A Family of Dictatorship Tests with Perfect Completeness for 2–to–2 Label Cover

Joshua Brakensiek* Venkatesan Guruswami†

Abstract

We give a family of dictatorship tests with perfect completeness and low-soundness for 2–to–2 constraints. The associated 2–to–2 conjecture has been the basis of some previous inapproximability results with perfect completeness. However, evidence towards the conjecture in the form of integrality gaps even against weak semidefinite programs has been elusive. Our result provides some indication of the expressiveness and non-triviality of 2–to–2 constraints, given the close connections between dictatorship tests and satisfiability and approximability of CSPs.

1 Introduction

In the study of constraint satisfaction problems and optimization, dictatorship tests are a surrogate for understanding the problems’ computational complexity. For a given optimization problem over a domain $D$, a dictatorship test for a function $f : D^n \rightarrow D$ is a randomized query whose distribution is based on the constraints from the optimization problem. For example, for NAE-3-SAT, $D = \{0, 1\}$, a query would pick uniformly at random three vectors $x, y, z \in \{0, 1\}^n$ such that $x_i \lor y_i \lor z_i = 1$ and $x_i \land y_i \land z_i = 0$ for all $i \in \{1, \ldots, n\}$ and then test whether $f(x) \lor f(y) \lor f(z) = 1$ and $f(x) \land f(y) \land f(z) = 0$. For a given function $f$, there is an associated probability $p \in [0, 1]$ for which it satisfies the dictatorship test. Typically some threshold $\tau > 0$ is assigned for which a function $f$ ‘passes’ the test if $p \geq \tau$. As their name suggests, these tests are usually designed so that certain dictator functions (also known as projections), functions which depend on only a single coordinate, pass with probability 1 (or $1 - \epsilon$, depending on the application).

For constraint satisfaction problems (CSPs), dictatorship tests with a passing probability of $\tau = 1$ have been used to understand the computational complexity of the associated satisfiability problems. In the universal algebraic approach to understanding CSPs, functions which pass such dictatorship tests are known as polymorphisms. (See [Che09] for an excellent survey on the algebraic study of CSPs.) For a long time (e.g., [BJK05]), it has been known that the computational complexity is completely characterized by which functions pass the dictatorship tests. The deep understanding of such connections has very recently culminated in two proofs of the Algebraic Dichotomy Conjecture [Bul17, Zhu17]. Although the exact statement of the conjecture is quite technical, at a moral level it says that a CSP has a polynomial time algorithm if and only if one is able to satisfy the canonical dictatorship test with arbitrarily complex polymorphisms. (Formally, such functions are known as “weak near unanimity” operators.)

In the context of optimization, where the goal is to satisfy as many constraints of the CSP as possible, one often seeks to prove that for some threshold $\tau \in (0, 1)$, if a function $f$ passes the dictatorship test...
with probability at least \( \tau \), then \( f \) essentially depends on a small number of coordinates. In this setting, a similar close connection between approximability and the passing of dictatorship tests is also known. In particular, Raghavendra [Rag08] showed that the threshold \( \tau \) for which dictatorship tests can be passed by highly non-dictatorial functions (those with no influential coordinates), is exactly the approximation ratio which can be found by the Basic SDP relaxation. Further, under Khot’s Unique Games Conjecture [Kho02], no polynomial time algorithm can deliver an approximation guarantee better than \( \tau \) [KKMO07].

The complexity of approximate optimization of every CSP is thus settled under the Unique Games Conjecture (UGC). The UGC itself asserts the inapproximability of a particular CSP called Unique Games. The fascinating aspect of this landscape is that the hardness of the single Unique Games problem reduces the complexity-theoretic task of showing inapproximability of every other CSP to the combinatorial/analytic task of designing a good dictatorship test that works with checks allowed by the CSP. While we do not seem to be close to a proof of the UGC, there is at least some evidence of the difficulty of the Unique Games problem, in the form of integrality gaps against strong semidefinite programming relaxations (from the so-called SA+ hierarchy) [KV15, RS09, KS09].

The complexity of approximate optimization of every CSP is thus settled under the Unique Games Conjecture (UGC). The UGC itself asserts the inapproximability of a particular CSP called Unique Games. The fascinating aspect of this landscape is that the hardness of the single Unique Games problem reduces the complexity-theoretic task of showing inapproximability of every other CSP to the combinatorial/analytic task of designing a good dictatorship test that works with checks allowed by the CSP. While we do not seem to be close to a proof of the UGC, there is at least some evidence of the difficulty of the Unique Games problem, in the form of integrality gaps against strong semidefinite programming relaxations (from the so-called SA+ hierarchy) [KV15, RS09, KS09].

