beta$ from Fact 23. ◀

Notice in the statement of Theorem 24 that if we have terms with many of the γ_i being trivial, then this expectation can be large, as $\lambda_{\text{triv}} = 1$. To see this, assume the extreme case when every $\lambda_\gamma = 1$. Then, the term is just an inductive way to count the multiplicity of the trivial rep in the tensor-rep, $\rho_1 \otimes \cdots \rho_n$. To give a better bound, we make the following important observation that as no two consecutive γ_j, γ_{j+1} can be trivial. We recall the definition of $\mathcal{I}_k$,

$$\mathcal{I}_k \;=\; \left\{\{1, k-1\} \subseteq I \subseteq [k-1] \mid \; \forall\, 1 < j < k-2,\; \{j, j+1\} \cap I \neq \emptyset\right\}$$

▶ **Observation 26.** *Let ρ be any non-trivial irrep of G. Then, $c_{\text{triv}}^{\rho,\text{triv}} = 0$. Let $\{\gamma_0, \gamma_1, \cdots, \gamma_{k-1}\}$ be a sequence of irreps such that $\gamma_0 = \text{triv}$ and $\gamma_{k-1} \neq \text{triv}$. Define, $T_\gamma := \{i \mid \gamma_i \neq \text{triv}\}$. Then,*

$$\prod_{i=1}^{k-1} c_{\gamma_{i-1}}^{\rho_i,\gamma_i} = 0 \quad \text{if } T_\gamma \notin \mathcal{I}_k \quad .$$

Proof. By definition, $c_{\text{triv}}^{\rho,\text{triv}}$ is the multiplicty of the trivial representation in $\rho \otimes \text{triv}$ which is zero as ρ is a non-trivial irrep. Now, if $T_\gamma \notin \mathcal{I}_k$, either $1 \notin T_\gamma$ or there exists j such that $\{j-1, j\} \notin T_\gamma$. This is because $k-1 \in T_\gamma$ by definition. In the first case, $\gamma_0 = \gamma_1 = \text{triv}$. In the second, we have $\gamma_j, \gamma_{j-1} = \text{triv}$. So we have that either the first term or the j^{th}-term in the product is zero. ◀

This shows that the term in Theorem 24 only sums over a subset of all possible sequences of irreps. To formalize this we make the following definition

▶ **Corollary 27.** *Let $\{\rho_1, \ldots, \rho_k\}$ be a set of k non-trivial irreps of G, and $\{\chi_1, \ldots \chi_k\}$ be the corresponding characters. Let X be any pseudo Cayley graph on G. Then for any subset $\mathcal{S}$ of size k,*

$$|\mathcal{E}_{X,\mathcal{S}}(\chi_{\vec{\rho}})| \quad \leq \quad \langle \chi_{\text{triv}},\, \chi_1 \cdots \chi_k \rangle \cdot \max_{T \in \mathcal{I}_k} \lambda^{\sum_{i \in T} \Delta_i(\mathcal{S})} \quad .$$

Proof. See the full version of the paper for this proof. ◀

4 Fooling Symmetric Functions and Word Functions

The main goal is to study the pseudorandomness of expander walks via families of test functions. For a function, $f : G^n \to \mathbb{C}^{k \times k}$, we wish to analyze

$$\mathcal{E}_X(f) = \mathop{\mathbb{E}}_{\vec{x} \sim \text{RW}_n}[f(x_1, \ldots, x_n)] - \mathop{\mathbb{E}}_{\vec{x} \sim \text{Unif}_n}[f(x_1, \ldots, x_n)] \,.$$

We have already analyzed this for tensor functions (Theorem 2). Using Fourier transform, we will first see how studying the fooling of arbitrary functions reduces the problem to measuring the fooling of tensor product of irreducible representations.

4.1 A general reduction to fooling irreps

▷ Claim 28. Let, $f : G^n \to \mathbb{C}$ be any function, and denote its degree-i component as f_i. Then,

$$\mathcal{E}_X(f) \;=\; \sum_{i \geq 2} \mathcal{E}_X(f_i), \;\text{ and}$$

$$\left|\,\mathcal{E}_X(f_i)\right| \;\leq\; \sum_{\vec{\rho}, |\vec{\rho}| = i} d_{\vec{\rho}} \left\|f(\hat{\rho})\right\|_{\text{tr}} \cdot \left\|\mathcal{E}_X(\vec{\rho})\right\|_{\text{op}}, \; \forall i \in [n].$$

Proof. See the full version of the paper for this proof. ◁

4.2 Fooling symmetric functions

Let $f : G^n \to \mathbb{C}$ be a function that is invariant under any permutation of the input tuple. Such a function only depends on the counts of each group element in the tuple and, therefore, can be viewed as a symmetric function on $\mathbb{Z}_{|G|+1}^n$. Appealing to the results of Golowich–Vadhan [10], one gets a decay of $O(|G|^{O(|G|)}\lambda)$. We obtain an exponentially better bound of $O(|G|\lambda)$ by utilizing a Fourier basis for G.

