Strong Refutation of Semirandom k-LIN over Larger Fields

Nicholas Kocurek
nkocurek@andrew.cmu.edu
Carnegie Mellon University

Peter Manohar
pmanohar@ias.edu
The Institute for Advanced Study

Abstract

We study the problem of strongly refuting semirandom instances of k-sparse inhomogeneous linear equations over a finite field $\mathbb{F}$. For the case of $\mathbb{F} = \mathbb{F}_2$, this is the problem of refuting semirandom instances of k-XOR. The work of [GKM22] and the follow-up [HKM23] give an $n^{O(\ell)}$-time algorithm to certify that there is no assignment that can satisfy more than $\frac{1}{|\mathbb{F}|} + \varepsilon$-fraction of constraints, provided that the k-XOR instance has $\Omega(n) \cdot \left(\frac{n}{\ell}\right)^{k/2-1} \log n/\varepsilon^4$ constraints, and the work of [KMOW17] provides good evidence that this tight up to a polylog(n) factor via lower bounds for the Sum-of-Squares hierarchy. However, for larger fields, there is a gap of $|\mathbb{F}|^{O(k)}$ between the current best upper and lower bounds.

In this paper, we give an $(|\mathbb{F}^*|n)^{O(\ell)}$-time algorithm to strongly refute semirandom k-LIN instances over any finite field $\mathbb{F}$ provided that the instance has at least $\Omega(n)\cdot\left(\frac{|\mathbb{F}^*|n}{\ell}\right)^{k/2-1}\log(n|\mathbb{F}^*|)/\varepsilon^4$ constraints. We additionally give good evidence that this dependence on the field size $|\mathbb{F}|$ is optimal by proving a lower bound for the Sum-of-Squares hierarchy that matches this threshold up to a polylog$(n|\mathbb{F}^*|)$ factor. Our key technical innovation is a generalization of the "$\mathbb{F}_2$ Kikuchi matrices" of [WAM19, GKM22] to larger fields.

Contents

1 Introduction

A k-LIN instance over a finite field $\mathbb{F}$ is a collection of k-sparse $\mathbb{F}$-linear inhomogeneous equations in n variables. Namely, the instance consists of n variables $x_1, \ldots, x_n$, as well as equations, where each equation has the form $\sum_{i \in I} \alpha_i x_i = b_I$, where $|I| = k$ and $\alpha_i \in \mathbb{F} \setminus \{0\}$. In this paper, we study the problem of strongly refuting instances of k-LIN over a finite field $\mathbb{F}$. Namely, we study the algorithmic task of certifying that all assignments for a given instance satisfy at most $\frac{1}{|\mathbb{F}|} + \varepsilon$-fraction of the equations. While this problem is known to be NP-hard in the worst case, there has been a long line of work on designing algorithms for this task in the average case. In the average case, the first natural model to consider is the *fully random* model, studied in [CGL07, AOW15, RRS17], where all equations are drawn independently and uniformly at random. More recently, there has been much work [AGK21, GKM22, HKM23] on designing algorithms for k-LIN in the harder *semirandom* model, where the "left-hand sides" of the equations are worst case, and only the "right-hand sides" b_I are random.

The problem of refuting k-LIN has been studied extensively in the Boolean case where $\mathbb{F} = \mathbb{F}_2$, where it is also called k-XOR. Building on many prior works [GL03, CGL07, AOW15, BM16, RRS17, AGK21], the work of [GKM22] gives an $n^{O(\ell)}$-time algorithm that, given a semirandom k-LIN instance over $\mathbb{F}_2$, certifies that no assignment can satisfy more than $\frac{1}{2} + \varepsilon$-fraction of the constraints, provided that the instance has at least $O(1) \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell \cdot \mathrm{polylog}(n)/\varepsilon^5$ constraints. A follow-up work of [HKM23] improved the polylog(n) factor in the above threshold to a single $\log n$ factor and the dependence on ε to $1/\varepsilon^4$. In this algorithm, the quantity ℓ is a parameter that allows one to trade-off between the runtime of the algorithm and the number of constraints in the instance required for refutation.

This trade-off between runtime and number of constraints is conjectured to be optimal up to the polylog(n) and ε-factors, with evidence coming in the form of lower bounds in various restricted computational models [Fei02, BGMT12, OW14, MW16, BCK15, KMOW17]. For the sum-of-squares hierarchy, the work of [KMOW17] shows that the canonical degree $\tilde{O}(\ell)$ sum-of-squares algorithm is unable to refute a *random* (and thus also semirandom) k-LIN instance over $\mathbb{F}_2$ with at most $O(1) \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell/\mathrm{polylog}(n)$ constraints, a threshold that matches the algorithmic threshold from [GKM22, HKM23] (and also [RRS17] for random k-LIN) up to a $\left(\log n\right)^{k/2}$ factor. Moreover, the sum-of-squares hierarchy is a powerful semidefinite programming hierarchy that captures many prior algorithms — in particular, the lower bound of [KMOW17] applies to the algorithms of [GL03, CGL07, AOW15, BM16, RRS17, AGK21, GKM22, HKM23] — and so the lower bound of [KMOW17] can be seen as giving good evidence that this $O(1) \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell$ threshold is tight up to polylog(n) factors.

Thus, for the Boolean case of $\mathbb{F} = \mathbb{F}_2$, we have a near-complete understanding: if the number of constraints in the semirandom k-LIN instance is at least $O(1) \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell \cdot \mathrm{polylog}(n)$, then the algorithm of [GKM22, HKM23] can strongly refute the instance in $n^{O(\ell)}$ time, and if the number of constraints is smaller than $O(1) \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell/\mathrm{polylog}(n)$, the lower bound of [KMOW17] provides good evidence that there is no algorithm to refute in $n^{O(\ell)}$ time.

What can we say about this problem over finite fields $\mathbb{F} \neq \mathbb{F}_2$? By simple reductions to the

Boolean case (see Appendix B in [AOW15]), one can give an algorithm to refute if there are $|\mathbb{F}|^{O(k)} \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell \cdot \mathrm{polylog}(n)$ constraints, i.e., we now have an extra factor of $|\mathbb{F}|^{O(k)}$. For lower bounds, the work [KMOW17] also proves a lower bound of $O(1) \cdot \left(\frac{n}{\ell}\right)^{\frac{k}{2}} \ell/\mathrm{polylog}(n)$ constraints for any finite field $\mathbb{F}$, which is the same as before. For constant-sized fields, this is the same behavior that we had in the Boolean case. However, for larger $\mathbb{F}$ of size, say $|\mathbb{F}| = n^{\varepsilon}$, there is a $\mathrm{poly}(n)$ gap between the upper and lower bounds.

