Low Soundness Linearity Testing on the Half-Slice

Haakon Larsen, Tushant Mittal, Silas Richelson, Sourya Roy

WORKING DRAFT
Please do not distribute

Abstract

In this work, we analyze a six-query version of the Blum–Luby–Rubinfeld (BLR) linearity test on the Boolean half-slice, i.e., the set of n-length vectors of Hamming weight $\frac{n}{2}$. We show that if an input function f over the slice passes the test with probability $\frac{1+\delta}{2}$, then it must agree with some affine function at $\frac{1+\sqrt{\delta}}{2}$ fraction of points.

The only other known linearity test for the slice in the low soundness regime (i.e., when δ can be arbitrarily small) was given by Kalai, Lifshitz, Minzer, and Ziegler [FOCS'24]. Their result uses the four-query BLR test and analyzes it via a dense model theorem for Gowers uniformity norms.

In contrast with their approach, our proof is elementary, relying on simple bounds on the Krawchouk polynomials. Additionally, our results extend to *small-bias subsets* of the hypercube, and, using a modified version of the BLR test, to slices over the general vector space $\mathbb{F}_q^n$. This gives the first low soundness linearity tests in these settings.

1 Introduction

Given oracle access to a boolean function, $f : \{0,1\}^n \to \{0,1\}$, we are interested in checking if f is *close* to being a linear function using a small number of queries. In theoretical computer science, this question is popularly known as the *linearity testing* problem.

The linearity testing problem (and its various variants) has been widely studied in the literature due to its key role in many applications across theoretical computer science. An important work in this area is the famous Blum–Luby–Rubinfeld (BLR) test [BLR90] that states if a function, f, passes the check $f(x+y) = f(x) + f(y)$ with non-trivial probability over a random pair (x, y), then f must correlate with some linear function.

The starting point of our work is the linearity testing problem over a Boolean slice. Let $t \leqslant n$ be any non-negative integer. The t-slice, denoted by $\mathcal{S}_t \subseteq \{0,1\}^n$, is the the set of all t-weight (Hamming) vectors. Now, given a function $f : \mathcal{S}_t \to \{0,1\}$, the task is to test whether f is close to some linear function restricted to the t-slice.

Motivated by questions in hardness amplification and direct product testing, David, Dinur, Goldenberg, Kindler, and Shinkar [DDG+17] first studied the linearity testing problem over slice. They showed that if $f : \mathcal{S}_t \subseteq \{0,1\}^n$ passes the BLR test (appropriately adopted to the slice setting) with probability at least $1 - \alpha$, then it must be $(1 - O(\alpha))$-close to some linear function restricted to t-slice and their result holds for any $1 \leqslant t \leqslant n/2$. Here, two functions are called ε-close if they agree on ε-fraction of inputs. [DDG+17] left the significantly more difficult (the *low soundness*) version of the problem open where the test passing probability can be very close to $1/2$. Recently, Kalai, Lifshitz, Minzer, and Ziegler [KLMZ24] gave the first low-soundness test for functions over the half-slice. The test they used was the following k-query variant of the BLR test:

k-query BLR Test

- Sample $(x_1, \ldots, x_k) \sim S^k$ such that $x_1 + \cdots + x_k = 0$.
- If $f(x_1) + \cdots + f(x_k) = 0$: return 1; otherwise: return 0

Using the four-query version of this test (i.e., $k = 4$ above), they proved the following,

Theorem 1.1 ([KLMZ24])**.** *Let, $f : \mathcal{S}_{n/2} \to \{0,1\}$ be a function over the middle slice. Then if f passes the four-query BLR test with probability at least $\frac{1+\delta}{2}$, then there exists a affine function $\varphi : \{0,1\}^n \to \{0,1\}$, such that*

$$\Pr_{\vec{x} \sim \mathcal{S}_{n/2}} \left[f(x) = \varphi(\vec{x}) \right] \geqslant \frac{1}{2} + \frac{\sqrt{\delta}}{400\sqrt{2}} .$$

One drawback of this result is that the agreement guarantee is quite weak. For instance, even if the test passing probability is close to 1, the closest function is only guaranteed to have a tiny agreement of 0.50018 (note that 0.5 agreement is trivial here). This contrasts with the situation over the full hypercube for which the guaranteed agreement tends to 1 as $\eta \to 1$. Our first result addresses this and bridges the gap between the hypercube and the half-slice by using the six-query BLR test.

Theorem 1.2 (Testing over Boolean Half-Slice)**.** *Let, $f : \mathcal{S}_{n/2} \to \{0,1\}$ be a function over the half-slice. Then if f passes the above six-query BLR test with probability at least $\frac{1+\delta}{2}$, then there exists an affine function $\varphi : \{0,1\}^n \to \{0,1\}$, such that*

$$\Pr_{\vec{x} \sim \mathcal{S}_{n/2}} \left[f(x) = \varphi(\vec{x}) \right] \geqslant \frac{1}{2} + \frac{\sqrt{\delta}}{2} .$$

Theorem 1.2 yields a guaranteed agreement of 1 as the test passing probability tends to 1. Our proof is also much simpler than that of [KLMZ24], which uses (in a black-box manner) a non-trivial dense model theorem due to [DK22] among other intricate techniques. In comparison, our approach only uses basic Fourier analysis.

Our main technical result shows that if any subset, $S \subseteq \mathbb{F}_q^n$ satisfies a certain Fourier analytic condition (see Eq. (4)), then we can test linearity for functions over S. Using this criterion, we can analyze subsets beyond the Boolean half-slice.

One such family of sets is *small-bias sets* of $\mathbb{F}_2^n$. Small-bias sets were introduced by Naor and Naor [NN93], and these have applications ranging from error-correcting codes to cryptography. There are many constructions of such sets in the literature, both random and explicit. These small-bias sets are unstructured and of exponentially smaller size than the slice. Therefore, testing over such a set is a priori more challenging. However, using our criterion, we obtain the first low-soundness linearity test over such sets (Theorem 3.8).

Slice over q-ary hypercube Our criteria is field-agnostic so the results generalize to $\mathbb{F}_q$ as well, but with For a general q, the BLR test does not suffice (even for the complete cube) and thus, we use the following variant of the BLR test introduced by Kiwi [Kiw03]:

$\mathbb{F}_q$-Test$_k$

- Sample $(x_1, \ldots, x_k) \sim S^k$ and $(a_1, \ldots, a_k) \in \mathbb{F}_q^*$ such that $a_1 x_1 + \cdots + a_k x_k = 0$.
- If $a_1 f(x_1) + \cdots + a_k f(x_k) = 0$: return 1; otherwise: return 0

Theorem 1.3 (Test over $\mathbb{F}_q^n$). *Let $\mathcal{S}_{\frac{q-1}{q}n} \subseteq \mathbb{F}_q^n$ be the set of vectors of Hamming weight $\frac{q-1}{q}n$. If for any odd $k \geqslant 5$, $f : S \longrightarrow \mathbb{F}_q$ passes $\mathbb{F}_q$-Test$_k$ with probability $\frac{1+(q-1)\delta}{q}$, then there exists a linear function $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$, such that,*

$$\operatorname{agr}(f, \varphi) \geqslant \frac{1}{q} + \frac{(q-1)}{q} \cdot \delta \cdot (1 - o_n(1)).$$

It is not clear if it is possible to derive this result using the approach of [KLMZ24] as their techniques seem to be tailored for the Boolean case.

