Electronic Colloquium on Computational Complexity, Report No. 70 (2019)

On Local Testability in the Non-Signaling Setting

Alessandro Chiesa
alexch@berkeley.edu
UC Berkeley

Peter Manohar
manohar@berkeley.edu
UC Berkeley

Igor Shinkar
ishinkar@sfu.ca
Simon Fraser University

May 13, 2019

Abstract

Non-signaling strategies are a generalization of quantum strategies that have been studied in physics for decades, and have recently found applications in theoretical computer science. These applications motivate the study of local-to-global phenomena for *non-signaling functions*.

We present general results about the local testability of linear codes in the non-signaling setting. Our contributions include formulating natural definitions that capture the condition that a non-signaling function "belongs" to a given code, and characterizing the sets of local constraints that imply membership in the code. We prove these results by relating the Fourier spectrum of non-signaling functions to Cayley hypergraphs induced by local constraints.

We apply the above results to show a separation between locally testable codes in the classical and non-signaling setting by proving that bivariate low-degree testing fails spectacularly in the non-signaling setting. Specifically, we show that there exist non-signaling functions that pass bivariate low-degree tests with probability 1, and yet are maximally far from low-degree.

Keywords: non-signaling strategies; locally testable codes; low-degree testing; Fourier analysis

ISSN 1433-8092

Contents

1 Introduction

Locally testable codes (LTCs) are error correcting codes in which one can verify whether a given string belongs to the code by reading only a few (randomly chosen) bits from the string. Goldreich and Sudan [GS06] have described LTCs as the "combinatorial counterparts of the complexity theoretic notion of PCPs", motivating the standalone study of these objects.

In this work we study local testability for *non-signaling strategies*, which are a class of non-local strategies that generalize quantum strategies, capturing the maximum amount of "non-local correlation" that can occur under the assumption that spatially-isolated parties cannot communicate instantaneously. Non-signaling strategies have been studied in physics for decades [Ras85; KT92; PR94], in order to better understand quantum entanglement. Recently they have gained attention in computer science due to their applications to hardness of approximation [KRR16] and delegation of computation [KRR13; KRR14]. PCPs sound against non-signaling strategies (nsPCPs) underlie these applications, which motivates the study of local testability in the non-signaling setting.

Given an integer n, a field $\mathbb{F}$, and a locality parameter $k \leq n$, the object that we study is a *k-non-signaling function* $\mathcal{F}\colon [n] \to \mathbb{F}$, which extends the notion of a function $f\colon [n] \to \mathbb{F}$ as follows.[1]

Definition 1.1. *A k-**non-signaling function** $\mathcal{F}\colon [n] \to \mathbb{F}$ is a collection $\{\mathcal{F}_S\}_{S\subseteq[n]:|S|\leq k}$ where each $\mathcal{F}_S$ is a distribution over local functions $g\colon S \to \mathbb{F}$, and for any two subsets $R \subseteq S \subseteq [n]$ with $|S| \leq k$ it holds that the distribution $\mathcal{F}_R$ and the marginal distribution $\mathcal{F}_S|_R$ are equal.[2] (The set of all such $\mathcal{F}$ are the solutions to the k-relaxation in the Sherali–Adams hierarchy [SA90].)*

The evaluation of $\mathcal{F}$ on a set S is a single sample $g\colon S \to \mathbb{F}$ from the distribution $\mathcal{F}_S$. Intuitively, a k-non-signaling function is like a quantum function: evaluation is probabilistic and only happens once, just like quantum measurement; and $\mathcal{F}$ can only be evaluated on at most k points simultaneously, which is similar to the uncertainty principle. As k approaches n, $\mathcal{F}$ behaves more like a classical function and, when $k = n$, $\mathcal{F}$ is a distribution over functions $f\colon [n] \to \mathbb{F}$.

Local testability of non-signaling functions may sound like an oxymoron, because non-signaling functions, at least superficially, are collections of local distributions with no global structure that we can talk about. Yet prior work has shown that local-to-global phenomena *are possible*.

For example, [CMS18] shows that any non-signaling function passing the linearity test [BLR93] with high probability is well-approximated by a *quasi-distribution* supported on linear functions. This result was later used in [CMS19] to show that the exponential-length constant-query PCP of [ALMSS98] is sound against non-signaling strategies.

The results obtained in [CMS18; CMS19] naturally raise the question of whether local testability in the non-signaling setting is possible for other codes, like those based on low-degree polynomials. After all, both linearity testing and low-degree testing do work in the quantum setting [NV18].

Recall that, in the classical setting, local testability plays a central role in PCP constructions, many of which can be described as having two main components.

- *Property testing:* check with few queries whether or not the given proof π belongs to a code $\mathbf{C}$.

[1] There are two distinct definitions of a non-signaling strategy, depending on whether the strategy is meant to represent isolated parties or a function. The former is used for MIPs [KRR13; KRR14], while the latter is used for PCPs and property testing [KRR13; KRR14; CMS18; CMS19]. We use the latter definition, although equivalent statements of all our results will hold when adopting the former definition (see the appendix in [CMS18]).

[2] A common relaxation of this condition requires that these two distributions are only statistically (or computationally) close. While we consider the standard definition, we note that this is without loss of generality as [CMS18] shows that every statistically (or computationally) non-signaling strategy is close to an (exact) non-signaling strategy.

- *Checking computation:* given that π is a codeword in $\mathbf{C}$ (or at least is close to a codeword), check with few queries whether or not π proves the desired statement.

This modular approach has enabled the study of local testability as a natural standalone goal, which in turn has led to improved PCP constructions.

Inspired by this state of affairs, we initiate the study of locally testable codes in the non-signaling setting. We believe that, similarly to the classical setting, understanding local testability against non-signaling strategies will enable researchers to construct more efficient non-signaling PCPs.

1.1 The curious case of bivariate testing

We study two simple bivariate low-degree tests: the *row/column test* and the *random lines test*. We prove that both of these tests *fail* to test proximity to low-degree non-signaling functions.

The row/column test. We first discuss the case of the row/column test. Given a function $f\colon \mathbb{F}^2 \to \mathbb{F}$, this test: (1) samples a random axis-parallel line L from the set of all rows and columns in $\mathbb{F}^2$; (2) samples a random subset $S \subseteq L$ of size $d+2$; (3) checks that $f|_S$ is a univariate polynomial of degree d. It is well-known that if f passes the row/column test with high probability, then f is close to (the evaluation of) a bivariate polynomial of degree at most d in each variable [PS94]. Below we ask whether the row/column test is also sound in the non-signaling setting.

Suppose that a k-non-signaling function $\mathcal{F}\colon \mathbb{F}^2 \to \mathbb{F}$ passes the row/column test with high probability. Can we deduce any global low-degree structure about $\mathcal{F}$?

In more detail, the probabilistic experiment that we consider is this: first we sample a query set S according to the distribution of the row/column test; then we sample a local $g\colon S \to \mathbb{F}$ according to the distribution $\mathcal{F}_S$; and finally we check that g is a univariate polynomial of degree d.

The answer to the above question will, in general, depend on the locality parameter k of $\mathcal{F}$. At minimum, we need $k \geq d+2$ for otherwise we cannot even run the row/column test (k is the maximum number of simultaneous queries to $\mathcal{F}$). At the other extreme, when k has the maximum value ($k = |\mathbb{F}|^2$) then we are back to the classical case because $\mathcal{F}$ is now a distribution over functions $f\colon \mathbb{F}^2 \to \mathbb{F}$; hence if $\mathcal{F}$ passes the test with high probability then (one can verify that) with high probability a function f sampled according $\mathcal{F}$ is close to low-degree. In fact, even when $k \geq (d+1)^2$, we are in a trivial case, as one can query $\mathcal{F}$ on an interpolating set, a "square of $(d+1)^2$ points".

We are thus interested in whether or not the test works for *non-trivial* values of k, namely when $d+2 \leq k < (d+1)^2$. In this regime, k is large enough to run the test, and yet is small enough so that one cannot query an interpolating set. We show, surprisingly, that the row/column test fails in the non-signaling setting for non-trivial values of k. In fact, we show that it fails *even when the test passes with probability* 1, namely, it fails in the worst possible sense.

Theorem 1 (informal)**.** *For every k with $2d+2 \leq k < \frac{7}{32}(d+2)^2$, there exists a k-non-signaling function that passes the row/column test with probability 1, and yet is $(1-\frac{1}{|\mathbb{F}|})$-far from all bivariate k-non-signaling functions of individual degree d.*

Theorem 1 is surprising. The row/column test is a natural test for which we would expect some guarantee to hold (regardless of how weak), at the very least when the test passes with probability 1. We note that although Theorem 1 does not cover all possible non-trivial values of k, it does capture an interval that is within a constant factor of the trivial regime on either side.

The random lines test. It is tempting to argue that the failure of the row/column test uncovered in Theorem 1 is due to the fact that the test only examines *axis-parallel* lines. This is not the case; our analysis can be modified to also show a strong negative result for the *random lines* test (which tests total degree d, rather than individual degree d).

Theorem 2 (informal)**.** *For every k with $2d+2 \leq k < \frac{3}{16}(d+2)^2$, there exists a k-non-signaling function that passes the random lines test with probability 1, and yet is $(1-\frac{1}{|\mathbb{F}|})$-far from all bivariate k-non-signaling functions of total degree d.*

The random lines test is arguably the most canonical bivariate low-degree test, and so Theorem 2 appears to give strong evidence that bivariate low-degree testing is *not possible* in the non-signaling setting, for non-trivial values of k. Formally ruling out *all* tests remains an intriguing open question.

Beyond bivariate test. The above theorems stand in sharp contrast to the fact that there is *no regime* of k where the linearity test fails [CMS18]. Our results thus suggest that bivariate low-degree testing is a qualitatively different task, as it has a regime of k where natural tests fail.

Our theorems on low-degree testing are in fact a direct application of more general results that we prove about the structure of local characterizations for *any linear code*, in the non-signaling setting. We view our general results on local characterizations as the main technical contribution of this paper, and we now discuss them.

1.2 Local characterizations and Cayley hypergraphs

Local characterizations are fundamental to the study of locally testable codes [RS96]. They express membership in a given linear code via a set of low-weight constraints, and they naturally induce a canonical tester: sample a random low-weight constraint and check if the given word satisfies it. In order to prove the negative results presented above, we do not need to consider distributions on constraints, but instead we only need to study how constraints express code membership, via *exact* local characterizations [RS96]. Below we describe our main technical contribution, which informally consists of establishing necessary and sufficient conditions for when a constraint set is a local characterization for a code, in the non-signaling setting. We begin by recalling known facts about local characterizations in the classical setting, and then proceed to the non-signaling setting.