Preparatory lemmas

In the Boolean case, the Fourier coefficient of a symmetric function f, is unchanged under permutation of the non-trivial coordinates, i.e., $\hat{f}(\chi_T) = \hat{f}(\chi_{T'})$ for any subsets T, T' of size k. Unsurprisingly, this extends to the case of general groups.

▶ **Observation 29** (Fourier Coefficient under permutation). *Let $\rho_1, \cdots \rho_k$ be any k non-trivial irreps and let $T = \{t_1, \cdots, t_k\}$ be some ordered subset of $[n]$. Denote by $\vec{\rho}_T$ the irrep with $(\vec{\rho}_T)_{t_j} = \rho_j$ and trivial otherwise. Let σ be the permutation that maps $T \to T'$ for any other T of size k. Then for any symmetric function f,*

$$\hat{f}(\vec{\rho}_T) \;=\; \hat{f}(\vec{\rho}_{T'}).$$

In particular, all norms are preserved.

We now obtain a trivial upper bound on the trace-norm of the Fourier transform, in terms of the L^2 norm. This is a fairly standard application of Cauchy-Schwarz.

▶ **Lemma 30** (Trace norm to L_2-norm). *For any symmetric function $f : G^n \to \mathbb{C}$,*

$$\sum_{\vec{\rho}=\rho_1\otimes\cdots\rho_k\otimes I\cdots\otimes I, \rho_i\neq \mathrm{triv}} d_{\vec{\rho}} \left\| \hat{f}(\vec{\rho}) \right\|_{\mathrm{tr}} \;\leq\; \frac{|G|^{\frac{k}{2}}}{\sqrt{\binom{n}{k}}} \cdot \|f_k\|_2 \,.$$

Proof. See the full version of the paper for this proof. ◀

We now recall the key combinatorial bound from [4]

▶ **Lemma 31** ([4, Lemma 4.4]). *For any $2 \leq k \leq n$, and $\lambda < 1/2$ we have*

$$\beta(k) = \sum_{|S|=k} \lambda^{\Delta(S)/2} \;\leq\; 2^k \binom{n-1}{\lfloor k/2 \rfloor} \Big(\frac{\lambda}{1-\lambda}\Big)^{k/2} \;\leq\; \binom{n}{k}^{\frac{1}{2}} (16e\lambda)^{k/2}.$$

Proof. The first inequality is from the reference and the second follows by observing that

$$\binom{n-1}{\lfloor k/2 \rfloor}^2 \leq \binom{n}{k}(2e)^k, \;\text{ and for }\; \lambda < 1/2, \; \left(\frac{\lambda}{1-\lambda}\right) \;\leq\; 2\lambda.$$ ◀

▶ **Theorem 32.** *Let f be any symmetric function over G^n where G is any finite group. Let $\tau = 16e\lambda|G|$. Then, for any $k \geq 2$,*

$$|\mathcal{E}_X(f_k)| \;\leq\; \tau^{k/2} \cdot \|f\|_2. \text{ And thus, } |\mathcal{E}_X(f)| \;\leq\; 2\tau \cdot \|f\|_2, \text{ if } \tau < 1.$$

Proof. We will use $\vec{\rho}_S$ to denote the representation given by $\rho_i =$.

$$\begin{aligned}
|\mathcal{E}(f_k)| &\leq \sum_{\vec{\rho}\in \mathrm{Irrep}(G^n), |\vec{\rho}|=k} d_{\vec{\rho}} \|\hat{f}(\vec{\rho})\|_{\mathrm{tr}} \cdot \left\|\mathcal{E}_X(\vec{\rho})\right\|_{\mathrm{op}} && \text{(Using Claim 28)} \\
&\leq \sum_{\vec{\rho}} d_{\vec{\rho}} \|\hat{f}(\vec{\rho})\|_{\mathrm{tr}} \sum_{S\in\binom{n}{k}} \|\mathcal{E}_X(\vec{\rho}_S)\|_{\mathrm{op}} && \text{(Using Observation 29)} \\
&\leq \sum_{\vec{\rho}} d_{\vec{\rho}} \|\hat{f}(\vec{\rho})\|_{\mathrm{tr}} \sum_{S\in\binom{n}{k}} \lambda^{\Delta(S)/2} && \text{(Using Corollary 20)} \\
&\leq \sum_{\vec{\rho}} d_{\vec{\rho}} \|\hat{f}(\vec{\rho})\|_{\mathrm{tr}} \cdot \binom{n}{k}^{\frac{1}{2}} (16e\lambda)^{k/2} && \text{(Using Lemma 31)} \\
&\leq (16e\lambda)^{k/2} \cdot |G|^{k/2} \cdot \|f\|_2 && \text{(Using Lemma 30)} \\
&= (\tau)^{k/2} \|f\|_2.
\end{aligned}$$

To get the last inequality, we use Claim 28 and obtain that:

$$|\mathcal{E}_X(f)| \leq \sum_{i\geq 2} |\mathcal{E}_X(f_i)| \leq \left(\sum_{k\geq 2} \tau^{k/2}\right) \|f\|_2 \leq 2\tau \|f\|_2 \quad \text{if } \tau < 1. \qquad \blacktriangleleft$$

4.3 Word functions

A *word map* of a finite group G is an element of the free group on G. Given any $h : G \to \mathbb{C}$ and a word map $w : G^n \to G$, one can consider the composed map $h(w(\cdot)) : G^n \to \mathbb{C}$, which is commonly referred to as a *word function*. Word functions are ubiquitous in mathematics and computer science literature.