The complexity of approximate optimization of every CSP is thus settled under the Unique Games Conjecture (UGC). The UGC itself asserts the inapproximability of a particular CSP called Unique Games. The fascinating aspect of this landscape is that the hardness of the single Unique Games problem reduces the complexity-theoretic task of showing inapproximability of every other CSP to the combinatorial/analytic task of designing a good dictatorship test that works with checks allowed by the CSP. While we do not seem to be close to a proof of the UGC, there is at least some evidence of the difficulty of the Unique Games problem, in the form of integrality gaps against strong semidefinite programming relaxations (from the so-called SA+ hierarchy) [KV15, RS09, KS09].

The Unique Games problem is a special case of a more general family of CSPs called Label Cover (see Section 2.1 for formal definitions relating to Label Cover, but briefly these are arity two CSPs whose constraint relations are unions of disjoint bipartite graphs). As the decision version of Unique Games is trivially polynomial time solvable, the UGC is useless in understanding the complexity of approximating satisfiable instances of CSPs (which is an important goal in itself, and also crucial for problems such as graph and hypergraph coloring). The most general form of Label Cover has also led to numerous strong inapproximability results, but without some restriction on the structure of the allowed constraints, it is not flexible enough to give a broad understanding similar to what the UGC provides.

Towards this end, Khot himself in his original UGC paper [Kho02] proposed a restricted form of Label Cover called 2-to-2 Label cover as a possible UG surrogate in some settings where inapproximability for satisfiable CSPs is desired. Unfortunately, for 2–to–2 Label Cover with perfect completeness (see a formal definition in Section 2.1), we do not know integrality gaps even for the standard SDP relaxation; the only gap known is for a weaker form where even simple non-negativity of inner products is not enforced [GKO+10]. In this paper, we give a dictatorship test with perfect completeness and arbitrarily small soundness for 2–to–2 Label Cover (a closely related version to 2–to–1 Label Cover that is more symmetric, see [DMR09, Thm A.3] for a reduction).

The main theorem we prove is informally as follows. The formal version appears as Theorem 3.5.

**Theorem 1.1** (Informal). There is a family of dictatorship tests with 2–to–2 constraints, which have perfect completeness (i.e., dictators pass the test with probability 1), and if a function \( f \) passes one of these tests with noticeable probability, then \( f \) has a coordinate that has noticeable low-degree influence.

While dictatorship tests are probably not the combinatorial/analytic core underlying inapproximability in the perfect completeness land, nevertheless our result can be viewed as some indication of the expressiveness and non-triviality of 2–to–1 constraints.

**Related work.** Other results proved using 2–to–1 or 2–to–2 conjecture include hardness results on finding independent sets in 3-uniform 2-colorable hypergraphs [KS14] and max \( k \)-coloring [GS13]. For the Max-\( k \)-CSP problem, dictatorship tests are known to exist within a constant factor of known polynomial time approximation algorithms [TY10, BKT17], although NP-hardness results have an exponential gap. In fact, only very recently has a Unique Games-surrogate been found which closes this gap up to a polynomial factor [BG17].

In the case of the Not-Two (NTW) predicate, defined as the elements of \( \{0, 1\}^3 \) which have Hamming weight not equal to 2, a series of papers [OW09a, OW09b, Hå14] went from a dictatorship test to conditional
hardness ($d$–to–$1$ conjecture) to finally unconditional hardness. The authors hope this family of dictatorship tests likewise provides valuable insights on the difficulty of the $2$–to–$2$ conjecture, and will perhaps aid in attempts to resolve the $2$–to–$2$ conjecture. Note that very recently there has been other progress [KMS17, DKK16] toward the $2$–to–$2$ conjecture, although they consider a variant without perfect completeness.

Note that nontrivial approximation algorithms are known for the $2$–to–$1$ Label Cover, although not strong enough to refute the $2$–to–$1$ conjecture. In particular, for all $\epsilon > 0$, [CMM06] found a $(L^{-\frac{\sqrt{2}-1+\epsilon}{2\sqrt{2}+1-\epsilon}})$ approximation algorithm for $2$–to–$1$ Label Cover (where $L$ is the label size of the instance) using an SDP relaxation.