The classical setting. A *constraint set* $T \subseteq \mathbb{F}^n$ for a linear code $\mathbf{C} \subseteq \mathbb{F}^n$ is a subset of its dual code $\mathbf{C}^\perp$. A constraint set T is a *ℓ-local characterization* of $\mathbf{C}$ if every $\alpha \in T$ has at most ℓ non-zero entries, and the condition "$\langle \alpha, f \rangle = 0$ for every $\alpha \in T$" implies that $f \in \mathbf{C}$ (and conversely).

For example, the set $\{e_x + e_y - e_{x+y} : x, y \in \{0,1\}^n\}$ where e_x is the x-th standard basis vector in $\{0,1\}^{\{0,1\}^n}$ is a 3-local characterization of the Hadamard code, because $f(x)+f(y)-f(x+y) = 0$ for every $x, y \in \{0,1\}^n$ implies that f is a linear function, and conversely. The Reed–Muller code containing all polynomials $f \colon \mathbb{F}^m \to \mathbb{F}$ in m variables of total degree at most d has a $(d+2)$-local characterization T, where T contains a constraint α for each subset S of $\mathbb{F}^m$ of size $d+2$ that is contained in a line.

There is a simple condition that is both necessary and sufficient for a constraint set T to be a local characterization for $\mathbf{C}$: the span of T equals $\mathbf{C}^\perp$. In this work it is useful to recall another equivalent condition, which may at first appear mysterious, that involves the connectivity of a Cayley graph. Namely, let $G(\mathbf{C}^\perp, T)$ be the Cayley graph with vertices $V := \mathbf{C}^\perp$ and edges E generated by T, i.e., $E := \{(\alpha, \alpha+\gamma) : \gamma \in T\} \cup \{(\alpha, b\alpha) : b \in \mathbb{F} \setminus \{0\}\}$. Then the following holds:

Lemma 1.2 ([GVZ14])**.** *A constraint set T is a local characterization of a linear code $\mathbf{C}$ if and only if the vertex 0^n has a path to every other vertex in the Cayley graph $G(\mathbf{C}^\perp, T)$.*

This elegant equivalence is an implication of a close relationship between locally testable codes and Cayley graphs with certain properties [GVZ14].

An equivalence for non-signaling functions. We prove an analogous equivalence in the non-signaling setting, which informally states that a suitable notion of local characterization for any linear code is equivalent to a connectivity property of a Cayley *hyper*graph. In fact, the equivalence that we prove is a strict generalization of Lemma 1.2, as explained below.

We begin by formulating a notion of local characterization that works for constraint sets applied to non-signaling functions rather than (classical) functions. There are two main qualitative differences with the classical case. First, the definition depends on the locality parameter k because we need to specify the locality of the non-signaling functions that we consider. Second, the requirement that a non-signaling function "belongs" to a code $\mathbf{C}$ is expressed via a property that we call $\mathbf{C}$-*explainability*, on which we comment after the definition.

Definition 1.3 (informal)**.** *A constraint set $T \subseteq \mathbf{C}^\perp$ is a* **ℓ-local characterization** *for $(\mathbf{C}, k)$ if every $\alpha \in T$ has at most ℓ non-zero entries, and the set of k-non-signaling functions that satisfy every $\alpha \in T$ with probability 1 equals the set of k-non-signaling functions that are "$\mathbf{C}$-explainable".*

The term "$\mathbf{C}$-explainable" refers to the condition that the given non-signaling function is, with probability 1, consistent with the restriction of some codeword in $\mathbf{C}$. This condition is motivated by non-trivial properties of the Fourier spectrum of non-signaling functions that we discuss later on (see Section 2.4). For now, it suffices to say that if a non-signaling function $\mathcal{F}$ is $\mathbf{C}$-explainable then $\mathcal{F}$ satisfies natural *global* properties that extend code membership to the non-signaling setting.

We remark that Definition 1.3 reduces to the classical notion of local characterization when setting $k := n$. We now define the Cayley hypergraph that will be used in our equivalence below.

Definition 1.4. *Given a set $T \subseteq \mathbf{C}^\perp$, the* **Cayley hypergraph** *$\Gamma_k(\mathbf{C}^\perp, T)$ has*
- *vertices $V = \{\alpha \in \mathbf{C}^\perp : \mathrm{wt}(\alpha) \leq k\}$,*
- *edges $E = \{(\alpha, \alpha + \gamma) : \gamma \in T, |\mathrm{supp}(\alpha) \cup \mathrm{supp}(\gamma)| \leq k\} \cup \{(\alpha, b\alpha) : b \in \mathbb{F} \setminus \{0\}\}$, and*
- *hyperedges $H = \{(\alpha, \beta, \alpha + \beta) : |\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)| \leq k\}$.*

Above, $\mathrm{supp}(\alpha)$ denotes the set of indices $i \in [n]$ where $\alpha_i \neq 0$, and $\mathrm{wt}(\alpha)$ is the size of $\mathrm{supp}(\alpha)$. The Cayley hypergraph is like the "weight restriction" of a Cayley graph (only low-weight elements of $\mathbf{C}^\perp$ are vertices), augmented with hyperedges that express certain linear relations among vertices.

The motivation behind the definition of Cayley hypergraphs is the following fact: if there is a path from 0^n to α in $\Gamma_k(\mathbf{C}^\perp, T)$, then any k-non-signaling function that satisfies every constraint in T must satisfy α as well. Cayley hypergraphs thus capture a notion of constraint propagation.

We now state our main technical contribution, a non-signaling analogue of Lemma 1.2:

Theorem 3 (informal)**.** *A constraint set T is a ℓ-local characterization for $(\mathbf{C}, k)$ if and only if the vertex 0^n has a path to every other vertex in the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$.*

When $k = n$ we recover the classical statement (Lemma 1.2). This is because when $k = n$, if α is reachable from 0^n in $\Gamma_k(\mathbf{C}^\perp, T)$ then α is reachable *without using any hyperedges*. In particular, when $k = n$ we can view $G(\mathbf{C}^\perp, T)$ as a degenerate case of $\Gamma_k(\mathbf{C}^\perp, T)$, as if we remove the hyperedges from the latter hypergraph we obtain the former graph and reachability from 0^n is unaffected.

However, when $k < n$, the equivalence is qualitatively different from its classical analogue. While Lemma 1.2 captures a simple linear algebraic statement (the constraints span the dual code), Theorem 3 is a non-trivial statement that *does not involve linear spaces*. This is because reachability in the Cayley hypergraph depends on the parameter k in a way that breaks linearity.

To emphasize the difference between the classical and the non-signaling settings, consider a subset $\{\gamma_1, \ldots, \gamma_r\} \subseteq T$ of size r, and let $\alpha = \sum_{i=1}^{r} \gamma_i$. In the classical setting $G(\mathbf{C}^\perp, T)$ has a path $(\alpha_0 = 0^n, \alpha_1, \ldots, \alpha_r = \alpha)$ from 0^n to α of length r, where α_i is $\gamma_1 + \cdots + \gamma_i$. In the non-signaling setting the situation may be different, because even if $\mathrm{wt}(\alpha) \leq k$ (which means that α is a vertex in $\Gamma_k(\mathbf{C}^\perp, T)$), it may be the case that the foregoing path has $\mathrm{wt}(\alpha_i) > k$ for some $0 < i < r$, so that α_i is not a vertex in $\Gamma_k(\mathbf{C}^\perp, T)$, and thus the path does not exist in $\Gamma_k(\mathbf{C}^\perp, T)$.

1.3 On robust local characterizations

We have so far discussed *exact* local characterizations, which suffice for the negative results about bivariate low-degree testing presented in Section 1.1. Can we say anything about *robust* local characterizations? In the classical setting, these are related to spectral properties of the Cayley graph $G(\mathbf{C}^\perp, T)$ [GVZ14]. In this work we show that a suitable non-signaling analogue of robust local characterizations is related to shortest paths in the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$. An application of this result is that much of the analysis of the linearity test in [CMS18] is tight up to constants.

Robust local characterizations. We consider the case where a non-signaling function $\mathcal{F}$ satisfies *every* constraint α in T with high probability (as opposed to probability 1, as in the exact case). This is different from the classical case where we assume that a function f satisfies a random constraint α in T (sampled from a distribution over T) with high probability. In the non-signaling setting, the assumption that $\mathcal{F}$ satisfies every constraint with high probability is typical, as for natural codes (e.g., Hadamard and Reed–Muller codes), $\mathcal{F}$ satisfying a *random* constraint α with high probability implies that its local correction satisfies *every* constraint $\alpha \in T$ with high probability.

A relation to shortest paths. We relate the local testability of $\mathbf{C}$ in the non-signaling setting to the (properly defined) length of shortest paths in the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$. Informally, we let $\mathsf{nsrank}_T(\alpha)$ denote the length of the shortest path from 0^n to α in the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$. We then show the following theorem, which is a robust analogue of Theorem 3.

Theorem 4 (informal)**.** *Let $T \subseteq \mathbf{C}^\perp$ be set of constraints each of weight at most k.*

1. *Suppose that a k-non-signaling function $\mathcal{F}$ satisfies every $\alpha \in T$ with probability at least $1 - \varepsilon$. Then $\mathcal{F}$ satisfies every α reachable from 0^n in $\Gamma_k(\mathbf{C}^\perp, T)$ with probability at least $1 - \mathsf{nsrank}_T(\alpha)\varepsilon$.*

2. *Conversely, there exists a k-non-signaling function $\mathcal{F}$ that satisfies every α reachable from 0^n in $\Gamma_k(\mathbf{C}^\perp, T)$ with probability exactly $1 - \mathrm{wt}(\alpha)\varepsilon$, and every other α with probability $\frac{1}{|\mathbb{F}|}$.*

We additionally show that $\mathsf{nsrank}_T(\alpha) \geq \mathrm{wt}(\alpha)/\mathrm{wt}(T)$ where $\mathrm{wt}(T) = \max_{\gamma \in T} \mathrm{wt}(\gamma)$, which shows that for any T the first statement is tight up to a factor of $\mathrm{wt}(T)$. In fact, we also show that if $\mathbf{C} = \{(b, \ldots, b) : b \in \mathbb{F}_2\}$ is the repetition code and $T = \{e_i + e_j : i, j \in [n]\}$ is the natural 2-local test, then $\mathsf{nsrank}_T(\alpha) = \mathrm{wt}(\alpha)/2$, showing that first statement is tight for some choice of $\mathbf{C}$. Finally, if $\mathbf{C}$ is the Hadamard code, then $\mathrm{wt}(\alpha)/3 \leq \mathsf{nsrank}_T(\alpha) \leq \mathrm{wt}(\alpha)$, implying that the first statement is tight up to a constant factor.