Understanding this dependence on the field size for refuting semirandom k-LIN instances has applications to proving lower bounds for locally decodable/correctable codes and information-theoretic private information retrieval schemes, which are essentially equivalent to locally decodable codes over large alphabets. Recent work of [AGKM23] has led to a flurry of improvements in lower bounds for *binary* locally decodable [AGKM23, BHKL24, JM24] and locally correctable codes [KM24a, AG24, KM24b, Yan24] by establishing a connection between these lower bounds and refuting "semirandom-like" instances of k-LIN over $\mathbb{F}_2$. Simple extensions of these results to larger alphabets are known (see Appendix A in [AGKM23, KM24a]). However, the dependence on the alphabet size is not good enough to yield any improvement yet in the known lower bounds for q-server PIR.

Our results. In this paper, we investigate the dependence on the field size in the number of constraints required to refute semirandom k-LIN instances over a finite field $\mathbb{F}$. As our main results, we give both an algorithm and a matching sum-of-squares lower bound with the "correct" dependence on the field size $|\mathbb{F}|$. Our algorithm is a generalization of [GKM22], and our lower bound is a generalization of [Gri01, Sch08, KMOW17].

Before stating our main results, we formally define semirandom k-LIN instances.

Definition 1.1 ((Semirandom) k-LIN)**.** An instance of k-LIN($\mathbb{F}$) is $\mathcal{I} = (\mathcal{H}, \{b_v\}_{v\in\mathcal{H}})$, where $\mathcal{H}$ is a set of k-sparse vectors[1] in $\mathbb{F}^n$ and $b_v \in \mathbb{F}$ for all $v \in \mathcal{H}$. We view $\mathcal{I}$ as representing the system of linear equations with variables $x_1, \dots, x_n$ specified by $\langle v, x\rangle = b_v$ for each $v \in \mathcal{H}$. The value of the instance, which we denote by $\mathrm{val}(\mathcal{I})$, is the maximum over $x \in \mathbb{F}^n$ of the fraction of constraints satisfied by x. That is, $\mathrm{val}(\mathcal{I}) = \max_{x\in\mathbb{F}^n} \frac{1}{|\mathcal{H}|} \sum_{v\in\mathcal{H}} \mathbf{1}(\langle x, v\rangle = b_v)$.

An instance of k-LIN is *random* if $\mathcal{H}$ is a random subset of k-sparse vectors and each b_v is drawn independently and uniformly from $\mathbb{F}$.

An instance of k-LIN is *semirandom* if each b_v is drawn independently and uniformly from $\mathbb{F}$ (but $\mathcal{H}$ may be arbitrary).

The first main result of this paper gives a refutation algorithm for semirandom k-LIN over any field $\mathbb{F}$.

Theorem 1.2 (Tight refutation of semirandom k-LIN($\mathbb{F}$))**.** *Fix $\ell \geq k/2$. There is an algorithm that takes as input a k-LIN($\mathbb{F}$) instance $\mathcal{I} = (\mathcal{H}, \{b_v\}_{v\in\mathcal{H}}$ in n variables and outputs a number* $\text{alg-val}(\mathcal{I}) \in [0, 1]$ *in time $(|\mathbb{F}|n)^{O(\ell)}$ with the following two guarantees:*

1. $\text{alg-val}(\mathcal{I}) \geq \mathrm{val}(\mathcal{I})$ *for every instance $\mathcal{I}$;*

[1] A vector $v \in \mathbb{F}^n$ is k-sparse if $|\{i : v_i \neq 0\}| = k$.

2. *If $|\mathcal{H}| \geq \Omega(n) \cdot \log(|\mathbb{F}^*|n) \left(\frac{n|\mathbb{F}^*|}{\ell}\right)^{k/2-1} \cdot \varepsilon^{-4}$ and $\mathcal{I}$ is drawn from the semirandom distribution described in Definition 1.1, then with probability $\geq 1 - \frac{1}{\mathrm{poly}(n)}$ over the draw of the semirandom instance, i.e., the randomness of $\{b_v\}_{v \in \mathcal{H}}$, it holds that $\text{alg-val}(\mathcal{I}) \leq \frac{1}{|\mathbb{F}|} + \varepsilon$.*

As a byproduct of the analysis of Theorem 1.2, we also establish an extremal combinatorics statement on the existence of short linear dependencies in any sufficiently dense collection of k-sparse vectors $\mathcal{H}$ over a finite field $\mathbb{F}$.

Theorem 1.3 (Short linear dependencies in k-sparse vectors over $\mathbb{F}$). *Let $\mathcal{H}$ be a set of $|\mathcal{H}| \geq \Omega(n) \cdot \log(|\mathbb{F}^*|n) \left(\frac{n|\mathbb{F}^*|}{\ell}\right)^{k/2-1}$ k-sparse vectors in $\mathbb{F}^n$. Then, there exists a set $\mathcal{V} \subseteq \mathcal{H}$ with $|\mathcal{V}| \leq \ell \log|\mathbb{F}^*|n$ and nonzero coefficients $\{\alpha_v\}_{v \in \mathcal{V}}$ in $\mathbb{F}^*$ such that:*

$$\sum_{v \in \mathcal{V}} \alpha_v \cdot v = 0\,.$$

That is, $\mathcal{V}$ is a linearly dependent subset of $\mathcal{H}$.

Theorem 1.3 is a generalization of the hypergraph Moore bound, or Feige's conjecture on the existence of short even covers in hypergraphs (first proven in [GKM22]) to arbitrary finite fields. The hypergraph Moore bound establishes (see [NV08]) a rate vs. distance trade-off for binary LDPC codes. One can similarly view Theorem 1.3 as establishing such a trade-off for LDPC codes over larger fields.