2 Preliminaries

We first formally define what the $2$–to–$2$ Label Cover problem and its corresponding conjecture are. Subsequently we review the Fourier analytical tools which shall be used to understand the dictatorship tests.

2.1 The $d_1$–to–$d_2$ Label Cover problems

For a positive integer $L$, we let $[L]$ denote the set $\{1, 2, \ldots, L\}$.

Let $d_1$, $d_2$, $L_1$, and $L_2$ be positive integers. For any relation $R \subseteq [L_1] \times [L_2]$ we may consider the bipartite graph whose two sides are identified with $[L_1]$ and $[L_2]$ respectively, and two vertices $u \in [L_1]$ and $v \in [L_2]$ are connected by an edge if $(u, v) \in R$. We say that $R$ is an $d_1$–to–$d_2$ constraint if all connected components of this bipartite graph are complete bipartite and have at most $d_1$ components on the $[L_1]$ side and at most $d_2$ vertices on the $[L_2]$ side. Note in particular that a $d'_1$–to–$d'_2$ relation is a $d_1$–to–$d_2$ relation as long as $d'_1 \leq d_1$ and $d'_2 \leq d_2$.

An instance of $d_1$–to–$d_2$ Label Cover consists of a bipartite graph $G = (U, V, E)$, positive integers $L_1$ and $L_2$, and constraints $d_1$–to–$d_2$ constraints $\pi_{(u, v)} \subseteq [L_1] \times [L_2]$ or all $(u, v) \in E$. The ‘goal’ is to find labelings $\sigma : U \rightarrow [L_1]$ and $\psi : V \rightarrow [L_2]$ such that for all $(u, v) \in E$, $(\sigma(u), \psi(v)) \in \pi_{(u, v)}$. Any edge which satisfies this property is said to be satisfied the labelings $\sigma$ and $\psi$.

Conjecture 2.1 ($d_1$–to–$d_2$ conjectures [Kho02]). Let $d_1, d_2 \geq 1$ be positive integers and $\varepsilon > 0$ be a constant.

The following promise decision problem is $\text{NP}$-hard. Let $\Psi = (U, V, E, L, \pi_{(u, v)})$ be an instance of $d_1$–to–$d_2$ Label Cover. Distinguish between the following cases.

- **Completeness.** There exist labelings $\sigma : U \rightarrow [L_1]$ and $\psi : V \rightarrow [L_2]$ which satisfy all of the constraints if $(d_1, d_2) \neq (1, 1)$ or at least $1 - \varepsilon$ fraction of the constraints if $d_1 = d_2 = 1$.

- **Soundness.** For all labelings at most $\varepsilon$ fraction of the constraints are satisfied.

The $1$–to–$1$ conjecture is more well-known as the Unique Games Conjecture.

2.2 Fourier Analysis over $\mathbb{Z}_p$

Before we describe the dictatorship tests, we first remind the reader of some the basics of Fourier Analysis over $\mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$, with addition modulo $p$, where $p$ is an odd prime.

Let $L^2(\mathbb{Z}_p^n, \mathbb{C})$ be the vector space of functions $f : \mathbb{Z}_p^n \rightarrow \mathbb{C}$ with inner product

$$\langle f, g \rangle = \frac{1}{p^n} \sum_{x \in \mathbb{Z}_p^n} f(x) \overline{g(x)}.$$  \hspace{1cm} (1)
The Fourier basis we pick for $\mathbb{Z}_p$ is the set of characters $\{\chi_0, \chi_1, \ldots, \chi_{p-1}\}$, where $\chi_i(j) = \zeta^{ij}$, in which $\zeta$ is the primitive $p$th root of unity for all $i, j \in \mathbb{Z}_p$. We extend this basis to $\mathbb{Z}_p^n$ multiplicatively. For all $\alpha, x \in \mathbb{Z}_p^n$, let

$$\chi_\alpha(x) = \prod_{i=1}^{n} \chi_{\alpha_i}(x_i).$$

It is well-known that the $\chi_\alpha$’s form an orthonormal basis with respect to the inner product $(\cdot)$. For a function $f : \mathbb{Z}_p^n \to \mathbb{C}$, its Fourier coefficients $\hat{f} : \mathbb{Z}_p^n \to \mathbb{C}$ are the unique function which satisfies

$$f = \sum_{\alpha \in \mathbb{Z}_p^n} \hat{f}(\alpha) \chi_\alpha.$$

For $\alpha \in \mathbb{Z}_p^n$, we let $|\alpha| = \{i \in [n] : \alpha_i \neq 0\}$. We can now state/define few basic properties of a $f : \mathbb{Z}_p^n \to \mathbb{C}$ (e.g., from [O’D14]):