1.4 Roadmap

In Section 2 we provide an overview of the proofs of our results. Then, in Section 3 and Section 4 we formally define non-signaling functions, quasi-distributions, and discuss the relationship between them using Fourier analysis. In Section 5 and Section 6 we discuss what it means for a non-signaling function to "belong" to a given linear code, and characterize local characterizations for non-signaling linear codes using Cayley hypergraphs. In Section 7, we prove Theorem 1 as an application of Theorem 3. We finish the paper in Section 8 by discussing robust local characterizations of non-signaling functions and proving Theorem 4.

2 Techniques

We outline the techniques used to prove our results. We begin by explaining the Fourier structure of non-signaling functions in Section 2.1. This structure is fundamental to the proofs of our results. In Section 2.2 we outline our proof of the relationship between local characterizations and Cayley hypergraphs. In Section 2.3 we use the techniques and main theorem from Section 2.2 to show that the row/column test and the random lines test fail for non-signaling functions. Finally, in Section 2.4 we justify our definition of "**C**-explainability".

Notation. A k-non-signaling function $\mathcal{F}$ is defined by local distributions $\mathcal{F}_S$ for each $S \subseteq [n]$ with $|S| \leq k$. Because of this, when studying non-signaling functions we naturally encounter situations where we only consider subsets of a domain containing at most k elements, or vectors in $\mathbb{F}^n$ of weight at most k. We introduce notation to make referring to these notions more convenient. For a subset $S \subseteq [n]$ we write $S \subseteq [n]_{\leq k}$ if $|S| \leq k$. For a vector $\alpha \in \mathbb{F}^n$, we let $\mathrm{supp}(\alpha) = \{i \in [n] : \alpha_i \neq 0\}$ and $\mathrm{wt}(\alpha) = |\mathrm{supp}(\alpha)|$. For a set of vectors $R \subseteq \mathbb{F}^n$, we let $R_{\leq k} \subseteq R$ denote the subset $\{\alpha \in R : \mathrm{wt}(\alpha) \leq k\}$. In particular, $\mathbb{F}^n_{\leq k}$ denotes the set $\{\alpha \in \mathbb{F}^n : \mathrm{wt}(\alpha) \leq k\}$. For a subset $S \subseteq [n]$, we use similar notation and let $R_{\subseteq S} = \{\alpha \in R : \mathrm{supp}(\alpha) \subseteq S\}$.

2.1 The Fourier structure of non-signaling functions

We make frequent use of Fourier analysis to state and establish properties of non-signaling functions. Below we recall basic facts about Fourier analysis, explain their application to quasi-distributions, and state an equivalence between non-signaling functions and quasi-distributions. This equivalence motivates a definition for the Fourier spectrum of a non-signaling function.

Refresher on Fourier analysis. Let $\mathbb{F}$ be the finite field of size q with characteristic p, and $\mathbb{F}_p$ the prime subfield of $\mathbb{F}$. The inner product of $F_1, F_2 \colon \mathbb{F}^n \to \mathbb{C}$ is $\langle F_1, F_2 \rangle := \frac{1}{q^n} \sum_{f \in \mathbb{F}^n} \overline{F_1(f)} F_2(f)$. The *character* corresponding to $\alpha \in \mathbb{F}^n$ is the function $\chi_\alpha \colon \mathbb{F}^n \to \mathbb{C}$ defined as $\chi_\alpha(f) := \omega^{\mathrm{Tr}(\langle \alpha, f \rangle)}$ where: $\mathrm{Tr} \colon \mathbb{F} \to \mathbb{F}_p$ is the trace map; $\langle \alpha, f \rangle$ is the inner product $\sum_{i=1}^n \alpha_i f_i$; $\omega = e^{2\pi i/p}$ is a primitive complex p-th root of unity; and ω^j is defined by thinking of $j \in \mathbb{F}_p$ as an integer in $\{0, 1, \ldots, p-1\}$. The characters $\{\chi_\alpha\}_{\alpha \in \mathbb{F}^n}$ form an orthonormal basis of the space of all functions $F \colon \mathbb{F}^n \to \mathbb{C}$, so every function $F \colon \mathbb{F}^n \to \mathbb{C}$ can be written as

$$F(\cdot) = \sum_{\alpha \in \mathbb{F}^n} \widehat{F}(\alpha) \chi_\alpha(\cdot) \ , \text{ where } \widehat{F}(\alpha) := \langle \chi_\alpha, F \rangle \ .$$

The values $\{\widehat{F}(\alpha)\}_{\alpha \in \mathbb{F}^n}$ are called the *Fourier coefficients* of F.

Quasi-distributions. A *quasi-distribution* $\mathcal{Q}$ over functions $f \colon [n] \to \mathbb{F}$ is a distribution where the probability weights are complex numbers that "add up" to real probabilities. More formally, a quasi-distribution is a function $\mathcal{Q} \colon \mathbb{F}^n \to \mathbb{C}$ where $\sum_{f \in \mathbb{F}^n} \mathcal{Q}(f) = 1$. (We abuse notation and identify a function $f \colon [n] \to \mathbb{F}$ with the vector in $\mathbb{F}^n$ corresponding to its evaluation table.) We say that $\mathcal{Q}$ is *k-local* if the marginals $\mathcal{Q}|_S$ for each $S \subseteq [n]_{\leq k}$ are distributions, namely, if for each $S \subseteq [n]_{\leq k}$ and $g \colon S \to \mathbb{F}$ it holds that $\sum_{f \in \mathbb{F}^n : f|_S = g} \mathcal{Q}(f)$ is a non-negative real number. We can decompose a quasi-distribution $\mathcal{Q}$ according to the Fourier basis: we can write $\mathcal{Q}(f) = \sum_{\alpha \in \mathbb{F}^n} \widehat{\mathcal{Q}}(\alpha) \chi_\alpha(f)$, where $\{\chi_\alpha\}_{\alpha \in \mathbb{F}^n}$ are the characters and $\{\widehat{\mathcal{Q}}(\alpha)\}_{\alpha \in \mathbb{F}^n}$ are the Fourier coefficients of $\mathcal{Q}$.

Equivalence lemma. The following lemma shows that k-local quasi-distributions and k-non-signaling functions are equivalent, and exposes the Fourier structure of non-signaling functions.

Lemma 2.1. *A quasi-distribution $\mathcal{Q}$ is equivalent to a k-non-signaling function $\mathcal{F}$ if and only if for every $\alpha \in \mathbb{F}^n_{\leq k}$ it holds that $\widehat{\mathcal{Q}}(\alpha) = \frac{1}{q^n} \sum_{j \in \mathbb{F}_p} \omega^{-j} \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F} \rangle) = j]$, where the random variable $\langle \alpha, \mathcal{F} \rangle$ has the probability distribution given by*

$$\left\{ \Pr[\langle \alpha, \mathcal{F} \rangle = b] := \Pr_{f \leftarrow \mathcal{F}_{\mathrm{supp}(\alpha)}} \left[\sum_{i \in \mathrm{supp}(\alpha)} \alpha_i f(i) = b \right] \right\}_{b \in \mathbb{F}} .$$

The foregoing lemma motivates defining the Fourier coefficients of a k-non-signaling function $\mathcal{F}$ as follows: for every $\alpha \in \mathbb{F}^n$ with $\mathrm{wt}(\alpha) \leq k$ we define

$$\widehat{\mathcal{F}}(\alpha) := \frac{1}{q^n} \sum_{j \in \mathbb{F}_p} \omega^{-j} \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F} \rangle) = j] \ .$$

For more details on the above, including the proof of our Equivalence Lemma, see Section 4.

2.2 Local characterizations and Cayley hypergraphs

We outline the proof of Theorem 3; we assume familiarity with the notions introduced in Section 1.2. We begin by formally defining local characterizations and reachability in the Cayley hypergraph.

Local characterizations. We say that a k-non-signaling function $\mathcal{F}$ is $\mathbf{C}$-*explainable* if for every $S \subseteq [n]_{\leq k}$, with probability 1 the function $f \colon S \to \mathbb{F}$ sampled from $\mathcal{F}_S$ is in $\mathbf{C}|_S$. (See Section 2.4 for a discussion of this definition.) Recall from Definition 1.3 that a subset $T \subseteq \mathbf{C}^\perp$ is an ℓ-local characterization of $(\mathbf{C}, k)$ if every $\alpha \in T$ has $\mathrm{wt}(\alpha) \leq \ell$ and the set of k-non-signaling functions $\mathcal{F}$ where $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in T$ equals the set of $\mathbf{C}$-explainable k-non-signaling functions.

Reachability in Cayley hypergraph. In the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$ we write $T \vdash_k \alpha$ (using the symbol "$\vdash$" from mathematical logic) if α is reachable from 0^n in $\Gamma_k(\mathbf{C}^\perp, T)$. Reachability is defined recursively as follows:

1. (Base case) $T \vdash_k 0^n$.
2. (Edges) If (α, β) is an edge and $T \vdash_k \alpha$ then $T \vdash_k \beta$.
3. (Hyperedges) If $(\alpha, \beta, \alpha + \beta)$ is an edge and $T \vdash_k \{\alpha, \beta\}$, then $T \vdash_k \alpha + \beta$.

Outline of the proof. The proof of Theorem 3 has two directions. In one direction, we show that if $T \vdash_k \alpha$, then for any k-non-signaling function $\mathcal{F}$ where $\langle \gamma, \mathcal{F} \rangle = 0$ holds with probability 1 for every $\gamma \in T$, it also holds that $\langle \alpha, \mathcal{F} \rangle = 0$ with probability 1. Intuitively, this means that any k-non-signaling function satisfying every constraint in T must satisfy α as well. This step justifies Cayley hypergraphs as a way of capturing constraint propagation, and shows that our definition makes sense. The proof of this direction is straightforward, and can be found in Section 6.1.

In the other direction, we explicitly construct a k-non-signaling function $\mathcal{F}$ that satisfies every constraint α where $T \vdash_k \alpha$ with probability 1, and satisfies every other constraint α with probability $\frac{1}{|\mathbb{F}|}$. Our construction of $\mathcal{F}$ makes crucial use of the notion of a *local subspace* that we introduce.