The key technical innovation in our proofs of Theorems 1.2 and 1.3 is the introduction of a new Kikuchi matrix for any finite field $\mathbb{F}$ (Definition 3.2). Our Kikuchi matrices can be seen as a generalization of the Kikuchi matrices of [WAM19, GKM22] specific to $\mathbb{F}_2$ to other fields and Abelian groups.

In our second main result, we prove a sum-of-squares lower bound for refuting k-LIN instances that nearly matches the threshold in Theorem 1.2.

Theorem 1.4 (Sum-of-squares lower bounds for refuting random k-LIN, informal). *Fix $\frac{n}{\max(|\mathbb{F}^*|,k)} \geq \ell \geq k$. Let $\mathcal{I}$ be a random k-LIN($\mathbb{F}$) instance $|\mathcal{H}| \leq O(n) \cdot \left(\frac{n|\mathbb{F}^*|}{\ell}\right)^{k/2-1} \cdot \varepsilon^{-2}$. Then, with high probability over the draw of $\mathcal{I}$, it holds that*

1. *$\mathrm{val}(\mathcal{I}) \leq \frac{1}{|\mathbb{F}|} + \varepsilon$.*

2. *The canonical degree-$\tilde{O}(\ell)$ sum-of-squares relaxation for k-LIN($\mathbb{F}$) fails to refute $\mathcal{I}$.*

2 Preliminaries

2.1 Basic notation

We let $[n]$ denote the set $\{1, \ldots, n\}$. For two subsets $S, T \subseteq [n]$, we let $S \oplus T$ denote the symmetric difference of S and T, i.e., $S \oplus T := \{i : (i \in S \wedge i \notin T) \vee (i \notin S \wedge i \in T)\}$. For a natural number $t \in \mathbb{N}$, we let $\binom{[n]}{t}$ be the collection of subsets of $[n]$ of size exactly t.

For a rectangular matrix $A \in \mathbb{C}^{m \times n}$, we let $\|A\|_2 := \max_{x \in \mathbb{C}^m, y \in \mathbb{C}^n : \|x\|_2 = \|y\|_2 = 1} x^\dagger A y$ denote the spectral norm of A.

For a vector $v \in \mathbb{F}^n$, we let $\mathrm{supp}(v) := \{i : v_i \neq 0\}$ and $\mathrm{wt}(v) := |\mathrm{supp}(v)|$. For a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) = p$, we let $\mathrm{Tr}(\cdot)$ denote the trace map of $\mathbb{F}$ over $\mathbb{F}_p$.

For a matrix $A \in \mathbb{C}^{n \times n}$, we let $\mathrm{tr}(A)$ be the trace of A, i.e., $\sum_{i=1}^n A_{i,i}$. This should not be confused with the trace map for field elements, which we denote by $\mathrm{Tr}(\cdot)$. For two vectors $x, y \in \mathbb{C}^n$ we define the following inner product:

$$\langle x, y \rangle = x^\dagger y = \sum_{i=1}^{n} \overline{x_i} \cdot y_i \,.$$

2.2 Fourier Analysis

Let G be an Abelian group isomorphic to $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ via the isomorphism ψ. For $m \in \mathbb{N}$, we let $\omega_m := e^{\frac{2\pi i}{m}}$. For $\alpha, x \in G$, we define

$$\chi_\alpha(x) = \prod_{i=1}^{r} \omega_{m_i}^{\psi(\alpha)_i \psi(x)_i} \,.$$

These functions form a Fourier basis for G, as shown in [O'D14]. This extends to a Fourier basis for G^n as follows. For $v, x \in G^n$, we define

$$\chi_v(x) = \prod_{i=1}^{n} \chi_{v_i}(x_i) \,.$$

For a function $f\colon G^n \to \mathbb{C}$, we have that for each $x \in G^n$,

$$f(x) = \sum_{v \in G^n} \hat{f}(v) \cdot \chi_v(x) \,,$$

where $\hat{f}(v) = \mathbb{E}_{x \in G^n}\left[f(x) \cdot \overline{\chi_v(x)} \right]$.

For the special case of functions $f\colon \mathbb{F}^n \to \mathbb{C}$ with $\mathrm{char}(\mathbb{F}) = p$, we note that the standard Fourier basis is simply

$$\chi_v(x) = \omega_p^{\mathrm{Tr}(\langle v, x \rangle)} \,.$$

2.3 Binomial coefficient inequalities

In this section, we state and prove the following fact about binomial coefficients that we will use.

Fact 2.1. *Let n, ℓ, q be positive integers with $\ell \leq n$. Let q be constant and ℓ, n be asymptotically large with $\ell \leq n/2$. Then,*

$$\frac{\binom{n}{\ell - q}}{\binom{n}{\ell}} = \Theta\left(\left(\frac{\ell}{n} \right)^q \right) ,$$

$$\frac{\binom{n-q}{\ell}}{\binom{n}{\ell}} = \Theta(1) \,.$$

Proof. We have that

$$\frac{\binom{n}{\ell-q}}{\binom{n}{\ell}} = \frac{\binom{\ell}{q}}{\binom{n-\ell+q}{q}}\,.$$

Using that $\left(\frac{a}{b}\right)^b \leq \binom{a}{b} \leq \left(\frac{ea}{b}\right)^b$ finishes the proof of the first equation.

We also have that

$$\frac{\binom{n-q}{\ell}}{\binom{n}{\ell}} = \frac{(n-q)!(n-\ell)!}{n!(n-\ell-q)!} = \prod_{i=0}^{q-1} \frac{n-\ell-i}{n-i} = \prod_{i=0}^{q-1} \left(1 - \frac{\ell}{n-i}\right)\,,$$

and this is $\Theta(1)$ since $\ell \leq n/2$ and q is constant. □

3 Proof of Theorem 1.2 for even k

In this section, we prove Theorem 1.2 in the case when k is even. As in [GKM22, HKM23], the proof is substantially simpler in the case of even k, so this section can also be viewed as a warmup to the proof for odd k.

Our refutation algorithm for semirandom k-LIN follows the framework established in [GKM22, HKM23]. The main technical tool we use is a generalization of the Kikuchi matrix of [WAM19] for $\mathbb{F}_2$ to arbitrary finite fields $\mathbb{F}$.

As the first step in the proof, we make the following observation. Throughout fix $\mathrm{char}(\mathbb{F}) = p$.