- $\mathbb{E}[f] = \hat{f}(0, \ldots, 0)$
- $\text{Var}[f] = \sum_{\alpha \in \mathbb{Z}_p^n, \alpha \neq 0} |\hat{f}(\alpha)|^2$
- $\text{Inf}_i(f) = \sum_{\alpha \in \mathbb{Z}_p^n, \alpha_i \neq 0} |\hat{f}(\alpha)|^2$
- $\text{Inf}_{\leq d}^i(f) = \sum_{\alpha \in \mathbb{Z}_p^n, \alpha_i \neq 0, |\alpha| \leq d} |\hat{f}(\alpha)|^2$.

In our analysis of the dictatorship tests, we need a few results from [MOO10] [KKMO07] on the noise stability of our function. There are many definitions, but we only need the Fourier analytic one (e.g., Proposition 8.28 of [O’D14]).

**Definition 2.1.** For $f \in \mathbb{Z}_p^n \to \mathbb{R}$ and $\eta \in [-1, 1]$,

$$S_\eta(f) = \sum_{\alpha \in \mathbb{Z}_p^n} \eta^{|\alpha|} |\hat{f}(\alpha)|^2,$$

where $0^0 = 1$.

We now cite a variant of the MOO theorem [MOO10] as stated in [KKMO07].

**Theorem 2.2** (Low-degree MOO theorem [MOO10] from [KKMO07]). Consider any $\eta \in [0, 1)$, $\epsilon > 0$, and $f : \mathbb{Z}_p^n \to [0, 1]$. If $\max_{i \in [n]} \text{Inf}_i^{\leq d}(f) \leq \delta$, where $\delta(\epsilon, \eta, p) > 0$ and $d(\epsilon, \eta, p) \in \mathbb{N}$, then

$$S_\eta(f) \leq \Lambda_\eta(\mathbb{E}[f]) + \epsilon,$$

where $\Lambda_\eta(\mu)$ is the probability that two $\eta$-correlated Gaussians with mean 0 and variance 1 are in the upper $\mu$ fraction of their CDFs.

The only fact we need about $\Lambda_\eta$ is the following upper bound.

**Lemma 2.3** (Corollary 3 of [KKMO07]). If $\eta \in (0, 1)$ and $q \geq 2$, then

$$\Lambda_q \left( \frac{1}{q} \right) \leq \left( \frac{1}{q} \right)^{\frac{1}{q}}.$$
3  A Family of Dictatorship Tests for 2–to–2 Label Cover

In this section, we construct the dictatorship tests for 2–to–2 constraints, and then analyze this construction using Fourier analysis.

3.1 The dictatorship tests

Consider the following 2–to–2 constraint. Let $S := \{0, 1, \ldots, (p - 1)/2\} \subseteq \mathbb{Z}_p$, where $p$ is an odd prime. Then our constraints are

$$\pi_{a,b} := \bigcup_{x \in S} \{(x + a, x + b), (-x + a, x + b), (x + a, -x + b), (-x + a, -x + b)\} \subseteq \mathbb{Z}_p^2.$$

In fact, we can replace $x \in S$ with $x \in \mathbb{Z}_p$ in the above definition. When we identify $\pi_{a,b}$ as a probability distribution, we give double weight to the 1–to–1 constraint $(a, b)$ so that the marginal distributions are uniform.

Our dictatorship test is then the following. Let $n \geq 1$ be a positive integer. The test is on a set of $p^n$ variables, whose labeling is represented by a function $F : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$. The test proceeds by the following algorithm.

- Draw $a, b \in \mathbb{Z}_p$ uniformly and independently at random.
- Draw $x, y \in \mathbb{Z}_p^n$ uniformly at random from $\pi_{a,b}^{\otimes n}$.
- Test $(F(x), F(y)) \in \pi_{a,b}$.