Note that this result differs from the Boolean case in two aspects. Firstly, the agreement is with a truly linear function (and not an affine function). And secondly, the guarantee is slightly weaker, i.e., the agreement is linear in δ instead of $\sqrt{\delta}$.

1.1 Our Techniques

Even though linearity testing is a well-studied problem, very few results are known in the low soundness regime. To tackle this issue, [MR25] recently proposed a general framework to design and analyze such tests. We quickly review the initial steps of their methodology as it serves as an inspiration for our approach. The description here focuses on the Boolean case, but the $\mathbb{F}_q^n$ case follows similarly, albeit with appropriate modifications.

A key way [MR25] differs from existing works is that instead of starting with a pre-defined test, it starts by analyzing the main quantity of interest - agreement of f with the closest homomorphism. In particular, for boolean functions over slice, the key quantity is $\max_\varphi \operatorname{agr}(f, \varphi)$ and for any distribution $\mathcal{D}$ on the set of linear functions, it satisfies the inequality:

$$\max_\varphi \operatorname{agr}(f, \varphi) \geqslant \mathop{\mathbb{E}}_{\varphi \sim \mathcal{D}} \left[\operatorname{agr}(f, \varphi)\right].$$

Due to certain technical reasons, for functions over $\mathbb{F}_2^n$, it is more prudent to work with the following shifted version of the agreement:

$$\widetilde{\text{agr}}(f, \varphi) \;:=\; 2\,\text{agr}\,(f, \varphi) - 1.$$

It can be easily seen that any lower bound on $\widetilde{\text{agr}}(f, \varphi)$ translates to an (adjusted) lower bound on $\text{agr}\,(f, \varphi)$. One of the main insights of [MR25] is to consider the distribtuion $\mathcal{D}$ that samples φ with probability proportional to $\widetilde{\text{agr}}(f, \varphi)^k$. This results in the following inequality:

$$\max_{\varphi} \widetilde{\text{agr}}(f, \varphi)^t \;\geqslant\; \frac{\sum_{\varphi} \widetilde{\text{agr}}(f, \varphi)^{2k+t}}{\sum_{\varphi} \widetilde{\text{agr}}(f, \varphi)^{2k}}\,. \tag{1}$$

Moreover, the expressions of the form: $\sum_{\varphi} \widetilde{\text{agr}}(f, \varphi)^k$ can be analyzed for functions over the full hypercube, from which it can be deduced that the ratio in Eq. (1) is the same as the ratio of probabilities of passing certain tests. This implies a lower bound on the maximum agreement in terms of such probabilities. Motivated by this, we also consider relations of the form Eq. (1). We utilize Fourier analysis[1] to compute the k-th level sum $\sum_{\varphi} \widetilde{\text{agr}}(f, \varphi)^k$. In particular, we begin by showing that if $f : S \to \{0, 1\}$ passes the Test_k with probability δ_k then:

$$\mathop{\mathbb{E}}_{\varphi \in \widehat{\mathbb{Z}_2^n}} \left[\widetilde{\text{agr}}(f, \varphi)^k\right] \;=\; P_k(S)\,\cdot \delta_k\,, \tag{2}$$

$$\text{where,}\quad P_k(S) \;=\; \Pr_{\vec{x} \sim S^k}\left[\textstyle\sum_{i=1}^k x_i = 0\right]. \tag{3}$$

Using Eq. (1), we can get a $(2k + t)$-query testing result over a subset S if we have,

$$\frac{P_{2k+t}(S)}{P_{2k}(S)} \;\geqslant\; c_{k,t}\,. \tag{4}$$

When S is the full hypercube, it is possible to pick $t = 1$ and $k = 1$, and bound the above ratio. This recovers the three-query BLR test and its analysis. Unfortunately, when S is the Boolean half-slice, this ratio is $O(n^{-c})$ for this choice of k, t, giving an extremely weak bound. However, we show that this can be remedied by picking a larger k, i.e., for any $k \geqslant 2$ and $t \geqslant 1$. In particular, it is possible to set $k = 2$ and $t = 2$, giving a six-query test.

Bounds on Krawchouk polynomials The quantity, $P_k(S)$, has been studied in coding theory, particularly in the context of weight distribution of random linear codes. This quantity can be written as the k^{th}-moment of the (appropriately normalized) Fourier coefficients of the indicator of the set S. When the set S is the slice, these coefficients are given by the *Krawchouk polynomials*, and expressions for the k^{th}-moment have been studied in earlier works such as [Cal96, Cal97, Pol19, CG21, Sam24]. While one could potentially use bounds from these works in our setting, we provide elementary proofs of all the bounds we need to keep the paper self-contained.

[1] It is perhaps possible to do such computations in a completely Fourier-free manner as in [MR25]. This is because the key quantity $P_k(S)$ is combinatorially defined, and can be bound by direct combinatorial methods.

2 Preliminaries

In this work, we will study linear functions between $\mathbb{F}_q^n$ to $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of order q. The following combinatorial quantity will be crucial to our analysis.

Definition 2.1 (Cycle Probability). Let $k \geqslant 1$ be an integer, and $S \subseteq \mathbb{F}_q^n$. We define,

$$P_k(S) \; := \; \Pr_{x \sim S^k}\left[\sum_{i=1}^{k} x_k = 0\right].$$

We will use Fourier analysis to bound the above quantity. To do so, we use the fact that $\mathbb{F}_q^n$ has the structure of an abelian group under (coordinate-wise) addition. Using this structure, one can define a Fourier basis and a Fourier transform. We first give the general definition here, and its implications that we will need.

Definition 2.2 (Characters and Fourier Transform over G). For every finite abelian group G, there exists a set (which is also a group) $\hat{G}$ of its *characters*, i.e., the set of linear functions, $\hat{G} = \{\chi : G \to \mathbb{C} \mid \chi \text{ is linear}\}$. Additionally, $G \cong \hat{G}$ as groups, and one has the general Fourier transform for any $f : G \to \mathbb{C}$,

$$\hat{f}(\chi) \; := \; \mathop{\mathbb{E}}_{x \sim G}[f(x) \cdot \overline{\chi}(x)]\,, \qquad \text{[Fourier Coefficients]}$$

$$f(x) \; = \; \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x)\,, \qquad \text{[Fourier Transform]}$$

$$\|f\|_2^2 \; = \; \mathop{\mathbb{E}}_{x \in G}\left[|f(x)|^2\right] \; = \; \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2\,. \qquad \text{[Plancharel Theorem]}$$

We now state the key way in which we use the Fourier transform to obtain an expression for our quantity $P_k(S)$.