Definition 2.2. *A* **k-local subspace** *$\mathcal{V}$ is a subset of $\mathbb{F}^n_{\leq k}$ that looks like a subspace when restricted to local views of size at most k, i.e., $\mathcal{V}_{\subseteq S}$ is a linear subspace in $\mathbb{F}^n$ for every $S \subseteq [n]_{\leq k}$.*

We show that for any k-local subspace $\mathcal{V}$ there is a k-non-signaling function $\mathcal{F}$ where $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathcal{V}$ and $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = \frac{1}{|\mathbb{F}|}$ otherwise. We then show that the set vertices reachable from 0^n, which is $\{\alpha \in \mathbb{F}^n_{\leq k} : T \vdash_k \alpha\}$, is a k-local subspace. This latter step is straightforward, and its proof is in Section 6.3. We now discuss the first step, which is non-trivial.

Non-signaling functions from local subspaces. Given a k-local subspace $\mathcal{V}$, we argue that there is a k-non-signaling function $\mathcal{F}$ where $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathcal{V}$, and $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = \frac{1}{|\mathbb{F}|}$ for every $\alpha \notin \mathcal{V}$. We construct $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq [n] : |S| \leq k}$ by specifying its local distributions $\mathcal{F}_S$.

A distribution over functions $f \colon S \to \mathbb{F}$ is a function that maps each f to a non-negative real number such that the total sum is 1. With this viewpoint, we first define $\mathcal{F}_S$ as a *function* that maps each $f \colon S \to \mathbb{F}$ to a complex number. Then, we show that the total sum is 1 and that each f is mapped to a non-negative real number, so that the function $\mathcal{F}_S$ is indeed a distribution.

We define the function $\mathcal{F}_S \colon \mathbb{F}^S \to \mathbb{C}$ by specifying its Fourier coefficients:

$$\widehat{\mathcal{F}_S}(\alpha) := \begin{cases} \frac{1}{q^{|S|}} & \text{if } \alpha \in \mathcal{V} \\ 0 & \text{if } \alpha \notin \mathcal{V} \end{cases} ,$$

These "local" Fourier coefficients should *not* be confused with the Fourier coefficients of $\mathcal{F}$ that are defined in Section 2.1. In fact, at this point the non-signaling function $\mathcal{F}$ is not yet defined.

This completely specifies $\mathcal{F}_S$ as a function $\mathbb{F}^S \to \mathbb{C}$. We show that since $\mathcal{V}$ is a k-local subspace, $\mathcal{F}_S$ is in fact a distribution. First, $\sum_{f \in \mathbb{F}^S} \mathcal{F}_S(f) = 1$ because $\widehat{\mathcal{F}_S}(0^S) = 1/q^{|S|}$ since $\mathcal{V}$ is a k-local subspace, and thus must contain 0^n. Hence, it suffices to show that $\mathcal{F}_S(f) \in \mathbb{R}_{\geq 0}$ for each $f \in \mathbb{F}^S$. For each $f \in \mathbb{F}^S$ we have

$$\mathcal{F}_S(f) = \sum_{\alpha \in \mathbb{F}^S} \widehat{\mathcal{F}_S}(\alpha) \chi_\alpha(f) = \sum_{\alpha \in \mathcal{V}_{\subseteq S}} \widehat{\mathcal{F}_S}(\alpha) \chi_\alpha(f) \ ,$$

since we have defined $\mathcal{F}_S$ in this way using its Fourier coefficients. There are two cases: either $\langle \alpha, f \rangle = 0$ for every $\alpha \in \mathcal{V}_{\subseteq S}$, in which case the sum is $|\mathcal{V}_{\subseteq S}|/q^{|S|}$, or $\langle \alpha, f \rangle \neq 0$ for some $\alpha \in \mathcal{V}_{\subseteq S}$. In the latter case, we use the fact that $\mathcal{V}_{\subseteq S}$ is a linear subspace to show that the sum is 0. In either case, we conclude that $\mathcal{F}_S(f)$ is a non-negative real number, and therefore that $\mathcal{F}_S$ is a distribution.

Next, we argue that the collection of local distributions $\{\mathcal{F}_S\}_{S \subseteq [n]_{\leq k}}$ is indeed non-signaling. This follows from a lemma that we prove that shows that a collection of local distributions is non-signaling if and only if the Fourier coefficients of the local distributions (after removing the normalization factors) are the same. Thus the k-non-signaling function $\mathcal{F}$ is well-defined.

Finally, we show that $\mathcal{F}$ satisfies the desired properties. This follows from our definition of each $\mathcal{F}_S$, as the construction implies that the Fourier coefficients of $\mathcal{F}$ satisfy:

$$\widehat{\mathcal{F}}(\alpha) := \begin{cases} \frac{1}{q^n} & \text{if } \alpha \in \mathcal{V} \\ 0 & \text{if } \alpha \notin \mathcal{V} \end{cases} .$$

This corresponds to having $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathcal{V}$, and the random variable $\langle \alpha, \mathcal{F} \rangle$ having the uniform distribution when $\alpha \notin \mathcal{V}$, which completes the proof.

On robust local characterizations. We discuss the proof of Theorem 4 only briefly, because it builds on the above ideas for (exact) local characterizations.

The first part of Theorem 4 is straightforward and follows from the definition of $\mathsf{nsrank}_T(\alpha)$, which is the length of the shortest path from 0^n to α in the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$. This connection motivates nsrank as a non-signaling analogue of rank, as $\mathsf{rank}_T(\alpha)$ is the length of the shortest path from 0^n to α in the Cayley graph $G(\mathbf{C}^\perp, T)$. (We discuss rank more in Section 2.3.)

The second part of Theorem 4 is more complicated, but informally follows a similar outline to how we construct a non-signaling function $\mathcal{F}$ in the above proof. The step showing that $\mathcal{F}_S(f) \geq 0$

for every $f \in \mathbb{F}^S$ is now more challenging as the Fourier coefficients are no longer either $\frac{1}{q^{|S|}}$ or 0, but this can still be done under the conditions of the theorem statement.

The proof of Theorem 4 can be found in Section 8.

2.3 Non-testability of bivariate polynomials

We discuss how to derive the negative results on bivariate low-degree testing discussed in Section 1.1. First we focus on the case of the row/column test (for individual degree d), and then we explain how to modify the proof to work for the random lines test (for total degree d).

We let $\mathbf{C}$ denote the linear code of bivariate functions $f\colon \mathbb{F}^2 \to \mathbb{F}$ of degree at most d in each variable, and let T be the constraints of the row/column test (it consists of $\alpha \in \mathbf{C}^\perp$ whose support is contained in exactly one row or column). The main combinatorial quantity that we use in our proof is the *rank* of an element $\alpha \in \mathbf{C}^\perp$, defined as

$$\mathsf{rank}_T(\alpha) := \min_{T' \subseteq T : \alpha \in \mathrm{span}(T')} \left|T'\right| \quad .$$

Note that $\mathsf{rank}_T(\alpha)$ is a non-negative integer, as $\mathrm{span}(T) = \mathbf{C}^\perp$.

We now sketch the proof of Theorem 1 in three steps.

(1) Interval Cut Lemma. We show a generic lemma about the relationship between rank and reachability in the Cayley hypergraph $\Gamma_k(\mathbf{C}^\perp, T)$. Informally, we show that in order to reach some α of rank at least r from 0^n, one must first reach some β of "intermediate" rank. Formally, we show that if there is an interval $[r/2, r)$ such that every β with rank in this interval is *not* reachable from 0^n, then every α of rank at least r is also not reachable from 0^n. We prove this *Interval Cut Lemma* via the fact that rank_T is subadditive, that is, $\mathsf{rank}_T(\alpha+\beta) \le \mathsf{rank}_T(\alpha) + \mathsf{rank}_T(\beta)$. Subadditivity implies that for every interval $[r/2, r)$, in order to reach a vertex of rank $\ge r$ from vertices of rank $< r/2$ there must be an intermediate vertex β with rank in $[r/2, r)$ bridging the gap.

(2) Two combinatorial facts. We prove two combinatorial facts about the dual code of $\mathbf{C}$.

- There exists $\alpha^* \in \mathbf{C}^\perp$ where $\mathrm{wt}(\alpha) = 2d+2$ and $\mathrm{supp}(\alpha) \subseteq \{(a,a) : a \in \mathbb{F}\} \subseteq \mathbb{F}^{n \times n}$, i.e., $\mathrm{supp}(\alpha)$ is contained in the diagonal of $\mathbb{F}^{n\times n}$.

  Proof sketch. Any bivariate polynomial of individual degree d is a polynomial of degree $\le 2d$ on the diagonal. Thus, there is an element $\alpha^* \in \mathbf{C}^\perp$ supported on the diagonal of weight $2d+2$ that checks this constraint. This shows the existence of the desired α^*.

- For every $\beta \in \mathbf{C}^\perp$ with $\mathsf{rank}_T(\beta) \in \{(d+2)/4, \ldots, (d+2)/2\}$ it holds that $\mathrm{wt}(\beta) \ge \frac{7}{32}(d+2)^2$.

  Proof sketch. Any β of rank r is the sum of *exactly* r row/column constraints, where each constraint is on a *distinct* row/column. Each new constraint adds at least $d+2$ weight to β, ignoring the weight that is removed by cancellation. The amount of cancellation is at most the number of intersection points, which is not too large when r is in $\{(d+2)/4, \ldots, (d+2)/2\}$, thus implying that $\mathrm{wt}(\beta) \ge \frac{7}{32}(d+2)^2$.

(3) Completing the proof. Theorem 1 follows from the Interval Cut Lemma, the two combinatorial facts, and Theorem 3. Any $\beta \in \mathbf{C}^\perp$ with rank in $[(d+2)/4, (d+2)/2)$ has weight $\ge \frac{7}{32}(d+2)^2$, and thus is *not* reachable when $k < \frac{7}{32}(d+2)^2$. Since α^* has weight $2d+2$ and is supported only on the diagonal, it has rank $\ge 2d+2$, as each row/column constraint increases the number of points on the diagonal by at most 1. The Interval Cut Lemma implies that α^* is also not reachable. The

non-signaling function constructed in the proof of Theorem 3 thus passes the row/column test with probability 1 yet satisfies α^* with probability only $1/|\mathbb{F}|$. But, α^* must be satisfied with probability 1 by any non-signaling function that is "locally low-degree", which completes the proof.