By a standard trick, we may assume that $F$ is folded. That is, for all $a \in \mathbb{Z}_p$ and $x \in \mathbb{Z}_p^n$, $F(x + (a, \ldots, a)) = F(x) + a$. As usual, to enforce this, when querying $F(x)$, we instead query $F(x - (x_1, \ldots, x_1))$ and add $x_1$ to the result. (For convenience, we write $1_n = (1, \ldots, 1)$.) This technicality can be moved within the CSP, by adjusting checking $(F(x), F(y)) \in \pi_{a,b}$ to $(F(x - x_1 1_n), F(y - y_1 1_n)) \in \pi_{a-x_1, b-y_1}$.

Note that the dictator functions $F(x) = x_i$ for some $i \in [n]$ pass this test with probability 1. We now seek to show that if some $F$ passes this test with probability at least $\epsilon$, then $F$ is ‘close’ to one of these dictator functions. Like O’Donnell and Wu [OW09a] we measure closeness in terms of having a coordinate with a significant low-degree influence.

3.2 Analysis of the Dictatorship Tests

Identify $F$ with the function $f : \mathbb{Z}_p^n \rightarrow \mathbb{C}$, where $f(x) = 1$ iff $F(x) = 0$ and $f(x) = 0$ otherwise. Since $F$ is folded, we must have that $\mathbb{E}[f] = \frac{1}{p}$. The success probability is

$$\epsilon \leq \mathbb{E}_{a,b} \left[ \mathbb{E}_{(x,y) \sim \pi_{a,b}^{\otimes n}} [1(F(x), F(y)) \in \pi_{a,b}] \right]$$

$$\leq \mathbb{E}_{a,b} \left[ \mathbb{E}_{(x,y) \sim \pi_{a,b}^{\otimes n}} \left[ 2p \mathbb{E}_{(i,j) \sim \pi_{a,b}} [f(x - i1_n) \bar{f}(y - j1_n)] \right] \right] \quad \text{(double counting when } (i,j) = (a,b) \text{)}$$

$$= 2p \mathbb{E}_{a,b} \left[ \mathbb{E}_{(x,y) \sim \pi_{a,b}^{\otimes n}} \left[ \mathbb{E}_{(i,j) \sim \pi_{a,b}} \left[ \sum_{a,\beta \in \mathbb{Z}_p^n} \hat{f}(a) \hat{\beta}(\beta) \chi_a(x-i1_n) \chi_\beta(y-j1_n) \right] \right] \right]$$
One can verify that entries
\[ \chi_{\alpha_k}(x_k - i) \chi_{\beta_k}(y_k - j) \]

For example, see [hs11].

Then, it is easy to see that the above probability equals

\[ \frac{1}{2} \sum_{(i,j) \in \pi_{a,b}} \hat{f}(\alpha) \hat{f}(\beta) \chi_{\alpha}(((a - i)1_n) \chi_{\beta}((b - j)1_n) 2^{-|\alpha|}} \]

If \( \alpha, \beta \in \mathbb{Z}_p^n \), define \( \alpha \beta \) to be the pointwise product. Furthermore, define

\[ C_\alpha = \{ \alpha z \in \mathbb{Z}_p^n \mid z \in \{1, p-1\}^n \subseteq \mathbb{Z}_p^n \}. \]

Then, it is easy to see that the above probability equals

\[ \epsilon \leq 2p \sum_{(i,j) \in \pi_{a,b}} \sum_{\alpha, \beta \in C_\alpha} \hat{f}(\alpha) \hat{f}(\beta) \chi_{\alpha}(((a - i)1_n) \chi_{\beta}((b - j)1_n) 2^{-|\alpha|}} \]

Note that \((i,j) \in \pi_{a,b}\) if and only if \(a - i = \pm(b - j)\). In fact, we can rewrite the above expression as

\[ \epsilon \leq 2p \sum_{\alpha, \beta \in C_\alpha} \hat{f}(\alpha) \hat{f}(\beta) 2^{-|\alpha|} \sum_{x \in \mathbb{Z}_p^n} \chi_{\alpha}(x) \chi_{\beta}(-x) \]

Note that the \( C_\alpha \)'s are equivalence classes of size \( 2^{|\alpha|} \). In particular, \( \beta \in C_\alpha \) iff \( \alpha \in C_\beta \). Let \( C = \{ C_\alpha : \alpha \in \mathbb{Z}_p^n \} \). Thus, we then have that

\[ \epsilon \leq p \sum_{C_\gamma \in C} \sum_{\alpha, \beta \in C_\gamma} \hat{f}(\alpha) \hat{f}(\beta) (1[\chi_{\alpha+\beta}(1) = 1] + 1[\chi_{\alpha-\beta}(1) = 1]) \]