The main result of this section is to give a complete characterization of the Fourier spectrum of a certain subclass of word functions that will be termed *monomial word functions*. In particular, first we will show that these have Fourier support on the highest level and thus are analogs of the PARITY function over $\mathbb{Z}_2^n$. Moreover, this support is also sparse. Combining this with Corollary 20, we deduce that such functions are exponentially fooled by expander walks.

▶ **Definition 33** (Monomials and Word function). *For an ordered subset $\mathcal{S} \subseteq [n]$, a word map of* degree $k = |S|$ *is a G-valued function $w_{\mathcal{S}} : G^n \to G$, defined as $w_{\mathcal{S}} = \prod_{s\in S} g_s^{e_s}$ where $e_S \in \mathbb{Z}$. A word is monomial if the variables are non-repeating and the exponent is ± 1. A function $f : G^n \to \mathbb{C}$ is a monomial word function of degree k, if $f = h(w(g_1, \cdots, g_n))$ for a monomial word w of degree k and a function $h : G \to \mathbb{C}$.*

In the second half of this section, we consider a subclass of functions within monomial word functions that we call *monotone word functions*. Essentially, these are word functions for which corrresponding word, w is monotone i.e., $w = x_{i_1} \cdots x_{i_k}$ for $i_1 \leq \cdots i_k$. We already mentioned that for monomial word functions gets fooled by expander walks upto an exponentially decaying error. However, the error bound has dependence on $|G|$. For monotone word functions we remove this dependence while achieving the same decay in terms of expansion.

4.3.1 Fourier Spectrum of Word functions

We begin by proving a structural claim about the fourier coefficients of word functions. The claim that we prove below essentially says that a word function $f : G^n \to \mathbb{C}$ that only utilizes a subset $\mathcal{S} \subseteq [n]$ of the input co-ordinates is only supported on representations $\vec{\rho}$ such that $\rho_i = \text{triv}$ for $i \notin \mathcal{S}$ and $\rho_i \in \{\rho, \rho^*\}$ otherwise. Note that, the fourier structure of these word functions on more general groups closely resemble the special case of parities.

▶ **Lemma 34** (Fourier Mass Support). *Let $f : G^n \to \mathbb{C}$ be a word function of degree k corresponding to a set $\mathcal{S}$. Let $\mathcal{S}^+$ (resp. $\mathcal{S}^-$) be the subset of elements such that $e_s = 1$ (resp., -1). Then, $\hat{f}(\vec{\rho}) \neq 0$ only if*

1. *For every $i \notin \mathcal{S}$, $\rho_i = \text{triv}$.*
2. *For every $i \in \mathcal{S}^+$ $\rho_i = \rho$ for some $\rho \in \text{Irrep}(G)$.*
3. *For every $i \in \mathcal{S}^-$ $\rho_i = \rho^*$ for the same ρ as above.*

Proof. See the full version of the paper for this proof. ◀

4.3.2 Fooling Word Functions

Before we state our first theorem in this section we recall two notations from Section 3. Let $\mathcal{S} = \{i_1 < i_2 < \cdots < i_{k-1} < i_k\}$ be an ordered subset of $\{1, 2, \ldots, n\}$. We define the following key quantities:

- $\mathcal{I}_k = \big\{\{1, k-1\} \subseteq I \subseteq [k-1] \mid \forall\, 1 < j < k-1,\ \{j, j+1\} \cap I \neq \emptyset\big\}$.
- $\Delta_j(\mathcal{S}) = i_{j+1} - i_j$.

We have the following theorem on monomial word functions.