The case of the random lines test. In order to prove Theorem 2, which is the analogous statement for the random lines test, it suffices to show that analogues of the combinatorial statements stated for bivariate polynomials of *individual* degree d hold for bivariate polynomials of *total* degree d. Rather than choosing α^* to be a constraint on the diagonal (which is now easily reachable when T contains all lines), we show that there is a constraint α^* of weight $2d+2$ that is supported on an *irreducible quadratic curve* in $\mathbb{F}^2$. This constraint has rank $\geq d+1$ as any line intersects the curve in at most 2 distinct points. The proof that every $\beta \in \mathbf{C}^\perp$ with $\mathsf{rank}_T(\beta) \in \{(d+2)/4, \ldots, (d+2)/2\}$ has large weight is almost identical in this setting, and this completes the proof.

2.4 Fourier spectrum of non-signaling linear codes

We have so far adopted the definition that a k-non-signaling function $\mathcal{F}$ is "in" a linear code $\mathbf{C} \subseteq \mathbb{F}^n$ if a function $f\colon S \to \mathbb{F}$ sampled from $\mathcal{F}_S$ is in $\mathbf{C}|_S$ with probability 1 for every $S \subseteq [n]_{\leq k}$. Indeed, we use this "$\mathbf{C}$-explainability" to define the notion of a *local characterization* (see Definition 1.3).

We now provide thorough justification for this choice. We view the definitions and results below as a conceptual contribution that sheds light on basic properties of non-signaling functions.

In the classical setting, a function $f\colon [n] \to \mathbb{F}$ "looks like" a codeword of $\mathbf{C}$ if, well, it equals some codeword in $\mathbf{C}$. The issue at hand is that, in the non-signaling setting, it is not immediately clear what it means for a non-signaling function $\mathcal{F}$ to be "in" $\mathbf{C}$ because $\mathcal{F}$ is a collection of local distributions. Below are two natural ways to capture this notion.

Definition 2.3 (informal)**.** *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function.*

- *We say that $\mathcal{F}$ is* **C-supported** *if it is equivalent to a k-local quasi-distribution $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ that is supported on $\mathbf{C}$, namely, $\mathcal{Q}(f) = 0$ for all $f \notin \mathbf{C}$.*[3]
- *We say that $\mathcal{F}$ is* **C-explainable** *if, for all $S \subseteq [n]_{\leq k}$, the distribution $\mathcal{F}_S$ is supported on $\mathbf{C}|_S$. In other words, the output of $\mathcal{F}$ is always consistent with the restriction of some codeword in $\mathbf{C}$.*

The first definition is motivated by our Equivalence Lemma (Lemma 2.1), and imposes a "global" property on the non-signaling function. The second definition, implied by the first one, instead takes a "local" approach, imposing consistency with relevant restrictions of the code.

In the following lemma, we quantify the difference between the notions of "$\mathbf{C}$-supported" and "$\mathbf{C}$-explainable" by characterizing the Fourier spectrum in each case. For convenience, we denote by $\mathbf{C}^\perp_{\leq k}$ the set $\{\alpha \in \mathbf{C}^\perp : \mathrm{wt}(\alpha) \leq k\}$, which are the constraints with at most k non-zero entries.

Lemma 2.4 (informal)**.** *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function.*

- *$\mathcal{F}$ is $\mathbf{C}$-supported $\leftrightarrow$ the Fourier coefficients $\{\widehat{\mathcal{F}}(\alpha)\}_{\alpha \in \mathbb{F}^n_{\leq k}}$ are constant on each coset of $\mathbf{C}^\perp$.*
- *$\mathcal{F}$ is $\mathbf{C}$-explainable $\leftrightarrow$ the Fourier coefficient $\widehat{\mathcal{F}}(\alpha)$ equals $\frac{1}{q^n}$ for every $\alpha \in \mathbf{C}^\perp_{\leq k}$.*

We additionally prove that the foregoing structure is robust to errors: $\mathcal{F}$ is close to being $\mathbf{C}$-supported if and only if its Fourier coefficients are almost constant on every coset of $\mathbf{C}^\perp$; moreover $\mathcal{F}$ is close to being $\mathbf{C}$-explainable if and only if $\widehat{\mathcal{F}}(\alpha)$ is close to $\frac{1}{q^n}$ for every $\alpha \in \mathbf{C}^\perp_{\leq k}$.

[3] When $\mathbf{C}$ is the Hadamard code, this definition equals the notion of a *linear* non-signaling function from [CMS18].

One may interpret Lemma 2.4 as "bad news" because it shows that the notions of "**C**-supported" and "**C**-explainable" are in fact *distinct*. Which one is the correct one to use? From the perspective of local testability, we may regard "**C**-supported" as more desirable, because it requires a global structure to hold. We prove that, fortunately, the two notions are equivalent up to a small change in parameters, reinforcing our belief that we have identified the right notions.

Lemma 2.5 (informal)**.** *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function.*

- *If $\mathcal{F}$ is **C**-supported, then $\mathcal{F}$ is **C**-explainable.*
- *If $\mathcal{F}$ is **C**-explainable, then $\mathcal{F}$ (viewed as a $k/2$-non-signaling function) is **C**-supported.*

In light of the above, it suffices to study non-signaling functions that are **C**-explainable. We have used this notion in our results on local characterizations (see Definition 1.3), as it is more natural in this setting: the set of **C**-explainable k-non-signaling functions are precisely those that are consistent with the set of constraints $\mathbf{C}^{\perp}_{\leq k}$.

Detailed definitions and proofs can be found in Section 5. Below we provide proof sketches for Lemmas 2.4 and 2.5. The Fourier structure of non-signaling functions, discussed in Section 2.1, underlies all of these proofs.

2.4.1 Fourier spectrum of a C-supported function

We outline the proof of the first item of Lemma 2.4. A k-non-signaling function $\mathcal{F}$ that is **C**-supported is by definition equivalent to a quasi-distribution $\mathcal{Q}$ supported on **C**. We explain why all such non-signaling functions have Fourier coefficients that are constant on cosets of $\mathbf{C}^{\perp}$, that is, $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{F}}(\alpha')$ for every $\alpha, \alpha' \in \mathbb{F}^n_{\leq k}$ with $\alpha - \alpha' \in \mathbf{C}^{\perp}$. We compare the following two affine spaces:

$$V_1 = \left\{ \mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C} \text{ s.t. } \sum_{f \in \mathbf{C}} \mathcal{Q}(f) = 1 \text{ and } \mathcal{Q}(f) = 0 \ \forall f \notin \mathbf{C} \right\} ,$$

$$V_2 = \left\{ \mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C} \text{ s.t. } \widehat{\mathcal{Q}}(0^n) = \frac{1}{q^n} \text{ and } \widehat{\mathcal{Q}}(\alpha) = \widehat{\mathcal{Q}}(\alpha + \gamma) \ \forall \alpha \in \mathbb{F}^n, \gamma \in \mathbf{C}^{\perp} \right\} .$$

The affine space V_1 corresponds to quasi-distributions that are supported on **C**, while V_2 corresponds to quasi-distributions whose Fourier coefficients satisfy the desired characterization. It suffices to prove that $V_1 = V_2$. First we show that $\dim(V_1) = \dim(V_2)$, and then that $V_1 \subseteq V_2$.

The dimension of V_1 is $|\mathbf{C}| - 1$ because the $|\mathbf{C}|$ free terms are subject to a single linear constraint. The dimension of V_2 is $q^n / \left|\mathbf{C}^{\perp}\right| - 1$ because the Fourier coefficients are constant on each coset of $\mathbf{C}^{\perp}$, and on each coset they may have an arbitrary value; the one exception is the coset $\mathbf{C}^{\perp}$, where the Fourier coefficients must be $\frac{1}{q^n}$. Recalling that $q^n = |\mathbf{C}| \cdot \left|\mathbf{C}^{\perp}\right|$, we deduce that $\dim(V_1) = \dim(V_2)$.

Next we show that $V_1 \subseteq V_2$. For any $\mathcal{Q} \in V_1$ and $\alpha \in \mathbb{F}^n$ we have by definition

$$\widehat{\mathcal{Q}}(\alpha) := \frac{1}{q^n} \cdot \sum_{f \in \mathbb{F}^n} \mathcal{Q}(f) \cdot \omega^{-\mathrm{Tr}(\langle \alpha, f \rangle)} .$$

Since $\mathcal{Q} \in V_1$, any function f in the support of $\mathcal{Q}$ must be in **C**. Therefore, for any $\gamma \in \mathbf{C}^{\perp}$ have $\langle \gamma, f \rangle = 0$, so that $\omega^{\mathrm{Tr}(\langle \gamma, f \rangle)} = \omega^{\mathrm{Tr}(0)} = 1$. This implies that $\widehat{\mathcal{Q}}(\alpha) = \widehat{\mathcal{Q}}(\alpha + \gamma)$. Intuitively, when we shift α by γ the sum remains unchanged because each term in the sum is multiplied by $\omega^{-\mathrm{Tr}(\langle \gamma, f \rangle)} = 1$. Thus $V_1 \subseteq V_2$. Since $\dim(V_1) = \dim(V_2)$ and $V_1 \subseteq V_2$, we conclude that $V_1 = V_2$.

2.4.2 Fourier spectrum of a C-explainable function

We outline the proof of the second item of Lemma 2.4. The characterization of **C**-explainable functions relies on the fact that the Fourier coefficient $\widehat{\mathcal{F}}(\alpha)$ is related to the distribution of the random variable $\langle \alpha, \mathcal{F} \rangle$, i.e., the distribution $(\Pr[\langle \alpha, \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$. This intuition can be quantified via (a generalization of) the DFT matrix $M \in \mathbb{C}^{q \times q}$, which is the matrix defined as $M_{a,b} := \omega^{-\mathrm{Tr}(ab)}$ (entries are indexed by $\mathbb{F}$); M is invertible and $\frac{1}{\sqrt{q}} M$ is unitary.

Recall that the Fourier coefficients of $\mathcal{F}$ are defined as follows:

$$\forall\, \alpha \in \mathbb{F}^n_{\leq k} \quad \widehat{\mathcal{F}}(\alpha) := \frac{1}{q^n} \sum_{j \in \mathbb{F}_p} \omega^{-j} \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F} \rangle) = j] \ .$$

Letting $v := (\Pr[\langle \alpha, \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$, expanding the definitions shows that $Mv = (q^n \widehat{\mathcal{F}}(a\alpha))_{a \in \mathbb{F}}$. The linear transformation M thus quantifies the relation between the distribution $(\Pr[\langle \alpha, \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$ and the Fourier coefficients $(q^n \widehat{\mathcal{F}}(a\alpha))_{a \in \mathbb{F}}$.