Let \( \hat{f}(C_\gamma) \) be the vector of length \( |C_\gamma| \) whose entries are \( \hat{f}(\alpha) \). Let \( M^\gamma \) be the \( |C_\gamma| \times |C_\gamma| \) matrix with entries

\[ M_{\alpha, \beta}^\gamma = \frac{1[\chi_{\alpha+\beta}(1) = 1] + 1[\chi_{\alpha-\beta}(1) = 1]}{|C_\gamma|}. \]

One can verify that \( M^\gamma \) is a real, symmetric, doubly stochastic matrix (modulo scaling of the entries). Thus, the largest eigenvalue of \( M^\gamma \), \( \lambda^\gamma \) is this common row/column sum. Then, we can see that

\[ \epsilon \leq p \sum_{C_\gamma \in C} \hat{f}(C_\gamma)^* M^\gamma \hat{f}(C_\gamma) \]

\[ \text{For example, see [hs11].} \]

\[ \text{This deduction non-obviously uses the facts that } \hat{f}(\alpha) = \hat{f}(-\alpha), -\alpha \in C_\alpha, \text{ and } M_{\alpha, -\beta}^\gamma = M_{|\alpha|, \beta}^\gamma. \]
\[
\leq p \sum_{C_\gamma \in C} \lambda' \|f(C_\gamma)\|^2
= p \sum_{C_\gamma \in C} \sum_{\alpha \in C_\gamma} |f(\alpha)|^2 \lambda'.
\]

(2)

We next seek to show that \(\lambda'\) is bounded by a particular decreasing function of \(|\gamma|\).

**Lemma 3.1.** There exists a universal constant \(C > 0\) such that for all \(n \in \mathbb{N}\), \(p\) odd prime, and \(\gamma \in \mathbb{Z}_p^n\):

\[
\lambda' \leq \frac{2}{p} + \frac{C}{|\gamma|^{1/4} + 1}.
\]

Before we can do that, we need the following result.

**Lemma 3.2.** There exists a universal constant \(C > 0\) such that for all \(n \in \mathbb{N}\), \(p\) prime, and \(\beta \in \mathbb{Z}_p^n\):

\[
\Pr_{z \sim \{0, 1\}^n} \bigg[ \chi_\beta(z) = 1 \bigg] = \Pr_{z \sim \{0, 1\}^n} \left[ \sum_{i=1}^n \beta_i z_i = 0 \right] \leq \frac{1}{p} + \frac{C}{|\beta|^{1/4} + 1}.
\]

**Remark.** This lemma can be considered a finite-field analogue of a result of Littlewood and Offord [LO43].

The exponent of \(1/4\) can in fact be improved to \(1/2 - o(1)\), but the former is all we need.

**Proof.** Let \(k = |\beta|\). Assume \(k \geq 1\). Assume without loss of generality that the nonzero terms of \(\beta\) are \(\beta_1, \ldots, \beta_k\). Then

\[
\Pr_{z \sim \{0, 1\}^n} \left[ \sum_{i=1}^n \beta_i z_i = 0 \right] = \mathbb{E}_{z \sim \{0, 1\}^n} \left[ \mathbb{E}_{j \sim \mathbb{Z}_p} \left[ \chi_{\sum_{i=1}^n \beta_i z_i}^j \right] \right]
\]

\[
= \mathbb{E}_{j \sim \mathbb{Z}_p} \left[ \prod_{i=1}^k \frac{1 + \zeta^j \beta_i}{2} \right]
\]

\[
\leq \frac{1}{p} \prod_{j=0}^{p-1} \left| \prod_{i=1}^k \frac{1 + \zeta^j \beta_i}{2} \right|.
\]

Since the \(\beta_i\) are nonzero for \(i \in [k]\), we have that for a fixed \(i, 1 + \zeta^j \beta_i\) is a permutation of \(1 + \zeta^0, \ldots, 1 + \zeta^{p-1}\).