▶ **Theorem 35** (Fooling for degree k word functions). *Let $f : G^n \to \mathbb{C}$ be a monomial word function of degree k corresponding to a set $\mathcal{S}$. Then for any expander X with an unbiased G-labelling,*

$$|\mathcal{E}_X(f)| \;\leq\; \sum_{I \in \mathcal{I}_k} \lambda^{\sum_{j \in I} \Delta_j(\mathcal{S})} \cdot |G|^{k/2} \cdot \|f\|_2 \,.$$

In particular, we have $|\mathcal{E}_X(f)| \;\leq\; \lambda^{-1}(\lambda|G|)^{k/2} \cdot \|f\|_2$

Proof. Let ρ^S denote the representation $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ where $\rho_i = \rho$ if $i \in S_I^+$, $\rho_i = \rho^*$ if $i \in S_I^-$, and is trivial otherwise, i.e., $\rho_i = 1$. From Lemma 34, we know that the only non-zero Fourier coefficients are for such ρ^S. Thus we will consider these irreps for expander walk fooling.

$$\begin{aligned}
\mathcal{E}(f) \;&\leq \sum_{\psi \in \text{Irrep}(G^n)} d_\psi \|\hat{f}(\psi)\|_{\text{tr}} \cdot \Big\| \mathop{\mathbb{E}}_{\vec{g} \sim X^n} [\psi(\vec{g})] \Big\|_{\text{op}} && \text{(Using Claim 28)} \\
&\leq \sum_{\rho \in \text{Irrep}(G)} d_{\rho^S} \|\hat{f}(\rho^S)\|_{\text{tr}} \cdot \Big\| \mathop{\mathbb{E}}_{\vec{g}} \big[\rho^S(\vec{g})\big] \Big\|_{\text{op}} && \text{(Using Lemma 34)} \\
&\leq \sum_{I \in \mathcal{I}_k} \lambda^{\sum_{j \in I} \Delta_j(\mathcal{S})} \sum_{\rho \in \text{Irrep}(G)} d_\rho^k \|\hat{f}(\rho^S)\|_{\text{tr}} && \text{(Using Corollary 20)} \\
&\leq \sum_{I \in \mathcal{I}_k} \lambda^{\sum_{j \in I} \Delta_j(\mathcal{S})} \cdot |G|^{k/2} \cdot \|f\|_2.
\end{aligned}$$

The last line follows from Cauchy-Schwarz and Hölder's inequality. ◀

We now give an alternate proof of the above result in the special case that the word is monotone i.e., $w = x_{i_1} \cdots x_{i_k}$ for $i_1 < \cdots < i_k$. The change is that we now the Fourier decomposition of $h : G \to \mathbb{C}$ i.e., over G rather than of f directly. To analyze this, we will need the result from [15].

▶ **Theorem 36** ([15]). *Let X be any λ-expander with an unbiased labelling of G. Then for any non-trivial irrep ρ of G,*

$$\|\mathcal{E}_X(\rho(x_1 \cdots x_k))\|_{\mathrm{op}} \;\leq\; \lambda^{k/2}.$$

The result in [15] works for any product function and thus if x_i contains an inverse then, we can pick $f_i = \rho^*$ instead of ρ as $\rho^*(x_i) = \rho({x_i}^{-1})$

▶ **Theorem 37.** *Let $f(\vec{x}) = h(x_1 \cdots x_k)$ be a monotone word function for some $h : G \to \mathbb{C}$. Then for any expander X with an unbiased G-labelling,*

$$|\mathcal{E}_X(f)| \;\leq\; \left(\sqrt{|G|} \cdot \|f\|_2\right) \cdot (2\lambda)^{k/2}.$$

In particular, for $f(\vec{x}) = \mathbb{1}_{\{x_1 \cdots x_k = t\}}$ for any $t \in G$, one has $|\mathcal{E}_X(f)| \;\leq\; (2\lambda)^{k/2}$.

Proof. We assume that the word does not contain inverses and is $x_1 \cdots x_k$ which is true up to renumbering the coordinates. By the Fourier transform on G,

$$h(t) = \sum_{\rho \in \mathrm{Irrep}(G)} d_\rho \langle \widehat{h}(\rho),\, \rho(t) \rangle.$$

Now we feed in $t = x_1 \cdots x_n$ into the function h.

$$\begin{aligned} f(\vec{x}) = h(x_1 \cdots x_k) \;&=\; \sum_{\rho \in \mathrm{Irrep}(G)} d_\rho \langle \widehat{h}(\rho),\, \rho(x_1 \cdots x_k) \rangle \\ \mathcal{E}_X(f) \;&=\; \sum_{\rho \in \mathrm{Irrep}(G)} d_\rho \langle \widehat{h}(\rho),\, \mathcal{E}_X(\rho(x_1 \cdots x_k)) \rangle \\ |\mathcal{E}_X(f)| \;&\leq\; \sum_{\rho \in \mathrm{Irrep}(G), \rho \neq \mathrm{triv}} d_\rho \|\widehat{h}(\rho)\|_{\mathrm{tr}} \, \|\mathcal{E}_X(\rho(x_1 \cdots x_k))\|_{\mathrm{op}} \\ &\leq\; \lambda^{k/2} \cdot \sqrt{|G|} \cdot \|h\|_2 = \lambda^{k/2} \cdot \sqrt{|G|} \cdot \|f\|_2. \end{aligned}$$

The last equality is a simple calculation that uses that for any fixed $x_1, \ldots, x_i$ the word $x_1 \cdots x_i \cdot g$ is uniform over G if g is sampled uniformly from G.