Now, given a k-non-signaling function $\mathcal{F}$, we first show that $\mathcal{F}$ is **C**-explainable if and only if $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathbf{C}^\perp_{\leq k}$. This follows from the fact that any local function $g \colon S \to \mathbb{F}$ that satisfies every $\alpha \in \mathbf{C}^\perp_{\subseteq S}$ can be extended into a codeword $f \in \mathbf{C}$. Using the matrix M, we can relate the condition that $\mathcal{F}$ satisfies every $\alpha \in \mathbf{C}^\perp_{\leq k}$ with probability 1 to its Fourier spectrum. Specifically, we have that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ if and only if $(q^n \widehat{\mathcal{F}}(a\alpha))_{a \in \mathbb{F}} = M(1, 0, \ldots, 0)^\top$. Since $M(1, 0, \ldots, 0)^\top = (1, \ldots, 1)^\top$, we get that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ if and only if $\widehat{\mathcal{F}}(a\alpha) = \frac{1}{q^n}$ for every $a \in \mathbb{F}$, completing the proof.

2.4.3 The relationship between C-supported and C-explainable

We outline the proof of Lemma 2.5. First note that Lemma 2.4 immediately implies that a **C**-supported k-non-signaling function $\mathcal{F}$ is **C**-explainable, because if $\mathcal{F}$ is **C**-supported then $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{F}}(0^n) = \frac{1}{q^n}$ for every $\alpha \in \mathbf{C}^\perp_{\leq k}$, implying that $\mathcal{F}$ is **C**-explainable.

Conversely, if $\mathcal{F}$ is **C**-explainable, then for any $\alpha, \alpha' \in \mathbb{F}^n_{\leq k/2}$ with $\alpha - \alpha' \in \mathbf{C}^\perp$ we get that for any $b \in \mathbb{F}$,

$$\Pr[\langle \alpha, \mathcal{F} \rangle = b] = \Pr[\langle \alpha', \mathcal{F} \rangle + \langle \alpha - \alpha', \mathcal{F} \rangle = b] = \Pr[\langle \alpha', \mathcal{F} \rangle = b] \ ,$$

since $\Pr[\langle \alpha - \alpha', \mathcal{F} \rangle = 0] = 1$ as $\alpha - \alpha' \in \mathbf{C}^\perp$ and $\mathcal{F}$ is **C**-explainable. This shows that the vectors $(\Pr[\langle \alpha, \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$ and $(\Pr[\langle \alpha', \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$ are equal, which implies that the Fourier coefficients $\widehat{\mathcal{F}}(\alpha)$ and $\widehat{\mathcal{F}}(\alpha')$ are equal. By Lemma 2.4, this completes the proof. Note that we crucially need $\mathrm{wt}(\alpha), \mathrm{wt}(\alpha') \leq k/2$ so that $\mathrm{wt}(\alpha - \alpha') \leq k$, as otherwise $\Pr[\langle \alpha - \alpha', \mathcal{F} \rangle = 0]$ is undefined.

3 Preliminaries

Throughout this paper we let $n \in \mathbb{N}$ be an arbitrary positive integer, and $k \in \mathbb{N}$ a positive integer that is at most n. We use $\mathbb{F}$ to denote the finite field of size q with characteristic p, and $\mathbb{F}_p$ to denote the prime subfield of $\mathbb{F}$. We often abuse notation and identify a function $f\colon [n] \to \mathbb{F}$ with its evaluation table in $\mathbb{F}^n$. For a vector $\alpha \in \mathbb{F}^n$ we let $\mathrm{supp}(\alpha) := \{i \in [n] : \alpha_i \neq 0\}$, and we let $\mathrm{wt}(\alpha) := |\mathrm{supp}(\alpha)|$. For a set of vectors $R \subseteq \mathbb{F}^n$, we let $R_{\leq \ell} \subseteq R$ denote the subset $\{\alpha \in R : \mathrm{wt}(\alpha) \leq \ell\}$. In particular, $\mathbb{F}^n_{\leq k}$ contains all vectors $\alpha \in \mathbb{F}^n$ of weight at most k. For a subset $S \subseteq [n]$, we let $R_{\subseteq S} = \{\alpha \in R : \mathrm{supp}(\alpha) \subseteq S\}$; we also write $S \subseteq [n]_{\leq \ell}$ if $|S| \leq \ell$.

3.1 Non-signaling functions

We define *non-signaling functions* and *quasi-distributions*, and introduce useful notation for them. The definitions are almost identical to those in [CMS18], but extended to any finite field.

Definition 3.1. *A k-non-signaling function $\mathcal{F}\colon [n] \to \mathbb{F}$ is a collection $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq [n]_{\leq k}}$ where (i) each $\mathcal{F}_S$ is a distribution over functions $f\colon S \to \mathbb{F}$, and (ii) for every two subsets S and R each of size at most k, the restrictions of $\mathcal{F}_S$ and $\mathcal{F}_R$ to $S \cap R$ are equal as distributions. (If $S = \emptyset$ then $\mathcal{F}_S$ always outputs the empty string.)*

Note that any function $f\colon [n] \to \mathbb{F}$ induces a n-non-signaling function by setting $\mathcal{F}_S$ to be the distribution that outputs $f|_S$ with probability 1. More generally, any distribution $\mathcal{D}$ over functions $f\colon [n] \to \mathbb{F}$ induces a corresponding n-non-signaling function by defining $\mathcal{F}_S$ to be the distribution that samples $f \leftarrow \mathcal{D}$ and outputs $f|_S$.

Given a set $S \subseteq [n]_{\leq k}$ and function $g \in \mathbb{F}^S$, we define

$$\Pr[\,\mathcal{F}(S) = g\,] := \Pr[\,g \leftarrow \mathcal{F}_S\,]\ .$$

The non-signaling property in this notation is the following: for every two subsets $S, R \subseteq [n]_{\leq k}$ and every string $g \in \mathbb{F}^{S \cap T}$, $\Pr[\,\mathcal{F}(S)|_{S\cap T} = g\,] = \Pr[\,\mathcal{F}(T)|_{S\cap T} = g\,]$, where the probability is over the randomness of $\mathcal{F}$.

We extend the above notation to every $E \subseteq \mathbb{F}^S$ in the natural way by defining $\Pr[\,\mathcal{F}(S) \in E\,] := \Pr_{f \leftarrow \mathcal{F}_S}[\,f \in E\,]$. We highlight the case when E is an "inner product event", as we will encounter this case frequently.

Definition 3.2. *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function. For $\alpha \in \mathbb{F}^n_{\leq k}$ and $b \in \mathbb{F}$, we define*

$$\Pr[\langle \alpha, \mathcal{F}\rangle = b] := \Pr_{f \leftarrow \mathcal{F}_{\mathrm{supp}(\alpha)}}\left[\sum_{i \in \mathrm{supp}(\alpha)} \alpha_i f(i) = b\right]\ .$$

Similarly, we define $\Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F}\rangle) = j] := \sum_{b \in \mathbb{F}:\mathrm{Tr}(b)=j} \Pr[\langle \alpha, \mathcal{F}\rangle = b]$ for every $j \in \mathbb{F}_p$.

The probability above is well-defined since $\mathrm{wt}(\alpha) \leq k$, and so we query $\mathcal{F}$ on at most k points.

Since $\mathcal{F}$ is non-signaling, $\Pr[\langle \alpha, \mathcal{F}\rangle = b] = \Pr_{f \leftarrow \mathcal{F}_S}[\sum_{i \in S} \alpha_i f(i)]$ for any set $S \supseteq \mathrm{supp}(\alpha)$. The intuition behind the above definition is that the inner product $\langle \alpha, g\rangle$ for any $g\colon [n] \to \mathbb{F}$ can be computed only given $g|_{\mathrm{supp}(\alpha)}$, namely, given g restricted to a set of size at most k.

3.2 Quasi-distributions

A quasi-distribution extends the notion of a probability distribution by allowing probabilities to be complex, and is the main tool that we use to analyze non-signaling functions.

Definition 3.3.
- *A* **quasi-distribution** *is a function* $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ *where* $\sum_{f\in\mathbb{F}^n} \mathcal{Q}(f) = 1$.
- *For a set of functions* $R \subseteq \mathbb{F}^n$*, we say that* $\mathcal{Q}$ *is* **supported** *on* R *if* $\{f \in \mathbb{F}^n : \mathcal{Q}(f) \neq 0\} \subseteq R$.
- *For a positive integer* ℓ*, we say that* $\mathcal{Q}$ *is* ℓ**-local** *if the marginals* $\mathcal{Q}|_S$ *for each* $S \subseteq [n]_{\leq \ell}$ *are distributions (*$\sum_{f\in\mathbb{F}^n : f|_S = g} \mathcal{Q}(f)$ *is a non-negative real number for each* $S \subseteq [n]_{\leq\ell}$ *and* $g\colon S \to \mathbb{F}$*).*

If $\mathcal{Q}$ is ℓ-local, then for every subset $S \subseteq [n]_{\leq\ell}$, we may view $\mathcal{Q}|_S$ as a probability distribution over $\mathbb{F}^S$. If $\mathcal{Q}$ is ℓ-local then it is s-local for every $s \in \{0, 1, \ldots, \ell\}$.

Definition 3.4. *Given a quasi-distribution* $\mathcal{Q}$*, a subset* $S \subseteq [n]$*, and* $g \in \mathbb{F}^S$*, we define the* **quasi-probability** *of the event "*$\mathcal{Q}(S) = g$*" to be the following complex number*

$$\widetilde{\Pr}[\mathcal{Q}(S) = g\,] := \sum_{f\in\mathbb{F}^n : f|_S = g} \mathcal{Q}(f)\ .$$

(The tilde above Pr *denotes that quasi-probabilities are not necessarily non-negative real numbers.)*

Given a subset $E \subseteq \mathbb{F}^S$, we similarly define $\widetilde{\Pr}[\mathcal{Q}(S) \in E\,] := \sum_{f\in\mathbb{F}^n : f|_S \in E} \mathcal{Q}(f)$.

As for non-signaling functions, we highlight the case when E is an inner product event.

Definition 3.5. *Let* $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ *be a quasi-distribution. For* $\alpha \in \mathbb{F}^n$ *and* $b \in \mathbb{F}$*, we define*

$$\widetilde{\Pr}[\langle \alpha, \mathcal{Q}\rangle = b] := \sum_{f\in\mathbb{F}^n : \langle\alpha, f\rangle = b} \mathcal{Q}(f)\ .$$

Similarly, we define $\widetilde{\Pr}[\mathrm{Tr}(\langle \alpha, \mathcal{Q}\rangle) = j] := \sum_{b\in\mathbb{F}:\mathrm{Tr}(b)=j} \widetilde{\Pr}[\langle \alpha, \mathcal{Q}\rangle = b]$ *for every* $j \in \mathbb{F}_p$.