Fact 2.3 (Fourier Expression for cycles). *Let $S \subseteq \mathbb{F}_q^n$ be any subset, and ι_S, be the indicator of the set normalized by the density, i.e., $\iota_S = \frac{q^n}{|S|} \cdot \mathbb{1}_S$. Then,*

$$P_k(S) \; = \; \mathbb{E}_\chi\left[\, \widehat{\iota_S}(\chi)^k\right].$$

Proof. Let T_S be the normalized adjacency matrix of $\mathrm{Cay}(\mathbb{F}_q^n, S)$. Then, its eigenvalues are $\{\widehat{\iota_S}(\chi) \mid \chi \in \widehat{\mathbb{F}_q^n}\}$. Now, since the graph is a Cayley graph, the number of k-cycles containing the identity are $\frac{\mathrm{Tr}(T_S^k)}{q^n}$ which is the same as $P_k(S)$. ∎

Notation 2.4 (Shifted Agreement). We will work thoughout with the following quantity,

$$\widetilde{\mathrm{agr}}(f, \varphi) = \frac{q\,\mathrm{agr}\,(f, \varphi) - 1}{q - 1}, \text{ where }, \mathrm{agr}\,(f, \varphi) \; = \; \Pr_{x \in S}[f(x) = \varphi(x)].$$

Note that this quantity depends on S but we omit denoting it as it will be unambiguous.

3 Linearity Test for the Boolean Half-Slice

In this section, we give a proof of Theorem 1.2. While the proof of the general result is along identical lines, we present the Boolean case separately for the reader interested specifically in this case. We consider $\mathbb{Z}_2 = \{0, 1\}$ as the additive group under addition modulo 2.

Lemma 3.1 (Moment Expression). *Let $S \subseteq \mathbb{Z}_2^n$, and $f : S \to \mathbb{Z}_2$, that passes the k-query BLR Test with probability $\frac{1+\delta_k}{2}$. Then,*

$$\mathop{\mathbb{E}}_{\varphi \in \widehat{\mathbb{Z}_2^n}} \left[\widetilde{\mathrm{agr}}(f, \varphi)^k \right] = P_k(S) \cdot \delta_k \,.$$

Proof. We begin by observing that,

$$\begin{aligned} \mathrm{agr}\,(f, \varphi) &= \mathop{\mathbb{E}}_{x \sim S} \left[\frac{1 + (-1)^{f(x) + \varphi(x)}}{2} \right] \\ \widetilde{\mathrm{agr}}(f, \varphi) &= 2\,\mathrm{agr}\,(f, \varphi) - 1 = \mathop{\mathbb{E}}_{x \sim S} \left[(-1)^{f(x)+\varphi(x)} \right]. \end{aligned}$$

Using this expression, we compute,

$$\begin{aligned} \widetilde{\mathrm{agr}}(f, \varphi)^k &= \mathop{\mathbb{E}}_{x_1, \cdots x_k \sim S} \left[(-1)^{\sum_i (f(x_i) + \varphi(x_i))} \right], \\ \mathop{\mathbb{E}}_{\varphi \in \mathrm{Hom}(\mathbb{F}_2^n, \mathbb{Z}_2)} \left[\widetilde{\mathrm{agr}}(f, \varphi)^k \right] &= \mathop{\mathbb{E}}_{x_1, \cdots x_k \sim S} \left[(-1)^{\sum_i f(x_i)} \cdot \mathop{\mathbb{E}}_{\varphi} \left[(-1)^{\varphi(\sum_i x_i)} \right] \right]. \end{aligned}$$

The last step here uses the linearity of φ. Now, for any $v \in \mathbb{F}_2^n$, we have,

$$\mathop{\mathbb{E}}_{\varphi} \left[(-1)^{\varphi(v)} \right] = \mathbb{1}_{v=0}.$$

Plugging this back, we get,

$$\begin{aligned} \mathop{\mathbb{E}}_{\varphi \in \mathrm{Hom}(\mathbb{F}_p^n, \mathbb{Z}_p)} \left[\widetilde{\mathrm{agr}}(f, \varphi)^k \right] &= \mathop{\mathbb{E}}_{x_1, \cdots x_k \sim S} \left[(-1)^{\sum_i f(x_i)} \cdot \mathbb{1}_{\sum_i x_i = 0} \right] \\ &= P_k(S) \cdot \mathop{\mathbb{E}}_{\substack{x_1, \cdots x_k \sim S \\ \sum_i x_i = 0}} \left[(-1)^{\sum_i f(x_i)} \right] \\ &= P_k(S) \cdot \widetilde{\delta}_k \,. \qquad \blacksquare \end{aligned}$$

Krawtchouk Bounds Lemma 3.1 shows that the key quantity to be analyzed is $P_k(S)$. For the half-slice $\mathcal{S}_{\frac{n}{2}}$, $P_k(\mathcal{S}_{\frac{n}{2}})$ can be computed using the Krawtchouk polynomials as the slice is invariant under permutations (and therefore its indicator is a symmetric function). This expression is standard, and the general version is given in Fact 4.7 and Fact 4.8. For the Boolean half-slice, one gets,

$$2^n \cdot |\mathcal{S}_{\frac{1}{2}}|^k \cdot P_k(\mathcal{S}_{\frac{1}{2}}) = \sum_{x=0}^{n} \binom{n}{x} \cdot \mathcal{K}_k(x)^k = \sum_{x=0}^{n} \binom{n}{x} \cdot \left(\sum_{i=0}^{n} \binom{x}{i} \binom{n-x}{\frac{n}{2} - i} (-1)^i \right)^k \tag{5}$$

The heart of the next lemma is a bound on these *Krawtchouk polynomials*, $\mathcal{K}_k(x)$. We prove a general bound later (Claim 4.9) and avoid repeating its proof here.