Observation 3.1. For a k-LIN($\mathbb{F}$) instance $\mathcal{I} = (\mathcal{H}, \{b_v\}_{v\in\mathcal{H}})$, let $\mathrm{val}(\mathcal{I}, x)$ denote the fraction of constraints satisfied by an assignment $x \in \mathbb{F}^n$. Then, we have

$$\mathrm{val}(\mathcal{I}, x) = \frac{1}{|\mathbb{F}|} + \frac{1}{|\mathcal{H}||\mathbb{F}|} \sum_{v\in\mathcal{H}} \sum_{\beta\in\mathbb{F}^*} \omega_p^{\mathrm{Tr}(\beta b_v)} \cdot \overline{\chi_{\beta v}(x)} = \frac{1}{|\mathbb{F}|} + \Phi(x)\,,$$

where

$$\Phi(x) = \frac{1}{|\mathcal{H}||\mathbb{F}|} \sum_{v\in\mathcal{H}} \sum_{\beta\in\mathbb{F}^*} \omega_p^{\mathrm{Tr}(\beta b_v)} \cdot \overline{\chi_{\beta v}(x)}\,.$$

Proof. Recall that a constraint in $\mathcal{I}$ takes the form $\langle v, x\rangle = b_v$ for $v \in \mathcal{H}$, where $x \in \mathbb{F}^n$ are the variables. The indicator variable for this event is simply:

$$\mathbf{1}(\langle v, x\rangle = b_v) = \mathbb{E}_{\beta\sim\mathbb{F}}\left[\omega_p^{\mathrm{Tr}(\beta b_v - \beta\langle v, x\rangle)}\right] = \frac{1}{|\mathbb{F}|} \sum_{\beta\in\mathbb{F}} \omega_p^{\mathrm{Tr}(\beta b_v)} \cdot \overline{\chi_{\beta v}(x)}\,.$$

where $p = \mathrm{char}(\mathbb{F})$. Indeed, if $\langle v, x\rangle = b_v$, then $\mathrm{Tr}(\beta b_v - \beta\langle v, x\rangle) = 0$ for all $\beta \in \mathbb{F}$. If $b_v - \langle v, x\rangle \neq 0$, i.e., it is some $\alpha \in \mathbb{F}^*$, then $\mathbb{E}_{\beta\in\mathbb{F}}\left[\omega_p^{\mathrm{Tr}(\beta\alpha)}\right] = \mathbb{E}_{\beta\in\mathbb{F}}\left[\omega_p^{\mathrm{Tr}(\beta)}\right] = 0$. Hence, it follows that

$$\mathrm{val}(\mathcal{I}, x) = \frac{1}{|\mathcal{H}|} \sum_{v\in\mathcal{H}} \mathbf{1}(\langle v, x\rangle = b_v) = \frac{1}{|\mathcal{H}|} \sum_{v\in\mathcal{H}} \frac{1}{|\mathbb{F}|} \sum_{\beta\in\mathbb{F}} \omega_p^{\mathrm{Tr}(\beta b_v)} \cdot \overline{\chi_{\beta v}(x)}$$

$$= \frac{1}{|\mathbb{F}|} + \frac{1}{|\mathcal{H}||\mathbb{F}|} \sum_{v \in \mathcal{H}} \sum_{\beta \in \mathbb{F}^*} \omega_p^{\mathrm{Tr}(\beta b_v)} \cdot \overline{\chi_{\beta v}(x)},$$

which finishes the proof. □

In light of Observation 3.1, it thus remains to find a certificate that bounds $\max_{x \in \mathbb{F}^n} \Phi(x)$. Following [GKM22], we do this by constructing a Kikuchi matrix whose spectral norm provides a certificate bounding the maximum value of Φ.

Definition 3.2. (Even-arity Kikuchi matrix over $\mathbb{F}$). Let $k/2 \le \ell \le n/2$ be a parameter,[2] and let $N = |\mathbb{F}^*|^\ell \binom{n}{\ell}$. For each k-sparse vector $v \in \mathbb{F}^n$ and $\beta \in \mathbb{F}^*$, we define a matrix $A_{v,\beta} \in \mathbb{C}^{N \times N}$ as follows. First, we identify N with the set of ℓ-sparse vectors in $\mathbb{F}^n$. Then, for ℓ-sparse vectors $U, V \in \mathbb{F}^n$, we let

$$A_{v,\beta}(U,V) = \begin{cases} 1 & U \xrightarrow{v,\beta} V \\ 0 & \text{otherwise} \end{cases}$$

where we say $U \xrightarrow{v,\beta} V$ if $U - V = \beta v$ and $\mathrm{supp}(U) \oplus \mathrm{supp}(V) = \mathrm{supp}(v)$.

Let $\Phi(x) = \frac{1}{|\mathbb{F}||\mathcal{H}|} \sum_{v \in \mathcal{H}} \sum_{\beta \in \mathbb{F}^*} c_{v,\beta} \cdot \chi_{\beta v}$ be a polynomial defined by a set $\mathcal{H}$ of k-sparse vectors from $\mathbb{F}^n$ and complex coefficients $\{c_{v,\beta}\}_{\substack{v \in \mathcal{H} \\ \beta \in \mathbb{F}^*}}$. We define the level-$\ell$ Kikuchi matrix for this polynomial to be $A = \sum_{v \in \mathcal{H}} \sum_{\beta \in \mathbb{F}^*} c_{v,\beta} \cdot A_{v,\beta}$. We refer to the graph (with complex weights) defined by the underlying adjacency matrix as the Kikuchi graph.

Remark 3.3. We note that in the above definition, we have $A_{v,\beta} = A_{\beta v, 1}$. The reason we use the above definition with two parameters v and β is that it will be more convenient when counting walks in the matrix A, as it makes explicit the choice of v and β. Note that in $\mathcal{H}$, there could exist v and v' with $\beta v = v'$ for some $\beta \in \mathbb{F}^*$.

Observation 3.4. The Kikuchi matrix A is always Hermitian.

Proof. To see this note that $U - V = \beta v \iff V - U = -\beta v$, $\overline{\chi_\beta} = \chi_{-\beta}$, and $\oplus$ is commutative. □

The following observation shows that we can express $\Phi(x)$ as a quadratic form on the matrix A defined in Definition 3.2.