$$\|f\|_2^2 = \mathop{\mathbb{E}}_{x_1, \cdots, x_k} \left[|h(x_1 \cdots x_k)|^2\right] = \mathop{\mathbb{E}}_{x_1, \cdots, x_{k-1}} \left[\mathop{\mathbb{E}}_{x_k} \left[|h(x_1 \cdots x_k)|^2\right] \right] = \mathop{\mathbb{E}}_{x_1, \cdots, x_{k-1}} \left[\|h\|_2^2\right].$$

When $h = \mathbb{1}_{x=t}$, then $\|h\|_2 = |G|^{-1/2}$ and the second claim follows. ◀

5 Function Classes with Group Symmetry

A general group G has a much richer symmetry structure than $\mathbb{Z}_2$, and this opens up the possibility of studying functions, $f : G^n \to \mathbb{C}$, that respect this additional symmetry (beyond permutation of coordinates).

5.1 Symmetric Class Functions

A function over G^n is a *class function* if it is invariant under conjugation, i.e., for any $\vec{x}, \vec{g} \in G^n$, $f(g_1 x_1 {g_1}^{-1}, \ldots, g_n x_n {g_n}^{-1})$. In other words, the function value depends only on the input's conjugacy class. In this subsection, we will give a better bound for symmetric class functions than the one for general symmetric functions. The improvement for class functions will come from a precise calculation of our $\mathcal{E}_X(f)$ expression, without resorting to a Cauchy-Schwarz–type bound to go from L_1-norm to L_2-norm (Lemma 30). To do this, we need to use the group structure.

Representation theory facts

We now state some basic facts about the representation theory of groups that we will need only in this subsection. These are well-known facts and proofs can be found in any introductory text.

▶ **Fact 38** (Class Function Fourier Coefficients). *For any class function $f : H \to \mathbb{C}$,*

$$\widehat{f}(\vec{\rho}) = c_{\vec{\rho}} I_{d_{\vec{\rho}}}, \qquad \|f\|_2^2 = \sum_{\vec{\rho}} d_\rho \|\widehat{f}(\vec{\rho})\|_{\mathrm{HS}}^2 = \sum_{\vec{\rho}} d_\rho^2 {c_{\vec{\rho}}}^2.$$

▶ **Fact 39** (Schur Orthogonality Relation). *For any $g, h \in G$, we denote $g \sim h$ if they belong to the same conjugacy class, say C_g. Then, we have,*

$$\sum_{\rho \in \mathrm{Irrep} G} \chi_\rho(g)\overline{\chi_\rho}(h) \;=\; \frac{|G|}{|C_g|} \cdot \mathbb{1}_{\{g \sim h\}}.$$

▶ **Fact 40.** *Let G be a D-quasirandom, i.e., the smallest non-trivial irrep has dimension D. Let $\mathcal{C}(G)$ denote the conjugacy classes of G. Then,*

$$|\mathcal{C}(G)| \;=\; |\widehat{G}| \;\leq\; \frac{|G|}{D^2} + 1.$$

Proof. The first equality follows from the fact that characters form a basis for class functions (or in other words, the character table is square). The second follows from the following:

$$\sum_{\rho \in \widehat{G}} d_\rho^2 \;=\; |G| \;\geq\; 1 + D^2 \cdot (|\mathcal{C}(G)| - 1). \qquad \blacktriangleleft$$

We are now ready to assemble the above facts to bound $\mathbb{E}_{g \sim G}[\chi_{\rho_1 \otimes \cdots \otimes \rho_k}]$ which counts the multiplicity of trivial rep in $\rho_1 \otimes \cdots \otimes \rho_k$. This claim allows us to improve upon Lemma 30 which would be analogous to a bound of $|G|^k$ in the below term.

▶ **Corollary 41.** *For any finite group G denote by $\mathcal{C}(G)$ the conjugacy classes of G. For any $k \geq 1$,*

$$\eta_{k,G}^2 \;:=\; \sum_{\rho_1, \cdots, \rho_k \in \mathrm{Irrep} \setminus \mathrm{triv}} \Big(\mathop{\mathbb{E}}_g[\chi_{\rho_1 \otimes \cdots \otimes \rho_k}]\Big)^2 \;\leq\; \sum_{C \in \mathcal{C}(G)} \frac{|G|^{k-2}}{|C|^{k-2}} + 1.$$

In particular, if G is D-quasirandom, then $\eta_{k,G}^2 \leq 4 \cdot \frac{|G|^{k-1}}{D^2}$.

Proof. See the full version of the paper for this proof. $\blacktriangleleft$

▶ **Proposition 42.** *Let G be a D-quasirandom group and $f : G^n :\to \mathbb{C}$ be a class function that is also symmetric. Let X be a pseudo Cayley graph with expansion λ. Then,*

$$|\mathcal{E}_X(f)| \;\le\; O\Big(\frac{|G|^{\frac{1}{2}}}{D}\lambda\Big)\cdot\|f\|_2.$$

In particular, for every symmetric function on an Abelian group, we get a bound of $O(\sqrt{|G|}\cdot\lambda)$.