Lemma 3.2 (Cycle Counts)**.** *Let* $n \geqslant 10^8$ *and* $k \geqslant 4$ *be even integers. Then we have,*

$$P_k(\mathcal{S}_{\frac{n}{2}}) \;=\; 2 \cdot 2^{-n} \cdot \Big(1 + O\big(n^{3-k}\big)\Big).$$

Proof (assuming Claim 4.9). We will write $k = 2m$ for some $m \geqslant 2$. By Eq. (5) we have that,

$$2^n \cdot P_{2m}(\mathcal{S}_{\frac{n}{2}}) \;=\; \sum_{x=0}^{n} \binom{n}{x} \cdot \left(\frac{\mathcal{K}_k(x)}{|\mathcal{S}_{\frac{n}{2}}|}\right)^{2m} \;=:\; \sum_{x=0}^{n} T_x.$$

We will now use Claim 4.9 to bound the terms. We assume here that $m \geqslant 2$.

$$\begin{aligned}
&T_0 \;=\; T_n \;=\; 1,\\
&T_1 \;=\; T_{n-1} \;=\; 0,\\
&T_2 \;=\; T_{n-2} \;=\; O(n^{2-2m}),\\
&T_x \;\leqslant\; n^m \cdot \binom{n}{x}^{1-m} \;\leqslant\; O\Big(n^m \cdot n^{(1-m)x}\Big), \qquad \forall\, x \in [3, n-3],\\
\Rightarrow &\sum_{x=3}^{n-3} T_x \;\leqslant\; O(n^{3-2m}).
\end{aligned}$$

Thus,

$$2^n \cdot P_{2m}(\mathcal{S}_{\frac{n}{2}}) \;=\; T_0 + T_n + \sum_{x=3}^{n-3} T_x \;=\; 2 + O(n^{3-2m}). \qquad \blacksquare$$

We are now ready to prove a general version of Theorem 1.2 for an arbitrary k.

Theorem 3.3 (Test for the Boolean Half-Slice)**.** *Let* $\mathcal{S}_{\frac{n}{2}}$ *denote the half-slice. Let any* $k \geqslant 6$ *be any even integer. If a function* $f : \mathcal{S}_{\frac{n}{2}} \longrightarrow \{0,1\}$ *passes the k-query BLR test with probability* $\frac{1+\delta}{2}$*, then:*

$$\max_{\varphi \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)} \mathrm{agr}\,(f, \varphi) \;\geqslant\; \frac{1}{2} + \frac{\sqrt{\delta}}{2} \cdot \big(1 - o_n(1)\big).$$

Proof. The main result follows immediately from the lemmas we have proven. The starting point is the following inequality,

$$\begin{aligned}
\max_{\varphi \in \mathrm{Lin}(\mathbb{F}_2^n, \mathbb{F}_2)} \widetilde{\mathrm{agr}}(f, \varphi)^2 \;&\geqslant\; \frac{\sum_{\varphi \in \mathrm{Lin}(\mathbb{F}_2^n, \mathbb{F}_2)} \widetilde{\mathrm{agr}}(f, \varphi)^k}{\sum_{\varphi \in \mathrm{Lin}(\mathbb{F}_2^n, \mathbb{F}_2)} \widetilde{\mathrm{agr}}(f, \varphi)^{k-2}}\\
&=\; \frac{P_k(\mathcal{S}_{\frac{n}{2}}) \cdot \delta_k}{P_{k-2}(\mathcal{S}_{\frac{n}{2}}) \cdot \delta_{k-2}} && [\text{Lemma 3.1}]\\
&\geqslant\; \frac{P_k(\mathcal{S}_{\frac{n}{2}})}{P_{k-2}(\mathcal{S}_{\frac{n}{2}})} \cdot \delta_k && [\delta_{k-2} \leqslant 1]\\
&\geqslant\; (1 + o_n(1))^{-1} \cdot \delta_k\,. && [\text{Lemma 3.2}]
\end{aligned}$$

This implies that there exists a linear function φ such that

$$|2\,\mathrm{agr}\,(f,\varphi)-1| \;\geqslant\; (1-o_n(1))\cdot\sqrt{\delta}.$$

Now, for either φ or $1+\varphi$, this term is positive (i.e., φ or $1+\varphi$ has an agreement of $> \frac{1}{2}$ with f), and thus for one of these two affine functions, we have the conclusion. ■

3.1 Linearity Testing over small-bias spaces

In this section, we will show how our techniques immediately yield testing results when the subset S is an ε*-biased set*. This is a direct consequence of the fact that their Fourier coefficients are very small, and thus, the quantity $P_k(S)$ saturates quickly.

Definition 3.4 (ε-biased sets)**.** A set $S \subset \mathbb{F}_2^n$ is called an ε-biased set if for every non-trivial character χ, we have the bound of $|\hat{\iota}_S(\chi)| \leqslant \varepsilon$, where $\iota_S = \frac{2^n}{|S|}\cdot \mathbb{1}_S$ is the normalized indicator.

We will be interested in the regime of very low bias, i.e., $\varepsilon \leqslant 2^{-cn}$ for some constant c. In this regime, the set has to be quite dense, and we quickly mention two constructions, a random one, and another via *bent functions* of density $\frac{1}{2}$.

Fact 3.5 (Random sets have small bias [AR94])**.** *Let $S \subseteq \mathbb{F}_2^n$ be a random set of size $\Omega(n\cdot 2^{2cn})$. Then, with high probability, S is an 2^{-cn}-biased set.*

Our result only requires a quantitative bound on the bias and does not rely on any structural properties of the set. However, we mention a more concrete construction of such very small-bias sets that is well-studied in the literature.

Definition 3.6 (Bent Functions)**.** A function $f:\mathbb{F}_2^n \to \{0,1\}$ is called a bent function if it satisfies: $\max_\varphi \mathrm{agr}(f,\varphi) = \frac{1}{2} - 2^{-n/2}$, where max is taken over all linear functions.

An equivalent characterization of bent functions is via its Fourier spectrum; i.e., a Boolean function $f:\mathbb{F}_2^n \to \{0,1\}$ is bent if and only if the absolute value of every Fourier coefficient of the $\{\pm 1\}$-valued function, $(-1)^{f(\cdot)}$ is $2^{-n/2}$. This implies the following fact:

Fact 3.7. *If a subset, $S \subseteq \mathbb{F}_2^n$ is the support of a bent function then, S is an $2^{-\frac{n}{2}-1}$-biased set.*

Theorem 3.8. *Let $S \subseteq \mathbb{F}_2^n$ be an ε-biased set for $\varepsilon \leqslant 2^{-cn}$. Let $k > \frac{1}{c}$ be an even integer. If, $f:\mathcal{S}_{\frac{n}{2}} \to \{0,1\}$ passes the k-query BLR test with probability $\frac{1+\delta}{2}$,*

$$\max_{\varphi\in \mathrm{Aff}(\mathbb{F}_2^n,\mathbb{F}_2)} \mathrm{agr}\,(f,\varphi) \;\geqslant\; \frac{1}{2}+\frac{\sqrt{\delta}}{2}\cdot(1-o_n(1)).$$

In particular, if S is the support of a bent function, we get a 4-query test.