Definition 3.6 (statistical distance)**.** *Given a finite domain* $[n]$ *and an integer* $\ell \in \{1, \ldots, |D|\}$*, the* Δ_ℓ**-distance** *between two quasi-distributions* $\mathcal{Q}$ *and* $\mathcal{Q}'$ *is*

$$\Delta_\ell(\mathcal{Q}, \mathcal{Q}') := \max_{S\subseteq[n]_{\leq\ell}} \Delta(\mathcal{Q}|_S, \mathcal{Q}'|_S)\ ,$$

where $\Delta(\mathcal{Q}|_S, \mathcal{Q}'|_S) := \max_{E\subseteq\mathbb{F}^S} \left|\widetilde{\Pr}[\mathcal{Q}(S) \in E] - \widetilde{\Pr}[\mathcal{Q}'(S) \in E]\right|$.

We say that $\mathcal{Q}$ *and* $\mathcal{Q}'$ *are* ε**-close in the** Δ_ℓ**-distance** *if* $\Delta_\ell(\mathcal{Q}, \mathcal{Q}') \leq \varepsilon$*; else, they are* ε*-far.*

Remark 3.7 (distance for non-signaling functions)**.** The definition of Δ_ℓ-distance naturally extends to defining distances between k-non-signaling functions, as well as between quasi-distributions and k-non-signaling functions, provided that $\ell \leq k$.

The notion above generalizes the standard notion of statistical (total variation) distance: if $\mathcal{Q}$ and $\mathcal{Q}'$ are *distributions* then their Δ_n-distance equals their statistical distance. Also note that if $\mathcal{Q}$ and $\mathcal{Q}'$ are ℓ-local quasi-distributions then their Δ_ℓ-distance equals the maximum statistical distance, across all subsets $S \subseteq [n]$ with $|S| \leq \ell$, between the two *distributions* $\mathcal{Q}|_S$ and $\mathcal{Q}'|_S$ — in particular this means that any experiment that queries exactly one set of size at most ℓ cannot distinguish between the two quasi-distributions with probability greater than $\Delta_\ell(\mathcal{Q}, \mathcal{Q}')$.

We stress that $\Delta_\ell(\mathcal{Q}, \mathcal{Q}') = 0$ does *not* necessarily mean that $\mathcal{Q} = \mathcal{Q}'$! In fact, it is possible to have $\Delta_\ell(\mathcal{Q}, \mathcal{Q}') = 0$ while $\sum_{f\in U} |\mathcal{Q}(f) - \mathcal{Q}'(f)|$ is arbitrarily large. We also remark that the Δ_ℓ-distance is not necessarily upper bounded by 1, and is in general unbounded.

4 Fourier analysis of non-signaling functions

We prove statements about the Fourier structure of non-signaling functions, and prove the Equivalence Lemma. In Section 4.1 we recall basic facts about Fourier analysis of functions over finite fields. In Section 4.2 we relate Fourier coefficients to probabilities and quasi-probabilities. In Section 4.3 we prove that non-signaling functions and quasi-distributions are equivalent notions.

4.1 Fourier analysis of functions over finite fields

We consider functions of the type $F\colon \mathbb{F}^n \to \mathbb{C}$. For two such functions F_1 and F_2, we define their inner product as $\langle F_1, F_2 \rangle := \frac{1}{q^n} \sum_{x \in \mathbb{F}^n} \overline{F_1(x)} F_2(x)$. For every $\alpha \in \mathbb{F}^n$, we define the *character* $\chi_\alpha\colon \mathbb{F}^n \to \mathbb{C}$ as $\chi_\alpha(x) := \omega^{\mathrm{Tr}(\langle \alpha, x \rangle)}$ where: (1) $\mathrm{Tr}\colon \mathbb{F} \to \mathbb{F}_p$ is the trace map; (2) $\langle \alpha, x \rangle$ is the inner product $\sum_{i=1}^n \alpha_i x_i$; (3) $\omega = e^{2\pi i/p}$ is a primitive complex p-th root of unity; and (4) ω^j is defined by thinking of $j \in \mathbb{F}_p$ as an integer in $\mathbb{Z}$. The functions $\{\chi_\alpha\}_{\alpha \in \mathbb{F}^n}$ form an orthonormal basis of the space of all functions $f\colon \mathbb{F}^n \to \mathbb{C}$, so every function $F\colon \mathbb{F}^n \to \mathbb{C}$ can be written as

$$F(\cdot) = \sum_{\alpha \in \mathbb{F}^n} \widehat{F}(\alpha) \chi_\alpha(\cdot) \ , \text{ where } \widehat{F}(\alpha) := \langle \chi_\alpha, F \rangle \ .$$

The values $\{\widehat{F}(\alpha)\}_{\alpha \in \mathbb{F}^n}$ are the *Fourier coefficients* of F. We recall and prove a few useful identifies.

Parseval's identity. For every two functions $F, G\colon \mathbb{F}^n \to \mathbb{C}$,

$$\langle F, G \rangle = \frac{1}{q^n} \sum_{x \in \mathbb{F}^n} \overline{F(x)} G(x) = \sum_{\alpha \in \mathbb{F}^n} \overline{\widehat{F}(\alpha)} \widehat{G}(\alpha) \ .$$

Proof.

$$\begin{aligned} \frac{1}{q^n} \sum_{x \in \mathbb{F}^n} \overline{F(x)} G(x) &= \frac{1}{q^n} \sum_{x \in \mathbb{F}^n} \overline{\left(\sum_{\alpha \in \mathbb{F}^n} \widehat{F}(\alpha) \chi_\alpha(x) \right)} \left(\sum_{\beta \in \mathbb{F}^n} \widehat{G}(\beta) \chi_\beta(x) \right) \\ &= \sum_{\alpha \in \mathbb{F}^n} \sum_{\beta \in \mathbb{F}^n} \overline{\widehat{F}(\alpha)} \widehat{G}(\beta) \langle \chi_\alpha, \chi_\beta \rangle = \sum_{\alpha \in \mathbb{F}^n} \overline{\widehat{F}(\alpha)} \widehat{G}(\alpha) \ , \end{aligned}$$

since $\{\chi_\alpha\}_{\alpha \in \mathbb{F}^n}$ are orthonormal. □

Plancherel's identity. As a corollary of the above,

$$\frac{1}{q^n} \sum_{x \in \mathbb{F}^n} |F(x)|^2 = \sum_{\alpha \in \mathbb{F}^n} |\widehat{F}(\alpha)|^2 \ .$$

The case of indicator functions. When analyzing non-signaling functions and quasi-distributions we will apply the above identities in the case where F is an indicator function $\mathbf{1}_E$ for a set $E \subseteq \mathbb{F}^n$. In this case, by Plancherel's identity we have that $|E|/q^n = \sum_{\alpha \in \mathbb{F}^n} |\widehat{\mathbf{1}_E}(\alpha)|^2$. In particular, by the Cauchy–Schwarz inequality, this implies that

$$\|\widehat{\mathbf{1}_E}\|_1 = \sum_{\alpha \in \mathbb{F}^n} |\widehat{\mathbf{1}_E}(\alpha)| \leq \sqrt{\sum_{\alpha \in \mathbb{F}^n} |\widehat{\mathbf{1}_E}(\alpha)|^2} \cdot \sqrt{\sum_{\alpha \in \mathbb{F}^n} 1} \leq \sqrt{|E|/q^n} \cdot q^{n/2} = \sqrt{|E|} \ .$$

If we let $F(x) = \mathbf{1}_E(x)$, then Parseval's identity becomes the following lemma.

Lemma 4.1. *Let $G\colon \mathbb{F}^n \to \mathbb{C}$ be a function and $E \subseteq \mathbb{F}^n$. Then*

$$\frac{1}{q^n}\sum_{x\in E} G(x) = \frac{1}{q^n}\sum_{\alpha\in\mathbb{F}^n} \overline{\widehat{\mathbf{1}_E}(\alpha)} \sum_{x\in\mathbb{F}^n} G(x)\omega^{-\mathrm{Tr}(\langle\alpha,x\rangle)} = \sum_{\alpha\in\mathbb{F}^n} \overline{\widehat{\mathbf{1}_E}(\alpha)}\widehat{G}(\alpha) \ .$$

4.2 Relating the Fourier spectrum to the probabilities of events

A quasi-distribution $\mathcal{Q}$ is a function $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ that maps a function $f\colon [n] \to \mathbb{F}$ (identified with the corresponding vector $\mathbb{F}^n$) to $\mathcal{Q}(f)$. We can write $\mathcal{Q}(\cdot) = \sum_{\alpha\in\mathbb{F}^n} \widehat{\mathcal{Q}}(\alpha)\chi_\alpha(\cdot)$, where $\{\chi_\alpha\}_{\alpha\in\mathbb{F}^n}$ are the characters and $\{\widehat{\mathcal{Q}}(\alpha)\}_{\alpha\in\mathbb{F}^n}$ are $\mathcal{Q}$'s Fourier coefficients. For $S \subseteq [n]$ and $\alpha \in \mathbb{F}^S$, we abuse notation and use $\widehat{\mathcal{Q}}(\alpha)$ to refer to $\widehat{\mathcal{Q}}(\beta)$ where $\beta \in \mathbb{F}^n$ has $\beta_i = \alpha_i$ for all $i \in S$ and 0 otherwise.

The lemma below relates the inner product quasi-probabilities defined in Definition 3.5 to the Fourier coefficients of $\mathcal{Q}$.