Observation 3.5. For $x \in \mathbb{F}^n$ define $y \in \mathbb{C}^N$ as follows. For each ℓ-sparse $U \in \mathbb{F}^n$, we set $y_U = \overline{\chi_U(x)}$. Then:

$$\Phi(x) = \frac{1}{|\mathcal{H}||\mathbb{F}|\Delta} y^\dagger A y,$$

where $\Delta := \binom{k}{k/2}\binom{n-k}{\ell - k/2} |\mathbb{F}^*|^{\ell - k/2}$.

Proof.

$$y^\dagger A y = \sum_{\substack{U,V \in \mathbb{F}^n \\ \mathrm{wt}(U) = \mathrm{wt}(V) = \ell}} A(U,V) \cdot \chi_U(x) \cdot \overline{\chi_V(x)}$$

[2] Note that it suffices to prove Theorem 1.2 for ℓ in this range

$$
\begin{aligned}
&= \sum_{\substack{U,V\in\mathbb{F}^n \\ \mathrm{wt}(U)=\mathrm{wt}(U)=\ell}} \mathbf{1}\left(U \xrightarrow{v,\beta} V\right) \cdot c_{v,\beta} \cdot \chi_U(x) \cdot \overline{\chi_V(x)} \\
&= \sum_{\substack{U,V\in\mathbb{F}^n \\ \mathrm{wt}(U)=\mathrm{wt}(U)=\ell}} \mathbf{1}\left(U \xrightarrow{v,\beta} V\right) \cdot c_{v,\beta} \cdot \chi_{U-V}(x) \\
&= \sum_{\substack{U,V\in\mathbb{F}^n \\ \mathrm{wt}(U)=\mathrm{wt}(U)=\ell}} \mathbf{1}\left(U \xrightarrow{v,\beta} V\right) \cdot c_{v,\beta} \cdot \chi_{\beta v}(x)\,.
\end{aligned}
$$

For each $v \in \mathcal{H}$ and $\beta \in \mathbb{F}^*$, the term $c_{v,\beta} \cdot \chi_{\beta v}(x)$ appears once for each pair of vertices (U, V) with $U \xrightarrow{v,\beta} V$. Let us now argue that the number of such pairs (U, V) is exactly $\Delta = \binom{k}{k/2}\binom{n-k}{\ell-k/2}|\mathbb{F}^*|^{\ell-k/2}$. We will count the number of pairs (U, V) by first specifying $\mathrm{supp}(U)$ and $\mathrm{supp}(V)$, and then by specifying U_i for each $i \in \mathrm{supp}(U)$ (and same for V). We first require that $\mathrm{supp}(U) \oplus \mathrm{supp}(V) = \mathrm{supp}(v)$, which in turn means that $\mathrm{supp}(U)$ has intersection exactly $k/2$ with $\mathrm{supp}(v)$ and likewise for $\mathrm{supp}(V)$. Thus, we can pay $\binom{k}{k/2}$ to count the number of ways to split $\mathrm{supp}(v)$ into two equal parts. Second, we need to specify $\mathrm{supp}(U) \setminus \mathrm{supp}(v)$, which is equal to $\mathrm{supp}(V) \setminus \mathrm{supp}(v)$, which is $\binom{n-k}{\ell-k/2}$ choices. Finally, we need to specify U_i for each $i \in \mathrm{supp}(U)$ and V_i for each $i \in \mathrm{supp}(V)$. For each $i \in \mathrm{supp}(U) \cap \mathrm{supp}(v)$, we set $U_i = (\beta v)_i$, and for each $i \in \mathrm{supp}(U) \setminus \mathrm{supp}(v)$, we can set U_i to be any element in $\mathbb{F}^*$. Note that specifying U then determines V, so we have $|\mathbb{F}^*|^{\ell-k/2}$ choices. This finishes the proof. □

Next, we compute the average degree (or number of nonzero entries) in a row/column in A.

Observation 3.6. For $U \in \mathbb{F}^n$ with $\mathrm{wt}(U) = \ell$ we define the graph degree as normal:

$$
\deg(U) := |\{\beta v \mid \beta \in \mathbb{F}^*, v \in \mathcal{H} \text{ s.t. } \exists V \in \mathbb{F}^n, \mathrm{wt}(V) = \ell, U \xrightarrow{v,\beta} V\}|.
$$

Then $\mathbb{E}[\deg(U)] \geq \frac{|\mathbb{F}^*|}{2}\left(\frac{\ell}{|\mathbb{F}^*|n}\right)^{k/2} \cdot |\mathcal{H}|$.

Proof. Each $v \in \mathcal{H}$ contributes $|\mathbb{F}^*|\Delta$ to the total degree, so the average degree is $\mathbb{E}[\deg(S)] = \frac{|\mathcal{H}||\mathbb{F}^*|\Delta}{N}$. We then have:

$$
\mathbb{E}[\deg(S)] = \frac{|\mathbb{F}^*|\Delta}{N} \cdot |\mathcal{H}| = \frac{|\mathbb{F}^*|^{\ell-k/2+1}\binom{k}{k/2}\binom{n-k}{\ell-k/2}}{|\mathbb{F}^*|^{\ell}\binom{n}{\ell}} \cdot |\mathcal{H}| \geq \frac{|\mathbb{F}^*|}{2}\left(\frac{\ell}{|\mathbb{F}^*|n}\right)^{k/2} \cdot |\mathcal{H}|\,,
$$

where the last inequality follows from Fact 2.1. □

The following spectral norm bound immediately implies Theorem 1.2.

Lemma 3.7. *Let A be the level-ℓ Kikuchi matrix over $\mathbb{F}^n$ defined in Definition 3.2 for the k-*LIN *instance $\mathcal{I} = (\mathcal{H}, \{b_v\}_{v\in\mathcal{H}})$. Let $\Gamma \in \mathbb{C}^{N\times N}$ be the diagonal matrix $\Gamma = D + d\mathbb{I}$ where $D_{U,U} := \deg(U)$ and $d = \mathbb{E}[\deg(U)]$. Suppose that the b_v's are drawn independently and uniformly from $\mathbb{F}$, i.e., the instance $\mathcal{I}$ is* semirandom *(Definition 1.1). Then, with probability $\geq 1 - \frac{1}{\mathrm{poly}(n)}$, it holds that*

$$
\|\Gamma^{-1/2}A\Gamma^{-1/2}\|_2 \leq O\left(\sqrt{\frac{\ell \log|\mathbb{F}^*|n}{d}}\right).
$$

We postpone the proof of Lemma 3.7 to the end of this section, and now finish the proof the proof of Theorem 1.2.