By the rearrangement inequality, the above product is maximized when all the permutations are consistent. That is,

\[
\frac{1}{p} \sum_{i=1}^{p-1} \prod_{j=1}^k \left| 1 + \zeta^i \beta_j \right| \leq \frac{1}{p} \sum_{j=0}^{p-1} \left| \frac{1 + \zeta^j}{2} \right|^k
\]

\[
= \frac{1}{p} \sum_{j=0}^{p-1} \left| 1 + \cos(2\pi j/p) + i \sin(2\pi j/p) \right|^k
\]

\[
\leq \frac{1}{p} \sum_{j=0}^{p-1} |\cos(\pi j/p)|^k
\]

\[
= \frac{1}{p} + \frac{2}{p} \left( \frac{(p-1)/2}{k} \right)
\]

To further bound, we need the following elementary inequality
Claim 3.3. For all $\theta \in [0, \pi/2]$,
\[
\cos \theta \leq 1 - \frac{\theta^2}{4}.
\]

Proof. Note that $\sin \eta \geq \eta/2$ for all $\eta \in [0, \pi/2]$ since $\sin \eta - \eta/2$ is a concave function in $[0, \pi/2]$ which is nonnegative at its endpoints. We then integrate this from 0 to $\theta$ to obtain the above inequality. \hfill \Box

Thus, for all $j \in \{1, \ldots, (p - 1)/2\}$,
\[
\cos^k(\pi j/p) \leq \left(1 - \frac{\pi^2 j^2}{4p^2}\right)^k.
\]

Let $\ell = \lfloor 2p/(k^{1/4}) \rfloor$. Then, we have that
\[
\frac{1}{p} + \frac{2}{p} \sum_{j=1}^{(p-1)/2} \cos^k(\pi j/p) \leq \frac{1}{p} + \frac{2}{p} \sum_{j=1}^{(p-1)/2} \left(1 - \frac{\pi^2 j^2}{4p^2}\right)^k
\leq \frac{1}{p} + \frac{2\ell}{p} + \max\left(\frac{2((p-1)/2 - \ell)}{p} \left(1 - \frac{\pi^2 (\ell + 1)^2}{4p^2}\right)^k, 0\right)
\leq \frac{1}{p} + \frac{4}{k^{1/4}} + \max\left(1 - \frac{\pi^2}{k^{1/2}}, 0\right)^k
\leq \frac{1}{p} + \frac{C'}{k^{1/4} + 1}
\]
for some universal constant $C' > 0$. To account for the case $k = 0$, we may set $C = \max(C', 1)$. \hfill \Box

Proof of Lemma 3.1. By the previously mentioned symmetries of $M^r$,
\[
\lambda^r = \mathbb{E}_{\alpha \sim C_r} \left[1_{\chi_{\alpha+\gamma}(1_n) = 1} + 1_{\chi_{\alpha-\gamma}(1_n) = 1}\right]
= 2 \mathbb{E}_{\alpha \sim C_r} \left[1_{\chi_{\alpha-\gamma}(1_n) = 1}\right]
= 2 \mathbb{E}_{z \sim (\{-1,1\})^n} \left[1_{\chi_{z-\gamma}(1_n) = 1}\right]
= 2 \mathbb{E}_{z \sim (\{-1,1\})^n} \left[1_{\chi_{z}(z-1_n) = 1}\right]
= 2 \mathbb{E}_{z' \sim (0,1)^n} \left[1_{\chi_{z'}((1_n - 2z') - 1_n) = 1}\right]
= 2 \mathbb{E}_{z' \sim (0,1)^n} \left[1_{\chi_{z'}(z') = 1}\right] \quad \text{(since } p \text{ odd prime)}
\leq \frac{2}{p} + \frac{2C}{|\gamma|^{1/4} + 1},
\]
where the last step follows from Lemma 3.2. \hfill \Box

We also need to invoke the following analytical lemma.
Lemma 3.4. For all \( \epsilon > 0 \) and \( L \in \mathbb{N} \), there exists \( P(\epsilon, L) \in \mathbb{N} \), such that for all primes \( p \geq P \), there exists \( \delta(\epsilon, L, p) > 0 \) and \( d(\epsilon, L, p) \in \mathbb{N} \) such that for all \( f : \mathbb{Z}_p^n \to \{0, 1\} \) with \( \mathbb{E}[f] = 1/p \) the following holds. If \( \text{Inf}_{i \in [n]}^{\leq d}(f) \leq \delta \) for all \( i \in [n] \) then

\[
\sum_{\alpha \in \mathbb{Z}_p^n, |\alpha| \leq L} |\hat{f}(\alpha)|^2 \leq \epsilon \mathbb{E}[f] = \frac{\epsilon}{p}.
\]

Remark. The LHS does not fundamentally depend on the choice of Fourier basis for \( \mathbb{Z}_p \). For example, the Efron-Stein decomposition \([ES81]\) works just as well.