Proof. For an ε-biased set, all non-trivial eigenvalues are at most ε. Thus,

$$\begin{aligned} 2^n\cdot P_k(S) \;&=\; \widehat{\iota_S}(\vec{0})^k + \textstyle\sum_{\gamma\in\mathbb{F}_2^n\setminus\vec{0}}\; \widehat{\iota_S}(\gamma)^k \\ &\approx\; 1+2^n\varepsilon^k. \end{aligned}$$

Therefore, for $\varepsilon \leqslant 2^{-cn}$, and $k > \frac{1}{c}$, we have $\frac{P_k(S)}{P_{k-2}(S)} \geqslant 1-o_n(1)$. The result now follows identiacally along the lines of Theorem 3.3. ■

4 Linearity Testing on the q-slice

Let $\mathbb{F}_q$ be a finite field of characteristic p, i.e., $q = p^r$. In this section, we focus on testing the proximity of a given function, $f : \mathbb{F}_q^n \to \mathbb{F}_q$, to $\mathrm{Lin}(\mathbb{F}_q^n, \mathbb{F}_q)$, the set of $\mathbb{F}_q$-linear maps from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. Fix ω, a primitive p-th root of unity. Define the trace map as,

$$\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p,\ \mathrm{Tr}(x) = \sum_{i=0}^{r} x^{p^i}.$$

Fact 4.1 (Characters and Fourier Transform over $\mathbb{F}_q$)**.** *The set of characters of the additive group $\mathbb{F}_q$, i.e., linear functions from $\mathbb{F}_q \to \mathbb{C}^\times$, is given by $\{\omega^{\beta\,\mathrm{Tr}(\cdot)} \mid \beta \in \mathbb{F}_q\}$. Using these characters, the Fourier transform of the function $\mathbb{1}_{z=0} : \mathbb{F}_q \to \mathbb{C}$ is given by,*

$$\mathbb{1}_{z=0} \;=\; \mathop{\mathbb{E}}_{\beta\in\mathbb{F}_q}\left[\omega^{\beta\,\mathrm{Tr}(z)}\right].$$

We will use $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ to denote the composition map, $\psi(\cdot) := \omega^{\mathrm{Tr}(\cdot)}$.

Using this fact, we get a $\mathbb{F}_q$-version of the useful “trick” over $\mathbb{F}_2$ that $\mathbb{1}_{x=y} = \frac{1+(-1)^{x+y}}{2}$.

Corollary 4.2. *Let S be any finite set and $f, \varphi : S \to \mathbb{F}_q$ be any pair of functions, Then,*

$$\widetilde{\mathrm{agr}}(f,\varphi) \;=\; \mathop{\mathbb{E}}_{x\sim S}\left[\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\psi^{a}\big(f(x)-\varphi(x)\big)\right]\right].$$

Proof. It is a direct computation using the above fact.

$$\begin{aligned}
\mathrm{agr}\,(f,\varphi) \;&=\; \mathop{\mathbb{E}}_{x\sim S}\left[\mathbb{1}_{f(x)-\varphi(x)=0}\right] \\
&=\; \mathop{\mathbb{E}}_{x\sim S}\left[\mathop{\mathbb{E}}_{\beta\in\mathbb{F}_q}\left[\psi^{\beta}\big(f(x)-\varphi(x)\big)\right]\right] && \text{[Fact 4.1]} \\
&=\; \mathop{\mathbb{E}}_{x\sim S}\left[\frac{q-1}{q}\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\psi^{a}\big(f(x)-\varphi(x)\big)\right] + \frac{1}{q}\right].
\end{aligned}$$

The last equality separates out the term corresponding to the trivial character, i.e., $\beta = 0$. The proof follows by rearranging as $\widetilde{\mathrm{agr}}(f,\varphi) = \frac{q\,\mathrm{agr}\,(f,\varphi)-1}{q-1}$. ∎

4.1 The test and its analysis

Over general fields $\mathbb{F}_q$, the BLR test does not yield good agreement guarantees, even over the full hypercube $\mathbb{F}_q^n$. To remedy this, Kiwi [Kiw03] defined a modification of the BLR test, and alternate Fourier-theoretic proofs for this test were given by [Gop13, GKS06]. Therefore, it is natural to use this test for functions over subsets of $\mathbb{F}_q^n$.

$\mathbb{F}_q$-Test$_k$

- Sample $(a_1,\ldots,a_k) \sim \mathbb{F}_q^*$ and $(x_1,\ldots,x_k) \sim S^k$ such that $a_1x_1 + \cdots + a_kx_k = 0$.
- If $a_1f(x_1) + \cdots + a_kf(x_k) = 0$: return 1; otherwise: return 0.

Test Distribution Let μ_k be the distribution over $(\mathbb{F}_q^*)^k \times S^k$ that is uniformly supported on elements, $((a_1, \ldots, a_k), (x_1, \ldots, x_k))$ such that $\sum_i a_i x_i = 0$. This is the distribution used to define the test. We note two useful properties of this distribution.

Claim 4.3. *For any fixed $\vec{a} = (a_1, \cdots a_k) \in (\mathbb{F}_q^*)^k$, the distribution, μ_k, satisfies:*

$$\mu_k(\vec{a}, \vec{x}) = \mu_k(\beta\vec{a}, \vec{x}), \quad \textit{for any } \beta \in \mathbb{F}_q^*,\ \vec{x} \in S^k. \tag{6}$$

$$\Pr_{\vec{x}\sim S^k}\left[\textstyle\sum_i a_i x_i = 0\right] = \Pr_{\vec{x}\sim S^k}\left[\textstyle\sum_i x_i = 0\right] = P_k(S). \tag{7}$$

Proof. The first claim is direct as $\sum_i a_i x_i = 0$ if and only if $\sum_i \beta a_i x_i = 0$ as $\beta \neq 0$. For the second claim, we observe that there is a bijection matching the support of the two sides of the equation. Since the probability is uniform over the support, their total probability mass is the same. Let $\vec{x}$ be such that $\sum_i x_i = 0$, i.e., $\mu(\vec{1}, \vec{x}) \neq 0$. We map the vector to $(a_1 x_1, \ldots, a_k x_k)$. This clearly satisfies that $\sum_i a_i x_i = 0$, and thus it lies in the support. The map is clearly injective, and it is surjective because $a_i \neq 0$, so it can be inverted. ∎

Claim 4.4 (Test Passing Probability)**.** *Let $S \subseteq \mathbb{F}_q^n$, $f : S \to \mathbb{F}_q$. Let $\frac{1+(q-1)\delta_k}{q}$ be the probability that f passes the General Test. Then, we have*

$$\delta_k = \mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu_k}\left[\, \psi\left(\textstyle\sum_i a_i f(x_i)\right)\right].$$