Proof of Theorem 1.2 from Lemma 3.7. Let $\mathcal{I} = (\mathcal{H}, \{b_v\}_{v\in\mathcal{H}})$ be the input to the algorithm. Given ℓ, the algorithm constructs the matrix A and computes $\text{alg-val}(\mathcal{I}) = \frac{1}{|\mathbb{F}|} + \frac{2|\mathbb{F}^*|}{|\mathbb{F}|}\|\tilde{A}\|_2$, where $\tilde{A} = \Gamma^{-1/2}A\Gamma^{-1/2}$. It remains to argue that this quantity has the desired properties.

Let $\Phi(x)$ be the polynomial defined in Observation 3.1. For each $x \in \mathbb{F}^n$, letting $y \in \mathbb{C}^n$ be the vector defined in Observation 3.5, we have

$$\Phi(x) = \frac{1}{|\mathbb{F}||\mathcal{H}|\Delta} \cdot y^\dagger A y = \frac{1}{|\mathbb{F}||\mathcal{H}|\Delta} \cdot (\Gamma^{1/2}y)^\dagger \tilde{A}(\Gamma^{1/2}y) \leq \frac{1}{|\mathbb{F}||\mathcal{H}|\Delta} \cdot \|\tilde{A}\|_2 \|\Gamma^{1/2}y\|_2^2$$
$$= \frac{1}{|\mathbb{F}||\mathcal{H}|\Delta} \cdot \|\tilde{A}\|_2 \cdot \mathrm{tr}(\Gamma) = \frac{2|\mathbb{F}^*|}{|\mathbb{F}|}\|\tilde{A}\|_2 \,,$$

where we use that $\|\Gamma^{1/2}y\|_2^2 = y^\dagger \Gamma y = \sum_U \Gamma_U |y_U|^2 = \sum_U \Gamma_U = \mathrm{tr}(\Gamma)$ since $|y_U| = 1$ for all U, and that $\mathrm{tr}(\Gamma) = 2|\mathcal{H}||\mathbb{F}^*|\Delta$. Hence,

$$\mathrm{val}(\mathcal{I}) = \frac{1}{|\mathbb{F}|} + \max_{x\in\mathbb{F}^n} \Phi(x) \leq \frac{1}{|\mathbb{F}|} + \frac{2|\mathbb{F}^*|}{|\mathbb{F}|}\|\tilde{A}\|_2 \,,$$

which proves Item (1) in Theorem 1.2.

To prove Item (2), we observe that by Lemma 3.7, if $\mathcal{I}$ is semirandom, then with high probability over the draw of the b_v's, it holds that

$$\|\tilde{A}\|_2 \leq O\left(\sqrt{\frac{\ell \log(|\mathbb{F}^*|n)}{d}}\right) .$$

From Observation 3.6, we have $d \geq \frac{|\mathbb{F}^*|}{2}\left(\frac{\ell}{|\mathbb{F}^*|n}\right)^{k/2} \cdot |\mathcal{H}|$. Hence, if $|\mathcal{H}| \geq Cn\log(|\mathbb{F}^*|n)\left(\frac{|\mathbb{F}^*|n}{\ell}\right)^{k/2-1}\varepsilon^{-2}$ for a sufficiently large constant C, then $\|\tilde{A}\|_2 \leq \varepsilon$ with probability $1 - 1/\mathrm{poly}(n)$. This proves Item (2). □

Proof of Lemma 3.7. By Observation 3.4, we have that $\|\tilde{A}\|_2 \leq \mathrm{tr}((\Gamma^{-1}A)^{2t})^{1/2t}$ for any positive integer t (see Appendix A). Because the b_v's are drawn independently from $\mathbb{F}$, the matrix $\tilde{A}$ is a random matrix. By Markov's inequality,

$$\Pr\left[\mathrm{tr}((\Gamma^{-1}A)^{2t}) \geq N \cdot \mathbb{E}[\mathrm{tr}((\Gamma^{-1}A)^{2t})]\right] \leq \frac{1}{N} .$$

We note this event is the same as $\mathrm{tr}((\Gamma^{-1}A)^{2t})^{1/2t} \geq N^{1/2t} \cdot \mathbb{E}[\mathrm{tr}((\Gamma^{-1}A)^{2t})]^{1/2t}$, and for $2t \geq \log N$ we have $N^{1/2t} \leq O(1)$. This immediately gives us that with probability $\geq 1 - \frac{1}{N}$, $\|\tilde{A}\|_2 \leq O\left(\mathbb{E}[\mathrm{tr}((\Gamma^{-1}A)^{2t})]^{1/2t}\right)$. We then have that

$$\mathbb{E}[\mathrm{tr}((\Gamma^{-1}A)^{2t})] = \mathbb{E}\left[\mathrm{tr}\left(\left(\Gamma^{-1}\sum_{v\in\mathcal{H},\beta\in\mathbb{F}^*} c_{v,\beta}\cdot A_{v,\beta}\right)^{2t}\right)\right]$$

$$= \mathbb{E}\left[\operatorname{tr}\left(\sum_{(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\in\mathcal{H}\times\mathbb{F}^*}\prod_{i=1}^{2t}\Gamma^{-1}\cdot c_{v_i,\beta_i}\cdot A_{v_i,\beta_i}\right)\right]$$

$$= \sum_{(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\in\mathcal{H}\times\mathbb{F}^*}\mathbb{E}\left[\operatorname{tr}\left(\prod_{i=1}^{2t}\Gamma^{-1}\cdot c_{v_i,\beta_i}\cdot A_{v_i,\beta_i}\right)\right]$$

$$= \sum_{(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\in\mathcal{H}\times\mathbb{F}^*}\mathbb{E}\left[\prod_{i=1}^{2t} c_{v_i,\beta_i}\right]\cdot\operatorname{tr}\left(\prod_{i=1}^{2t}\Gamma^{-1}A_{v_i,\beta_i}\right).$$