Proof. We first prove a bound for the degree k component of f.

$$\begin{aligned}
\mathcal{E}_X(f_k) &= \sum_{\vec{\rho}\in\mathrm{Irrep}(G^n)} d_{\vec{\rho}}c_{\vec{\rho}}\cdot\mathcal{E}_X(\chi_{\vec{\rho}}) \\
&= \sum_{\rho_1,\cdots\rho_k\in\mathrm{Irrep}(G)\setminus\mathrm{triv}}\;\sum_{S\subseteq\binom{n}{k}} d_{\vec{\rho}}c_{\vec{\rho}}\cdot\mathcal{E}_X(\chi_{\vec{\rho}}) \\
|\mathcal{E}_X(f_k)| &\le \sum_{\rho_1,\cdots\rho_k\in\mathrm{Irrep}(G)\setminus\mathrm{triv}} d_{\vec{\rho}}\sum_{S\subseteq\binom{n}{k}}|c_{\vec{\rho}}|\cdot|\mathcal{E}_X(\chi_{\vec{\rho}})| \\
&\le \sum_{\rho_1,\cdots\rho_k\in\mathrm{Irrep}(G)\setminus\mathrm{triv}} |d_{\vec{\rho}}c_{\vec{\rho}}|\cdot\Big(\mathop{\mathbb{E}}_g[\chi_{\vec{\rho}}]\Big)\sum_{S\subseteq\binom{n}{k}}\lambda^{\Delta(S)/2} \\
&\le \beta(k)\sum_{\rho_1,\cdots\rho_k\in\mathrm{Irrep}(G)\setminus\mathrm{triv}} |d_{\vec{\rho}}c_{\vec{\rho}}|\cdot\Big(\mathop{\mathbb{E}}_g[\chi_{\vec{\rho}}]\Big) \\
&\le \beta(k)\sqrt{\sum_{\rho_1,\cdots\rho_k}|d_{\vec{\rho}}c_{\vec{\rho}}|^2}\cdot\sqrt{\sum_{\rho_1,\cdots\rho_k}\Big(\mathop{\mathbb{E}}_g[\chi_{\vec{\rho}}]\Big)^2} \\
&\le \beta(k)\cdot\frac{\|f_k\|_2}{\sqrt{\binom{n}{k}}}\cdot\sqrt{\eta_{k,G}^2} \\
&\le \Big(16e\lambda\Big)^{k/2}\cdot\eta_{k,G}\cdot\|f_k\|_2 \\
&\le \Big(16e\lambda\cdot 2|G|\Big)^{k/2}\cdot\frac{1}{D\sqrt{|G|}}\cdot\|f\|_2.
\end{aligned}$$

Therefore,

$$|\mathcal{E}_X(f)| \;\le\; \sum_{k=2}^{n}|\mathcal{E}_X(f_k)| \;\le\; \Big(\frac{64e\lambda|G|}{D\sqrt{|G|}}\Big)\cdot\|f\|_2 = O\Big(\frac{\lambda\sqrt{|G|}}{D}\Big)\cdot\|f\|_2 \quad . \qquad \blacktriangleleft$$

5.2 Diagonal action and G-invariant functions

▶ **Definition 43** (Diagonal action and Projection)**.** *Let $h\in G$ and $f : G^n \to \mathbb{C}$. Define $(h\cdot f)(\vec{x}) := f(hx_1,\ldots,hx_n) = f(h\cdot\vec{x})$. The projection to the space of functions invariant under this action is $P_G f(\vec{x}) := \mathbb{E}_{h\sim G}[(h\cdot f)(\vec{x})]$.*

This generalizes the notion of even and odd functions over $\mathbb{Z}_2^n$ which are the special cases when $P_G(f) = f$ and $P_G f = 0$, respectively. We now make a simple observation that walks over Cayley graphs smooth out the function via this projection.

▶ **Observation 44.** *If X is a Cayley graph, then $\mathcal{E}_X(f) = \mathcal{E}_X(P_G f)$.*

We will now compute the Fourier spectrum of $P_G f$ and utilize this to get a precise calculation of level-2 mass. While this can be generalized to state a more general claim, we just include the version we will need later for the lower bound.