Proof. We start by rewriting the test probability usinng Fact 4.1.

$$\begin{aligned}
\delta_k &= \mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\mathbb{1}_{\sum_i a_i f(x_i)=0}\right] \\
&= \mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\mathop{\mathbb{E}}_{\beta\sim\mathbb{F}_q}\left[\psi\left(\beta \textstyle\sum_i a_i f(x_i)\right)\right]\right] && \text{[Fact 4.1]} \\
&= \frac{q-1}{q}\mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\mathop{\mathbb{E}}_{\beta\sim\mathbb{F}_q^*}\left[\psi\left(\beta \textstyle\sum_i a_i f(x_i)\right)\right]\right] + \frac{1}{q}. && \text{[Separating } \beta = 0\text{]} \\
\widetilde{\delta}_k &= \mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\mathop{\mathbb{E}}_{\beta\sim\mathbb{F}_q^*}\left[\psi\left(\beta \textstyle\sum_i a_i f(x_i)\right)\right]\right] && \text{[Rearranging].}
\end{aligned}$$

Now, we will use the invariance property of the distribution.

$$\begin{aligned}
\widetilde{\delta}_k &= \mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\mathop{\mathbb{E}}_{\beta\sim\mathbb{F}_q^*}\left[\psi\left(\beta \textstyle\sum_i a_i f(x_i)\right)\right]\right]. \\
&= \mathop{\mathbb{E}}_{\beta\sim\mathbb{F}_q^*}\left[\mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\psi\left(\beta \textstyle\sum_i a_i f(x_i)\right)\right]\right] && \text{[Fubini].} \\
&= \mathop{\mathbb{E}}_{\beta\sim\mathbb{F}_q^*}\left[\mathop{\mathbb{E}}_{(\beta^{-1}\vec{a},\vec{x})\sim\mu}\left[\psi\left(\beta \textstyle\sum_i \beta^{-1} a_i f(x_i)\right)\right]\right] && \text{[Eq. (6)].} \\
&= \mathop{\mathbb{E}}_{(\vec{a},\vec{x})\sim\mu}\left[\psi\left(\textstyle\sum_i a_i f(x_i)\right)\right]. && \text{[Using Eq. (6) again].}
\end{aligned}$$

∎

We now write an exact expression for the k-moment of the agreement. This is the key lemma that enables the analysis of the modified BLR test.

Lemma 4.5 (Agreement Expression)**.** *Let* $f : S \to \mathbb{F}_q$*, which we extend to* $\mathbb{F}_q^n$ *by defining it to be zero outside* S*.*

$$\mathop{\mathbb{E}}_{\varphi \in \mathrm{Lin}(\mathbb{F}_q^n, \mathbb{F}_q)} \left[\widetilde{\mathrm{agr}}(f, \varphi)^k \right] = P_k(S) \cdot \delta_k$$

Proof. We start by using the expression for the agreement from Corollary 4.2,

$$\widetilde{\mathrm{agr}}(f, \varphi) = \mathop{\mathbb{E}}_{x \sim S} \left[\mathop{\mathbb{E}}_{a \in \mathbb{F}_q^*} \left[\psi\left(af(x) - a\varphi(x)\right) \right] \right],$$

$$\widetilde{\mathrm{agr}}(f, \varphi)^k = \mathop{\mathbb{E}}_{\vec{x} \sim S} \left[\mathop{\mathbb{E}}_{\vec{a} \in {\mathbb{F}_q^*}^k} \left[\psi\left(\textstyle\sum_i a_i (f(x_i) - \varphi(x_i))\right) \right] \right].$$

Since ψ is a character, it satisfies $\psi(a+b) = \psi(a) \cdot \psi(b)$. Using this, we get,

$$\mathop{\mathbb{E}}_{\varphi \in \mathrm{Lin}(\mathbb{F}_q^n, \mathbb{F}_q)} \left[\widetilde{\mathrm{agr}}(f, \varphi)^k \right] = \mathop{\mathbb{E}}_{\substack{\vec{x} \sim S^k \\ \vec{a} \in {\mathbb{F}_q^*}^k}} \left[\psi\left(\textstyle\sum_i a_i f(x_i)\right) \cdot \mathop{\mathbb{E}}_{\varphi} \left[\psi \circ \varphi\left(-\textstyle\sum_i a_i x_i\right) \right] \right].$$

Now, for any $v \in \mathbb{F}_q^n$, we have,

$$\mathop{\mathbb{E}}_{\varphi \in \mathrm{Lin}(\mathbb{F}_q^n, \mathbb{F}_q)} [\psi \circ \varphi(v)] = \begin{cases} 1 & \text{if} \quad v = 0, \\ \mathbb{E}_{\beta \in \mathbb{F}_q}[\psi(\beta)] = 0 & \text{if} \quad v \neq 0. \end{cases}.$$

The second equality above uses that the image of v is uniform over $\mathbb{F}_q$ if $v \neq 0$. And then, from Fact 4.1, we get that this sum is $\mathbb{1}_{1=0} = 0$. Plugging this back, we get,

$$\begin{aligned}
\mathop{\mathbb{E}}_{\varphi \in \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q)} \left[\widetilde{\mathrm{agr}}(f, \varphi)^k \right] &= \mathop{\mathbb{E}}_{\substack{\vec{x} \sim S^k \\ \vec{a} \in {\mathbb{F}_q^*}^k}} \left[\psi\left(\textstyle\sum_i a_i f(x_i)\right) \cdot \mathbb{1}_{\sum_i a_i x_i = 0} \right] \\
&= \Pr_{\vec{x} \sim S^k, \vec{a} \in {\mathbb{F}_q^*}^k} \left[\textstyle\sum_i a_i x_i = 0\right] \cdot \mathop{\mathbb{E}}_{(\vec{a}, \vec{x}) \sim \mu} \left[\psi\left(\textstyle\sum_i a_i f(x_i)\right) \right] \\
&= P_k(S) \cdot \delta_k \,. \quad \text{[Eq. (7)]} \quad \blacksquare
\end{aligned}$$

4.2 Cycle counts over the q-slice

Let $\mathcal{S}_t$ be the subset[2] of vectors of Hamming weight t over $\mathbb{F}_q^n$. We will denote the Fourier coefficients of its normalized indicator by $\widehat{\iota}_{q,t}(\chi)$ instead of $\widehat{\iota_{\mathcal{S}_t}}(\chi)$ for brevity. It is a standard fact from the theory of association schemes that these Fourier coefficients are given by the q-*Krawtchouk polynomials*.