Let us now make the following observation. Let $(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\in\mathcal{H}\times\mathbb{F}^*$ be a term in the above sum. Fix $v\in\mathcal{H}$, and let $R(v)$ denote the set of $i\in[2t]$ such that $v_i=v$. We observe that if for some $v\in\mathcal{H}$, $\sum_{i\in R(v)}\beta_i\neq 0$, then $\mathbb{E}\left[\prod_{i=1}^{2t}c_{v_i,\beta_i}\right]=0$. Indeed, this is because b_v is independent for each $v\in\mathcal{H}$, and so $\mathbb{E}\left[\prod_{i=1}^{2t}c_{v_i,\beta_i}\right]=\prod_{v\in\mathcal{H}}\mathbb{E}\left[\prod_{i\in R(v)}c_{v,\beta_i}\right]$, and

$$\mathbb{E}\left[\prod_{i\in R(v)}c_{v,\beta_i}\right]=\mathbb{E}\left[\prod_{i\in R(v)}\omega_p^{\operatorname{Tr}(\beta_i b_v)}\right]=\mathbb{E}\left[\omega_p^{\operatorname{Tr}((\sum_{i\in R(v)}\beta_i)b_v)}\right].$$

Then, since b_v is uniform from $\mathbb{F}$, it follows that $\mathbb{E}\left[\omega_p^{\operatorname{Tr}((\sum_{i\in R(v)}\beta_i)b_v)}\right]=0$ if $\sum_{i\in R(v)}\beta_i\neq 0$, and $\mathbb{E}\left[\omega_p^{\operatorname{Tr}((\sum_{i\in R(v)}\beta_i)b_v)}\right]=1$ if $\sum_{i\in R(v)}\beta_i=0$. This motivates the following definition.

Definition 3.8 (Trivially closed sequence)**.** Let $(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\in\mathcal{H}\times\mathbb{F}^*$. We say that $(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\in\mathcal{H}\times\mathbb{F}^*$ is trivially closed with respect to v if it holds that $\sum_{i\in R(v)}\beta_i=0$. We say that the sequence is trivially closed if it is trivially closed with respect to all $v\in\mathcal{H}$.

With the above definition in hand, we have shown that

$$\mathbb{E}[\operatorname{tr}((\Gamma^{-1}A)^{2t})]=\sum_{\substack{(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\\ \text{trivially closed}}}\operatorname{tr}\left(\prod_{i=1}^{2t}\Gamma^{-1}A_{v_i,\beta_i}\right).$$

The following lemma yields the desired bound on $\mathbb{E}[\operatorname{tr}((\Gamma^{-1}A)^{2t})]$.

Lemma 3.9. $\sum_{\substack{(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})\\ \textit{trivially closed}}}\operatorname{tr}\left(\prod_{i=1}^{2t}\Gamma^{-1}A_{v_i,\beta_i}\right)\leq N\cdot 2^{2t}\cdot\left(\frac{2t}{d}\right)^t$.

With Lemma 3.9, we thus have the desired bound $\mathbb{E}[\operatorname{tr}((\Gamma^{-1}A)^{2t})]$. Taking t to be $c\log_2 N$ for a sufficiently large constant c and applying Markov's inequality finishes the proof. □

Proof of Lemma 3.9. We bound the sum as follows. First, we observe that for a trivially closed sequence $(v_1,\beta_1),\ldots,(v_{2t},\beta_{2t})$, we have

$$\operatorname{tr}\left(\prod_{i=1}^{2t}\Gamma^{-1}A_{v_i,\beta_i}\right)=\sum_{U_0,U_1,\ldots,U_{2t-1}}\prod_{i=0}^{2t-1}\Gamma_{U_i}^{-1}\cdot\mathbf{1}\left(U_i\xrightarrow{v_{i+1},\beta_{i+1}}U_{i+1}\right),$$

where we define $U_{2t} = U_0$. Thus, the sum that we wish to bound in Lemma 3.9 simply counts the total weight of "trivially closed walks" $U_0, v_1, \beta_1, U_1, \dots, U_{2t-1}, v_{2t}, \beta_{2t}, U_{2t}$ (where $U_{2t} = U_0$) in the Kikuchi graph A, where the weight of a walk is simply $\prod_{i=0}^{2t-1} \Gamma_{U_i}^{-1}$.

Let us now bound this total weight by uniquely encoding a walk $U_0, v_1, \beta_1, U_1, \dots, U_{2t-1}, v_{2t}, \beta_{2t}, U_{2t}$ as follows.

- First, we write down the start vertex U_0.
- For $i = 1, \dots, 2t$, we let z_i be 1 if $v_i = v_j$ for some $j < i$. In this case, we say that the edge is "old". Otherwise $z_i = 0$, and we say that the edge is "new".
- For $i = 1, \dots, 2t$, if z_i is 1 then we encode U_i by writing down the smallest $j \in [2t]$ such that $v_i = v_j$. We note that we *do not* need to specify the element β_i, as for any vertex U, there is at most one V and one $\beta \in \mathbb{F}^*$ such that $\mathbf{1}\left(U \xrightarrow{v_i, \beta} V\right)$.
- For $i = 1, \dots, 2t$, if z_i is 0 then we encode U_i by writing down an integer in $1, \dots, \deg(U_{i-1})$ that specifies the edge we take to move to U_i from U_{i-1} (we associate $[\deg(U_{i-1})]$ to the edges adjacent to U_{i-1} with an arbitrary fixed map).

With the above encoding, we can now bound the total weight of all trivially closed walks as follows. First, let us consider the total weight of walks for some fixed choice of $z_1, \dots, z_{2t}$. We have N choices for the start vertex U_0. For each $i = 1, \dots, 2t$ where $z_i = 0$, we have $\deg(U_{i-1})$ choices for U_i, and we multiply by a weight of $\Gamma_{U_{i-1}}^{-1} \leq \frac{1}{\deg(U_{i-1})}$. For each $i = 1, \dots, 2t$ where $z_i = 1$, we have at most $2t$ choices for the index $j < i$, and we multiply by a weight of $\Gamma_{U_{i-1}}^{-1} \leq \frac{1}{d}$. Hence, the total weight for a specific $z_1, \dots, z_{2t}$ is at most $N\left(\frac{2t}{d}\right)^r$, where r is the number of z_i such that $z_i = 1$.