▶ **Corollary 45.** *Let $f : G \times G \to \mathbb{C}$, and X be a quasi-Ableian Cayley expander such that all non-trivial eigenvalues are λ. Then,*

$$\mathcal{E}_X(f) \;=\; \lambda \cdot \big(P_G f(\vec{1}) - \mu(f)\big).$$

Proof. See the full version of the paper for this proof. ◀

6 Lower Bounds for decay of Symmetric functions

6.1 Fourier Coefficient of Threshold Function

Threshold Function

Let, $A \subseteq G$ and $t \in [n]$. We define a boolean function $\mathrm{Th}_{A,t}$ as :

$$\mathrm{Th}_{A,t}(\vec{x}) = 1 \quad \text{if } \; |\{i \mid x_i \in A\}| \geq t; \;\; 0 \;\text{ otherwise.}$$

▷ Claim 46. Let, $\vec{\rho} = \rho_1 \otimes \rho_2 \otimes \ldots \rho_n \in \widehat{G^n}$ such that $\rho_i = \alpha$, $\rho_j = \alpha^*$ for some $\alpha \in \hat{G}$ and $1 \leq i < j \leq n$ and $\rho_k = \mathrm{triv}$ for any $k \notin \{i, j\}$. Then,

$$\widehat{\mathrm{Th}_{A,t}}(\vec{\rho}) = \left(\frac{a_{t-2}^{n-2} - a_{t-1}^{n-2}}{|G|^{n-2}}\right) \cdot \widehat{\mathbb{1}_A}(\alpha) \otimes \widehat{\mathbb{1}_A}(\alpha^*)$$

where $a_t^n := \binom{n}{t}|A|^t|A^c|^{n-t}$.

Proof. See the full version of the paper for this proof. ◁

▶ **Proposition 47.** *If $|A| = \frac{|G|}{2}$ and $t = \frac{n+1-\sqrt{n}}{2}$, then*

$$C_{A,n,t} := \left(\frac{a_{t-1}^{n-2} - a_{t-2}^{n-2}}{|G|^{n-2}}\right) \;\geq\; \Omega\Big(\frac{1}{n-1}\Big).$$

Proof. See the full version of the paper for this proof. ◀

▷ Claim 48 (Lower Bound on fooling level-2 component). Let X be a pseudo Cayley graph such that all non-trivial eigenvalues are equal to $\lambda < 1/2$. Let A be any subset of G. Then for the level-2 component of the threshold function, the following holds:

$$\big|\mathcal{E}_X\big((\mathrm{Th}_{A,t})_2\big)\big| \;\geq\; (n-2) \cdot \lambda \cdot \mathsf{C}_{A,n,t} \cdot \mu_A \cdot \mu_{A^c} \;.$$

Proof. See the full version of the paper for this proof. ◁

▶ **Theorem 49.** *Let G be any finite group, $A \subseteq G$ such that $\frac{|A|}{|G|} = \frac{1}{2}$, and $X = \mathrm{Cay}(G^r, G^r \setminus \{1\})$ be the complete graph on G^r without self-loops for some $r \geq 4$. Then for every n large enough,*

$$\left|\mathcal{E}_X\left(\mathrm{Th}_{A,\frac{n+1-\sqrt{n}}{2}}\right)\right| \;\geq\; \Omega\big(\lambda(X)\big).$$

Proof. Using Claim 28 we can separate the calculation into fooling the level-2 function and those beyond it, and thus for any function we have:

$$\mathcal{E}_X(f) \;=\; \sum_{i=2}^{n} \mathcal{E}_X(f),$$

$$\big|\mathcal{E}_X(f)\big| \;\geq\; \big|\mathcal{E}_X(f_2)\big| - \left|\sum_{k=3}^{n} \mathcal{E}_X(f_k)\right|.$$

We now let f be the threshold function, $f = \mathrm{Th}_{A,\frac{n+1-\sqrt{n}}{2}}$. The graph X has all non-trivial eigenvalues to be equal to $\frac{-1}{|G|^r} < 1/2$. We can then apply Claim 48, which when combined with Proposition 47, we get $\left|\mathcal{E}_X(f_2)\right| \geq \Omega(\lambda)$. To bound the remaining part, we use our upper bound Theorem 32 and obtain that,

$$\left|\sum_{i=3}^{n} \mathcal{E}_X(f_i)\right| \;\leq\; 2(16e|G|\lambda)^{\frac{3}{2}} \cdot \|f\|_2 \;\leq\; o\Big(\lambda^{\frac{3(r-1)}{2r}}\Big) = o(\lambda). \qquad \blacktriangleleft$$

References

1 M. Ajtai, J. Komlos, and E. Szemeredi. Deterministic simulation in LOGSPACE. In *Proceedings of the 19th ACM Symposium on Theory of Computing*, 1987. doi:10.1145/28395.28410.

2 David A. Mix Barrington. Bounded-Width Polynomial-Size Branching Programs Recognize Exactly Those Languages in NC^1. *J. Comput. Syst. Sci.*, 38(1), 1989. doi:10.1016/0022-0000(89)90037-8.

3 Gil Cohen, Dor Minzer, Shir Peleg, Aaron Potechin, and Amnon Ta-Shma. Expander Random Walks: The General Case and Limitations. In *Proceedings of the 49th International Colloquium on Automata, Languages and Programming*, 2022. doi:10.4230/LIPIcs.ICALP.2022.43.