Fact 4.6 (Fourier Coefficients of q-slice)**.** [BBIT, Prop 2.84] *Let* $n > 0$ *be an integer and* $0 \leqslant k, t \leqslant n$.

$$\widehat{\iota}_{q,t}(\chi) = \frac{\mathcal{K}_{q,t}(|\chi|)}{|\mathcal{S}_t|} \text{, where, } \quad \mathcal{K}_{q,t}(x) = \sum_{i=0}^{t} \binom{x}{i} \binom{n-x}{t-i} (1-q)^{t-i} \,.$$

[2] We omit denoting q here as we will work with a single fixed q throughout the section.

Fact 4.7. *Let $\mathcal{S}_t \subseteq \mathbb{F}_q^n$ be the subset of vectors of Hamming weight tn over $\mathbb{F}_q^n$. Then,*

$$P_k(\mathcal{S}_t) \;=\; q^{-n} \sum_{x=0}^{n} \binom{n}{x} (q-1)^x \cdot \widehat{\iota}_{q,t}(x)^k$$

Proof. Follows immediately from Fact 2.3 and Fact 4.6. ∎

Some Bounds on Krawtchouk Polynomials

Fact 4.8 (Stirling's Bound). *For any $q, n \geqslant 2$, and $\alpha \in (0,1)$, we have,*

$$|\mathcal{S}_{\alpha n}| \;=\; \binom{n}{\alpha n}(q-1)^{\alpha n} \;\approx\; \frac{1}{\sqrt{2\pi\alpha(1-\alpha)n}} \cdot \left(\frac{(q-1)(1-\alpha)}{\alpha}\right)^{\alpha n} \cdot \frac{1}{(1-\alpha)^n}$$

In particular, for $\alpha = \frac{q-1}{q}$, one gets a bound of $\approx \frac{q^n}{\sqrt{n}}$, while for $\alpha = \frac{1}{2}$, one gets, $\approx \frac{\left(2\sqrt{q-1}\right)^n}{\sqrt{n}}$.

Claim 4.9 (Bounds for the Mean-Slice). *For $t = \frac{q-1}{q} n$, the following bounds hold:*

1. *For any q, $\widehat{\iota}_{q,t}(1) = 0$, and thus for $q = 2$, $\widehat{\iota}_{q,t}(1) = \widehat{\iota}_{q,t}(n-1) = 0$*
2. *For $x = 2, n-2$, the Fourier coefficient satisfies, $|\widehat{\iota}_{q,t}(x)| \;\leqslant\; O\left(\frac{1}{n}\right)$.*
3. *For any $0 \leqslant x \leqslant n$, the Fourier coefficients satisfy, $\widehat{\iota}_{q,t}(x)^2 \;\leqslant\; O(\sqrt{n}) \cdot \binom{n}{x}^{-1} \cdot (q-1)^{-x}$.*

Proof. Observe that for $q = 2$, $\mathcal{K}_{2,t}(n-i) = \mathcal{K}_{2,t}(i)$ for any i as the terms are the same. We now compute the level-1 coefficient.

$$\begin{aligned} \mathcal{K}_{q,t}(1) \;&=\; \binom{n-1}{t}(1-q)^t + \binom{n-1}{t-1}(1-q)^{t-1}, \\ &=\; \binom{n-1}{t}(1-q)^{t-1}\left((1-q) + \frac{t}{n-t}\right) \;=\; 0. \qquad \left[t \;=\; n - \frac{n}{q}\right] \end{aligned}$$

$$\begin{aligned} \mathcal{K}_{q,t}(n-1) \;&=\; \binom{n-1}{t} + \binom{n-1}{t-1}(1-q) \\ &=\; \binom{n-1}{t} q(2-q). \\ |\widehat{\iota}_{q,t}(n-1)| \;&=\; \frac{(2-q)}{(q-1)^{n-1}}. \end{aligned}$$

The second claim is also a direct calculation.

$$\mathcal{K}_{q,t}(2) \;=\; \binom{n-2}{t}(1-q)^t + 2\binom{n-2}{t-1}(1-q)^{t-1} + \binom{n-2}{t-2}(1-q)^{t-2}$$

$$= \binom{n-2}{t-1} \cdot (1-q)^{t-1} \cdot \left(\frac{n-t-1}{t}(1-q) + 2 + \frac{t-1}{n-t}(1-q)^{-1} \right)$$

$$= \binom{n-2}{t-1} \cdot (1-q)^{t-1} \cdot \left(\frac{q-1}{t} + \frac{1}{(q-1)n-t} \right) \qquad \left[t = n - \frac{n}{q} \right]$$

$$= -\binom{n-2}{t-1} \cdot (1-q)^{t-2} \cdot \frac{q^2}{n},$$

$$\Rightarrow |\widehat{\iota}_{q,t}(2)| = \frac{1}{(q-1)(n-1)}.$$

The above settles the case for $q = 2$, as $\mathcal{K}_{2,t}(n-2) = \mathcal{K}_{2,t}(2)$. We now compute the expression for a general q.

$$\mathcal{K}_{q,t}(n-2) = \binom{n-2}{t} + 2\binom{n-2}{t-1}(1-q) + \binom{n-2}{t-2}(1-q)^2$$

$$= \binom{n-2}{t-1} \cdot (1-q) \cdot \left(\frac{n-t-1}{t}(1-q)^{-1} + 2 + \frac{t-1}{n-t}(1-q) \right)$$

$$= \binom{n-2}{t-1} \cdot (1-q) \cdot \left(-(1-q)^{-2} + \frac{q}{(q-1)^2 n} + 2 - (q-1)^2 + \frac{q(q-1)}{n} \right)$$

$$|\mathcal{K}_{q,t}(n-2)| \leqslant 2\binom{n-2}{t-1} \cdot (q-1)^3$$

$$\Rightarrow |\widehat{\iota}_{q,t}(n-2)| \leqslant \frac{2n}{(q-1)^{t-2}(n-1)} \leqslant O\left((q-1)^{-(t-2)}\right).$$

The last claim follows from Plancharel (Definition 2.2) when applied to the function, $\iota_{\mathcal{S}_{q,t}}$.

$$\sum_{x=0}^{n} \binom{n}{x}(q-1)^x \cdot \iota_{\mathcal{S}_{q,\alpha n}}(x)^2 = \|\iota_{\mathcal{S}_{q,\alpha n}}\|_2^2 = \frac{q^n}{|\mathcal{S}_{q,\alpha n}|} \leqslant O(\sqrt{n}).$$

Since the terms are non-negative for each x, the above inequality holds for every summand. This implies our desired bound. ∎

We now prove a lemma that we will crucially use.