Proof. First, we set the parameters

\[
\eta = 1/2
\]

\[
P = \lceil (\epsilon \eta L)^{-\frac{11n}{14p}} \rceil + 1
\]

\[
\epsilon' = \frac{\epsilon \eta L}{p} - \left( \frac{1}{p} \right)^{\frac{1}{2p}} (\text{positive since } p \geq P)
\]

Let \( d \) and \( \delta \) be the parameters guaranteed by the modified MOO theorem (Theorem 2.2) where their \((\epsilon', \eta, p)\) is our \((\epsilon, \eta, p)\). If \( \max_{i \in [n]} \text{Inf}_{i \in [n]}^{\leq d}(f) \leq \delta \), by a standard argument

\[
\sum_{\alpha \in \mathbb{Z}_p^n, |\alpha| \leq L} |\hat{f}(\alpha)|^2 \leq \sum_{\alpha \in \mathbb{Z}_p^n} \eta^{|\alpha|-L} |\hat{f}(\alpha)|^2
\]

\[
\leq \eta^{-L} \mathbb{S}_\eta(f)
\]

\[
\leq \eta^{-L} (\Lambda_\eta (1/p) + \epsilon') \quad \text{(modified MOO theorem, since } \max_{i \in [n]} \text{Inf}_{i \in [n]}^{\leq d}(f) \leq \delta)
\]

\[
\leq \eta^{-L} \left( \left( \frac{1}{p} \right)^{\frac{1}{2p}} + \epsilon' \right) \quad \text{(Lemma 2.3)}
\]

\[
= \eta^{-L} \frac{\epsilon \eta L}{p} = \frac{\epsilon}{p},
\]

as desired. \( \square \)

Now, we may establish the main result.

Theorem 3.5. For every \( \epsilon > 0 \), there exists \( P \in \mathbb{N} \) such that for all primes \( p \geq P \), there exists \( \delta > 0 \) and \( d \in \mathbb{N} \) such that the following holds. If \( F : \mathbb{Z}_p^n \to \mathbb{Z}_p \) is a folded function which passes the 2–to–2 Label Cover modulo \( p \) dictatorship test with probability at least \( \epsilon \), then

\[
\max_{i \in [n]} \text{Inf}_{i \in [n]}^{\leq d} f \geq \delta,
\]

where \( f(x) = 1[F(x) = 0] \).

Proof. First select the following parameters

\[
\epsilon' = \frac{\epsilon}{8C}
\]

\[
L = \left\lceil \left( \frac{1}{\epsilon'} \right)^4 \right\rceil.
\]
Let $P'$ be the $P$ guaranteed by Lemma 3.4 when $\epsilon = \epsilon'/2$ and $L = L$. Let $P = \max(P', 4/e)$. Assume $p \geq P$.

Let $\delta$ and $d$ be the values (independent of $n$) guaranteed by Lemma 3.4 for our choice of $p$.

From our previous analysis (2), we know that

$$\sum_{C, \alpha \in C} |\hat{f}(\alpha)|^2 \leq \frac{2}{p} + \frac{C}{|\alpha|^{1/4} + 1}.$$  (Lemma 3.1)

Thus, the first term contributes at most $\epsilon/2$ to the sum. For the next part, note that $\frac{C}{|\alpha|^{1/4} + 1} \leq \frac{\epsilon}{8}$. Then,

$$\epsilon \leq \epsilon/2 + pC \sum_{\beta \in \mathbb{Z}_n^d, |\beta| \leq L} |\hat{f}(\beta)|^2 \leq \frac{\epsilon}{2} + pC \sum_{\beta \in \mathbb{Z}_n^d, |\beta| > L} |\hat{f}(\beta)|^2 \leq \frac{\epsilon}{2} + pC \sum_{\beta \in \mathbb{Z}_n^d} |\hat{f}(\beta)|^2 + \epsilon/8.$$  

Thus, we have that

$$\sum_{\beta \in \mathbb{Z}_n^d, |\beta| \leq L} |\hat{f}(\beta)|^2 \geq \frac{3\epsilon}{8pC} > \frac{\epsilon'}{2} \mathbb{E}[f].$$

By the contrapositive to Lemma 3.4, we have that $\max_{i \in [n]} \inf_{f' \leq d} f \geq \delta$, as desired.  \qed

### Acknowledgments

We would like to thank an anonymous reviewer for pointing us to [LO43].

### References