Finally, we observe that any trivially closed walk must have $r \geq t$. Hence, after summing over all $z_1, \dots, z_{2t}$, we have the final bound of $N 2^{2t} \left(\frac{2t}{d}\right)^t$, which finishes the proof. $\square$

References

[AG24] Omar Alrabiah and Venkatesan Guruswami. Near-tight bounds for 3-query locally correctable binary linear codes via rainbow cycles. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*. IEEE, 2024.

[AGK21] Jackson Abascal, Venkatesan Guruswami, and Pravesh K. Kothari. Strongly refuting all semi-random Boolean CSPs. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021*, pages 454–472. SIAM, 2021.

[AGKM23] Omar Alrabiah, Venkatesan Guruswami, Pravesh K. Kothari, and Peter Manohar. A near-cubic lower bound for 3-query locally decodable codes from semirandom CSP refutation. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1438–1448. ACM, 2023.

[AOW15] Sarah R. Allen, Ryan O'Donnell, and David Witmer. How to Refute a Random CSP. In *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 689–708. IEEE Computer Society, 2015.

[BCK15] Boaz Barak, Siu On Chan, and Pravesh K. Kothari. Sum of Squares Lower Bounds from Pairwise Independence. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 97–106. ACM, 2015.

[BGMT12] Siavosh Benabbas, Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. SDP gaps from pairwise independence. *Theory of Computing*, 8(1):269–289, 2012.

[BHKL24] Arpon Basu, Jun-Ting Hsieh, Pravesh Kothari, and Andrew Lin. Improved lower bounds for all odd-query locally decodable codes. *Electron. Colloquium Comput. Complex.*, pages TR24–189, 2024.

[BM16] Boaz Barak and Ankur Moitra. Noisy Tensor Completion via the Sum-of-Squares Hierarchy. In *Proceedings of the 29th Conference on Learning Theory, COLT 2016, New York, USA, June 23-26, 2016*, volume 49 of *JMLR Workshop and Conference Proceedings*, pages 417–445. JMLR.org, 2016.

[CGL07] Amin Coja-Oghlan, Andreas Goerdt, and André Lanka. Strong refutation heuristics for random k-SAT. *Combinatorics, Probability & Computing*, 16(1):5, 2007.

[Fei02] Uriel Feige. Relations between average case complexity and approximation complexity. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 534–543, 2002.

[GKM22] Venkatesan Guruswami, Pravesh K. Kothari, and Peter Manohar. Algorithms and certificates for Boolean CSP refutation: smoothed is no harder than random. In *STOC*

'22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 678–689. ACM, 2022.

[GL03] Andreas Goerdt and André Lanka. Recognizing more random unsatisfiable 3-sat instances efficiently. *Electron. Notes Discret. Math.*, 16:21–46, 2003.

[Gri01] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1):613–622, 2001.

[HKM23] Jun-Ting Hsieh, Pravesh K. Kothari, and Sidhanth Mohanty. A simple and sharper proof of the hypergraph Moore bound. In *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 2324–2344. SIAM, 2023.

[JM24] Oliver Janzer and Peter Manohar. A $k^{\frac{q}{q-2}}$ lower bound for odd query locally decodable codes from bipartite kikuchi graphs. *Electron. Colloquium Comput. Complex.*, pages TR24–187, 2024.

[KM24a] Pravesh K. Kothari and Peter Manohar. An exponential lower bound for linear 3-query locally correctable codes. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 776–787. ACM, 2024.

[KM24b] Pravesh K. Kothari and Peter Manohar. Exponential lower bounds for smooth 3-lccs and sharp bounds for designs. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*. IEEE, 2024.

[KMOW17] Pravesh K. Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 132–145. ACM, 2017.

[MW16] Ryuhei Mori and David Witmer. Lower Bounds for CSP Refutation by SDP Hierarchies. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2016, September 7-9, 2016, Paris, France*, volume 60 of *LIPIcs*, pages 41:1–41:30, 2016.

[NV08] Assaf Naor and Jacques Verstraëte. Parity check matrices and product representations of squares. *Combinatorica*, 28(2):163–185, 2008.

[O'D14] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[OW14] Ryan O'Donnell and David Witmer. Goldreich's PRG: evidence for near-optimal polynomial stretch. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 1–12. IEEE, 2014.

[RRS17] Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random CSPs below the spectral threshold. In *Proceedings of the 49th Annual ACM SIGACT Symposium* *on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 121–131. ACM, 2017.

[Sch08] Grant Schoenebeck. Linear level lasserre lower bounds for certain k-csps. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 593–602. IEEE Computer Society, 2008.

[WAM19] Alexander S. Wein, Ahmed El Alaoui, and Cristopher Moore. The Kikuchi Hierarchy and Tensor PCA. In *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 1446–1468. IEEE Computer Society, 2019.

[Yan24] Tal Yankovitz. A stronger bound for linear 3-lcc. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*. IEEE, 2024.

A Complex trace moment method

Claim A.1. Let $A \in \mathbb{C}^{n\times n}$ be Hermitian. Then $\|A\|_2 \le \operatorname{tr}(A^{2t})^{1/2t}$.

Proof. Since A is Hermitian we have $A^2 = A^\dagger A$. Suppose $v \in \mathbb{C}^n$ is an eigenvector of A with eigencalue $\lambda \in \mathbb{C}$. Then $A^\dagger A v = \lambda(A^\dagger v) = \lambda\overline{\lambda} = |\lambda|^2$. It follows that the eigenvalues of A^{2t} are $|\lambda_1|^{2t}, \ldots, |\lambda_n|^{2t}$. Let $\lambda = \operatorname{argmax}_{i\in[n]}|\lambda_i|$. Since $\operatorname{tr}(A^{2t}) = \sum_{i=1}^n |\lambda_i|^{2t} \ge \lambda^{2t}$ and $\|A\|_2 = |\lambda|$ it follows that $\|A\|_2 \le \operatorname{tr}(A^{2t})^{1/2t}$.

Note since $\operatorname{tr}(A^{2t}) \le n|\lambda|^{2t}$ it follows that $\operatorname{tr}(A^{2t})^{1/2t} \le n^{1/2t} \cdot |\lambda|$, which when $t = \Omega(\log n)$ is nearly tight. ◻