Lemma 4.10. *Let $q \neq 2$ be a power of a prime, $n \geqslant 10^8$ and $k \geqslant 4$ be even integers. Then,*

$$P_k\left(\mathcal{S}_{\frac{q-1}{q}n}\right) = q^{-n} \cdot \left(1 + O\left(n^{3-k}\right)\right).$$

Proof. We will write $k = 2m$ for some $m \geqslant 2$. By Fact 4.7 and Fact 4.8 we have that,

$$q^n \cdot P_{2m}\left(\mathcal{S}_{\frac{q-1}{q}n}\right) = \sum_{x=0}^{n} \binom{n}{x}(q-1)^x \cdot \widehat{\iota}_{q,t}(x)^{2m} =: \sum_{x=0}^{n} T_x.$$

We will now use Claim 4.9 to bound the terms. We assume here that $m \geqslant 2$.

$$\begin{aligned}
T_0 &= 1,\ T_1 = 0, \\
T_n &= O(2^{-n}) \\
T_2, T_{n-2} &= O(n^{2-2m}) \\
T_x &\leqslant n^m \cdot \left(\binom{n}{x}(q-1)^x\right)^{1-m} \leqslant O\left(n^m \cdot n^{(1-m)x}\right), \qquad \forall\, x \in [3, n-3], \\
\Rightarrow \sum_{x=3}^{n-3} T_x &\leqslant O(n^{3-2m}).
\end{aligned}$$

Now, the result follows by summing up these terms. ∎

We are now ready to prove our final theorem.

Theorem 1.3 (Test over $\mathbb{F}_q^n$). *Let $\mathcal{S}_{\frac{q-1}{q}n} \subseteq \mathbb{F}_q^n$ be the set of vectors of Hamming weight $\frac{q-1}{q}n$. If for any odd $k \geqslant 5$, $f : S \longrightarrow \mathbb{F}_q$ passes $\mathbb{F}_q$-Test$_k$ with probability $\frac{1+(q-1)\delta}{q}$, then there exists a linear function $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$, such that,*

$$\operatorname{agr}(f, \varphi) \geqslant \frac{1}{q} + \frac{(q-1)}{q} \cdot \delta \cdot (1 - o_n(1)).$$

Proof. Lemma 4.10 implies that for any $k \geqslant 2$, we get

$$\frac{P_{2k+1}(\mathcal{S}_{\frac{q-1}{q}n})}{P_{2k}(\mathcal{S}_{\frac{q-1}{q}n})} \geqslant (1 - o_n(1)).$$

Now the main trick of the proof is to use the following inequality:

$$\begin{aligned}
\max_{\varphi \in \mathrm{Lin}(\mathbb{F}_q^n, \mathbb{F}_q)} \widetilde{\operatorname{agr}}(f, \varphi) &\geqslant \frac{\sum_{\varphi \in \widehat{\mathbb{F}_q^n}} \widetilde{\operatorname{agr}}(f, \varphi)^{2k+1}}{\sum_{\varphi \in \widehat{\mathbb{F}_q^n}} \widetilde{\operatorname{agr}}(f, \varphi)^{2k}} \\
&= \frac{P_{2k+1}(\mathcal{S}_{\frac{q-1}{q}n}) \cdot \delta_{2k+1}}{P_{2k}(S) \cdot \delta_{2k}} && [\text{Lemma 4.5}] \\
&\geqslant \frac{P_{2k}(\mathcal{S}_{\frac{q-1}{q}n})}{P_{2k}(\mathcal{S}_{\frac{q-1}{q}n})} \cdot (\delta_{2k+1}) && [\delta_{2k} \leqslant 1] \\
&\geqslant (1 - o_n(1)) \cdot \delta_{2k+1}.
\end{aligned}$$

Thus, we get $\frac{q \max_\varphi \operatorname{agr}(f,\varphi) - 1}{q-1} \geqslant (1 - o_n(1)) \cdot \delta_{2k}$, which yields the claim. ∎

References

[AR94] Noga Alon and Yuval Roichman. Random Cayley Graphs and Expanders. 5(2):271–285, 1994. doi:10.1002/rsa.3240050203. 8

[BBIT] Eiichi Bannai, Etsuko Bannai, Tatsuro Ito, and Rie Tanaka. *Algebraic Combinatorics*. Number volume 5 in De Gruyter Series in Discrete Mathematics and Applications. De Gruyter. doi:10.1515/9783110630251. 11

[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

[Cal96] Neil J Calkin. Dependent sets of constant weight vectors in gf (q). *Random Structures & Algorithms*, 9(1-2):49–53, 1996. 4

[Cal97] Neil J Calkin. Dependent sets of constant weight binary vectors. *Combinatorics, Probability and Computing*, 6(3):263–271, 1997. 4

[CG21] Andrea Collevecchio and Robert C. Griffiths. A Class of Random Walks on the Hypercube. In Maria Eulália Vares, Roberto Fernández, Luiz Renato Fontes, and Charles M. Newman, editors, *In and Out of Equilibrium 3: Celebrating Vladas Sidoravicius*, volume 77, pages 265–298. Springer International Publishing, Cham, 2021. doi:10.1007/978-3-030-60754-8_13. 4

[DDG+17] Roee David, Irit Dinur, Elazar Goldenberg, Guy Kindler, and Igor Shinkar. Direct Sum Testing. *SIAM Journal on Computing*, 46(4):1336–1369, 2017. doi:10.1137/16M1061655. 2

[DK22] Pandelis Dodos and Vassilis Kanellopoulos. Uniformity norms, their weaker versions, and applications. *Acta Arith*, 203(3):251–270, 2022. 2

[GKS06] Elena Grigorescu, Swastik Kopparty, and Madhu Sudan. Local decoding and testing for homomorphisms. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, volume 4110 of *Lecture Notes in Computer Science*, pages 375–385. Springer, 2006. doi:10.1007/11830924_35. 9

[Gop13] Parikshit Gopalan. A Fourier-Analytic Approach to Reed-Muller Decoding. *IEEE Trans. Inf. Theory*, 59(11):7747–7760, 2013. doi:10.1109/TIT.2013.2274007. 9

[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. 3, 9

[KLMZ24] Gil Kalai, Noam Lifshitz, Dor Minzer, and Tamar Ziegler. A Dense Model Theorem for the Boolean Slice. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 797–805. IEEE, 2024. arXiv:2402.05217, doi:10.1109/FOCS61266.2024.00056. 2, 3

[MR25] Tushant Mittal and Sourya Roy. A General Framework for Low Soundness Homomorphism Testing, 2025. arXiv:2509.05871. 3, 4

[NN93] J. Naor and M. Naor. Small-bias probability spaces: efficient constructions and applications. 22(4):838–856, 1993. doi:10.1137/0222053. 3

[Pol19] Yury Polyanskiy. Hypercontractivity of spherical averages in hamming space. *SIAM Journal on Discrete Mathematics*, 33(2):731–754, 2019. 4

[Sam24] Alex Samorodnitsky. Weight distribution of random linear codes and krawtchouk polynomials. *Random Structures & Algorithms*, 65(2):261–274, 2024. 4