4 Gil Cohen, Noam Peri, and Amnon Ta-Shma. Expander Random Walks: A Fourier-Analytic Approach. In *Proceedings of the 53nd ACM Symposium on Theory of Computing*, 2021. doi:10.1145/3406325.3451049.

5 Anindya De. Pseudorandomness for Permutation and Regular Branching Programs. In *Proceedings of the 26th IEEE Conference on Computational Complexity*, 2011. doi:10.1109/CCC.2011.23.

6 Ankit Garg, Yin Tat Lee, Zhao Song, and Nikhil Srivastava. A matrix expander Chernoff bound. In *Proceedings of the 50th ACM Symposium on Theory of Computing*, 2018. doi:10.1145/3188745.3188890.

7 E.N. Gilbert. A Comparison of Signalling Alphabets. *Bell System Technical Journal*, 31:504–522, 1952. doi:10.1002/j.1538-7305.1952.tb01393.x.

8 D. Gillman. A Chernoff Bound for Random Walks on Expander Graphs. In *focs93*, pages 680–691, 1993. doi:10.1109/SFCS.1993.366819.

9 Louis Golowich. A New Berry-Esseen Theorem for Expander Walks. In *Proceedings of the 55nd ACM Symposium on Theory of Computing*, 2023. doi:10.1145/3564246.3585141.

10 Louis Golowich and Salil Vadhan. Pseudorandomness of Expander Random Walks for Symmetric Functions and Permutation Branching Programs. In *Proceedings of the 37th IEEE Conference on Computational Complexity*, 2022. doi:10.4230/LIPIcs.CCC.2022.27.

11 W. T. Gowers. Quasirandom groups. *Comb. Probab. Comput.*, 2008. doi:10.1017/S0963548307008826.

12 Pooya Hatami and William Hoza. Paradigms for Unconditional Pseudorandom Generators. *Found. Trends Theor. Comput. Sci.*, 16(1-2), 2024. doi:10.1561/0400000109.

13 Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander Graphs and Their Applications. *Bull. Amer. Math. Soc.*, 43(04):439–562, August 2006.

14 Russell Impagliazzo, Noam Nisan, and Avi Wigderson. Pseudorandomness for network algorithms. In *Proceedings of the 26th ACM Symposium on Theory of Computing*, 1994. doi:10.1145/195058.195190.

15 Fernando Granha Jeronimo, Tushant Mittal, Sourya Roy, and Avi Wigderson. Almost Ramanujan Expanders from Arbitrary Expanders via Operator Amplification. In *Proceedings of the 63st IEEE Symposium on Foundations of Computer Science*, 2022. doi:10.1109/FOCS54457.2022.00043.

16 Fernando Granha Jeronimo, Tushant Mittal, Shashank Srivastava, and Madhur Tulsiani. Explicit Codes approaching Generalized Singleton Bound using Expanders. In *Proceedings of the 57th ACM Symposium on Theory of Computing*, 2025. doi:10.48550/arXiv.2502.07308.

17 Alexander Lubotzky. *Discrete Groups, Expanding Graphs and Invariant Measures*, volume 125 of *Progress in mathematics*. Birkhäuser, 1994.

18 Raghu Meka and David Zuckerman. Small-Bias Spaces for Group Products. In *APPROX-RANDOM 2009 Proceedings*, 2009. doi:10.1007/978-3-642-03685-9_49.

19 Silas Richelson and Sourya Roy. Gilbert and Varshamov Meet Johnson: List-Decoding Explicit Nearly-Optimal Binary Codes. In *Proceedings of the 64st IEEE Symposium on Foundations of Computer Science*, 2023. doi:10.1109/FOCS57990.2023.00021.

20 Silas Richelson and Sourya Roy. Analyzing Ta-Shma's Code via the Expander Mixing Lemma. *IEEE Trans. Inf. Theory*, 70(2):1040–1049, 2024. doi:10.1109/TIT.2023.3304614.

21 Ron M. Roth. Higher-Order MDS Codes. *IEEE Transactions on Information Theory*, 68(12):7798–7816, 2022. doi:10.1109/TIT.2022.3194521.

22 Jean-Pierre Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer New York, 1977.

23 Chong Shangguan and Itzhak Tamo. Combinatorial list-decoding of Reed-Solomon codes beyond the Johnson radius. In *Proceedings of the 52nd ACM Symposium on Theory of Computing*, 2020. doi:10.1145/3357713.3384295.

24 Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *stoc17*, pages 238–251. ACM, 2017. doi:10.1145/3055399.3055408.

25 Amnon Ta-Shma and Ron Zadicario. The Expander Hitting Property When the Sets Are Arbitrarily Unbalanced. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2024)*, 2024. doi:10.4230/LIPIcs.APPROX/RANDOM.2024.31.

26 Salil P. Vadhan. *Pseudorandomness*. Now Publishers Inc., 2012. doi:10.1561/0400000010.

27 R.R. Varshamov. Estimate of the number of signals in error correcting codes. *Doklady Akademii Nauk SSSR*, 117:739–741, 1957.