Lemma 4.2. *Let $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ be a quasi-distribution. For every $\alpha \in \mathbb{F}^n$,*

$$\widehat{\mathcal{Q}}(\alpha) = \frac{1}{q^n}\sum_{j\in\mathbb{F}_p} \omega^{-j}\widetilde{\Pr}[\mathrm{Tr}(\langle\alpha,\mathcal{Q}\rangle) = j] \ .$$

Proof of Lemma 4.2. By definition,

$$\begin{aligned}\widehat{\mathcal{Q}}(\alpha) = \langle\chi_\alpha,\mathcal{Q}(\cdot)\rangle &= \frac{1}{q^n}\sum_f \overline{\chi_\alpha(f)}\mathcal{Q}(f) = \frac{1}{q^n}\sum_{j\in\mathbb{F}_p}\omega^{-j}\sum_{f:\chi_\alpha(f)=\omega^j}\mathcal{Q}(f)\\ &= \frac{1}{q^n}\sum_{j\in\mathbb{F}_p}\omega^{-j}\sum_{f:\mathrm{Tr}(\langle\alpha,f\rangle)=j}\mathcal{Q}(f) = \frac{1}{q^n}\sum_{j\in\mathbb{F}_p}\omega^{-j}\widetilde{\Pr}[\mathrm{Tr}(\langle\alpha,\mathcal{Q}\rangle) = j] \ . \qquad \square\end{aligned}$$

The above lemma implies that the Fourier coefficients $(\widehat{\mathcal{Q}}(a\alpha))_{a\in\mathbb{F}}$ are determined by the quasi-probabilities $(\Pr[\langle\alpha,\mathcal{Q}\rangle = b])_{b\in\mathbb{F}}$, as the quasi-probabilities $(\Pr[\langle\alpha,\mathcal{Q}\rangle = b])_{b\in\mathbb{F}}$ determine the quasi-probabilities $(\Pr[\langle a\alpha,\mathcal{Q}\rangle = b])_{b\in\mathbb{F}}$ for every $a \in \mathbb{F}$. In fact, there is a linear transformation M that maps $(\Pr[\langle\alpha,\mathcal{Q}\rangle = b])_{b\in\mathbb{F}}$ to $(q^n\widehat{\mathcal{Q}}(a\alpha))_{a\in\mathbb{F}}$. Below, we state a well-known lemma about M.

Lemma 4.3. *Let $M \in \mathbb{C}^{q\times q}$ be the matrix defined as $M_{a,b} := \omega^{-\mathrm{Tr}(ab)}$ (entries are indexed by $\mathbb{F}$). Then M is invertible and $\frac{1}{\sqrt{q}}M$ is unitary (namely, $M^\dagger \cdot M = qI$). In particular, for every vector $(v_b)_{b\in\mathbb{F}}$ with values in $\mathbb{C}$, the map $(v_b)_{b\in\mathbb{F}} \mapsto (\sum_{b\in\mathbb{F}}\omega^{-\mathrm{Tr}(ab)}v_b)_{a\in\mathbb{F}}$ is a bijection.*

We additionally prove the following lemma, which relates the Fourier spectrum of the quasi-distribution $\mathcal{Q}|_S$ to the Fourier spectrum of $\mathcal{Q}$.

Lemma 4.4. *Let $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ be a quasi-distribution. Let $S \subseteq [n]$, and let $\mathcal{Q}|_S$ denote the restriction of $\mathcal{Q}$ to S, namely, $\mathcal{Q}|_S$ is the quasi-distribution from $\mathbb{F}^S$ to $\mathbb{C}$ where $\mathcal{Q}|_S(g) := \sum_{f:f|_S=g}\mathcal{Q}(f)$. Then for every $\alpha \in \mathbb{F}^S$ it holds that $q^{|S|}\widehat{\mathcal{Q}|_S}(\alpha) = q^n\widehat{\mathcal{Q}}(\alpha)$.*[4]

Proof of Lemma 4.4.

$$q^{|S|}\widehat{\mathcal{Q}|_S}(\alpha) = \sum_{g\in\mathbb{F}^S}\mathcal{Q}|_S(g)\omega^{-\mathrm{Tr}(\langle\alpha,g\rangle)} = \sum_{f\in\mathbb{F}^n}\mathcal{Q}(f)\omega^{-\mathrm{Tr}(\langle\alpha,f\rangle)} = q^n\widehat{\mathcal{Q}}(\alpha) \ . \qquad \square$$

[4]The vector α in $\widehat{\mathcal{Q}}(\alpha)$ is treated as a element in $\mathbb{F}^n$ with $\alpha_j = 0$ for all $j \notin S$

If $\mathcal{F}\colon [n] \to \mathbb{F}$ is a k-non-signaling function, then for any $\alpha \in \mathbb{F}^n_{\le k}$ and $b \in \mathbb{F}$ we have defined $\Pr[\langle \alpha, \mathcal{F}\rangle = b]$ in Definition 3.2 to be $\Pr_{f \leftarrow \mathcal{F}_{\mathrm{supp}(\alpha)}}[\langle \alpha, f\rangle = b]$. Note that the probability is well-defined since $\mathrm{wt}(\alpha) \le k$ (so we query $\mathcal{F}$ on at most k points). Also note that Lemma 4.2 implies that, for every $\alpha \in \mathbb{F}^n_{\le k}$, we can define the Fourier coefficient $\widehat{\mathcal{F}}(\alpha)$ of $\mathcal{F}$ as

$$\widehat{\mathcal{F}}(\alpha) := \frac{1}{q^n} \sum_{j \in \mathbb{F}_p} \omega^{-j} \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F}\rangle) = j] \ .$$

With the above definitions, we can prove the following two corollaries of Lemma 4.1. The first is for non-signaling functions, and the second is for quasi-distributions.

Corollary 4.5. *For any k-non-signaling function $\mathcal{F}\colon [n] \to \mathbb{F}$, set $S \subseteq [n]$, and event $E \subseteq \mathbb{F}^S$,*

$$\Pr[\mathcal{F}(S) \in E] = \sum_{\alpha \in \mathbb{F}^S} \overline{\widehat{\mathbf{1}_E}(\alpha)} \sum_{j \in \mathbb{F}_p} \omega^{-j} \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F}\rangle) = j] = q^n \sum_{\alpha \in \mathbb{F}^S} \overline{\widehat{\mathbf{1}_E}(\alpha)} \widehat{\mathcal{F}}(\alpha) \ .$$

Proof. Apply Lemma 4.1 with $G\colon \mathbb{F}^S \to \mathbb{C}$ defined as $G(x) := \Pr[\mathcal{F}_S(i) = x_i \ \forall i \in S]$. □

Corollary 4.6. *For any quasi-distribution $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$, set $S \subseteq [n]$, and event $E \subseteq \mathbb{F}^S$,*

$$\widetilde{\Pr}[\mathcal{Q}(S) \in E] = \sum_{f\colon f(S) \in E} \mathcal{Q}(f) = \sum_{\alpha \in \mathbb{F}^S} \overline{\widehat{\mathbf{1}_E}(\alpha)} \sum_{j \in \mathbb{F}_p} \omega^{-j} \widetilde{\Pr}[\mathrm{Tr}(\langle \alpha, \mathcal{Q}\rangle) = j] = q^n \sum_{\alpha \in \mathbb{F}^S} \overline{\widehat{\mathbf{1}_E}(\alpha)} \widehat{\mathcal{Q}}(\alpha) \ .$$

Proof. Apply Lemma 4.1 to the function $G\colon \mathbb{F}^S \to \mathbb{C}$ that is the quasi-distribution $\mathcal{Q}|_S$. Then observe that for every $\alpha \in \mathbb{F}^S$, $q^{|S|}\widehat{\mathcal{Q}|_S}(\alpha) = q^n \widehat{\mathcal{Q}}(\alpha)$ by Lemma 4.4. □

The above two lemmas allow us to bound the distance between a k-non-signaling function $\mathcal{F}$ and a quasi-distribution $\mathcal{Q}$ in terms of their Fourier spectra.

Lemma 4.7. *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function and $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ a quasi-distribution. For any set $S \subseteq [n]_{\le k}$ and event $E \subseteq \mathbb{F}^S$,*

$$\left|\Pr[\mathcal{F}(S) \in E] - \widetilde{\Pr}[\mathcal{Q}(S) \in E]\right| \le q^n \sum_{\alpha \in \mathbb{F}^S} \left|\widehat{\mathbf{1}_E}(\alpha)\right| \left|\widehat{\mathcal{F}}(\alpha) - \widehat{\mathcal{Q}}(\alpha)\right| \ .$$

In particular, $\Delta_k(\mathcal{Q}, \mathcal{F}) \le q^{n+k/2} \max_{\alpha \in \mathbb{F}^n_{\le k}} |\widehat{\mathcal{F}}(\alpha) - \widehat{\mathcal{Q}}(\alpha)|$.

Corollary 4.8. *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function and $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ a quasi-distribution. Then $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$ if and only if $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{Q}}(\alpha)$ for every $\alpha \in \mathbb{F}^n_{\le k}$.*

Proof of Lemma 4.7. The first equation follows immediately from Corollary 4.5 and Corollary 4.6. For the second part of the lemma,

$$\begin{aligned}
\Delta_k(\mathcal{Q}, \mathcal{F}) &\le \max_{S \subseteq [n]_{\le k}} \max_{E \subseteq \mathbb{F}^S} q^n \sum_{\alpha \in \mathbb{F}^S} \left|\overline{\widehat{\mathbf{1}_E}(\alpha)}\right| \left|\widehat{\mathcal{F}}(\alpha) - \widehat{\mathcal{Q}}(\alpha)\right| \\
&\le q^n \max_{S \subseteq [n]_{\le k}} \left(\left(\max_{E \subseteq \mathbb{F}^S} \sum_{\alpha \in \mathbb{F}^S} \left|\widehat{\mathbf{1}_E}(\alpha)\right| \right) \max_{\alpha \in \mathbb{F}^S} \left|\widehat{\mathcal{F}}(\alpha) - \widehat{\mathcal{Q}}(\alpha)\right| \right) \\
&\le q^n \left(\max_{S \subseteq [n]_{\le k}} q^{|S|/2} \right) \max_{\alpha \in \mathbb{F}^n_{\le k}} \left|\widehat{\mathcal{F}}(\alpha) - \widehat{\mathcal{Q}}(\alpha)\right| \\
&\le q^{n+k/2} \max_{\alpha \in \mathbb{F}^n_{\le k}} \left|\widehat{\mathcal{F}}(\alpha) - \widehat{\mathcal{Q}}(\alpha)\right| \ .
\end{aligned}$$

□

Proof of Corollary 4.8. If $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{Q}}(\alpha)$ for every $\alpha \in \mathbb{F}^n_{\leq k}$, then by Lemma 4.7 it follows that $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$. Conversely, if $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$, then for every $\alpha \in \mathbb{F}^n_{\leq k}$ and $j \in \mathbb{F}_p$ it holds that $\widetilde{\Pr}[\mathrm{Tr}(\langle \alpha, \mathcal{Q} \rangle) = j] = \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F} \rangle) = j]$, as these are both events. This implies that $q^n \widehat{\mathcal{Q}}(\alpha) = \sum_{j \in \mathbb{F}_p} \omega^{-j} \widetilde{\Pr}[\mathrm{Tr}(\langle \alpha, \mathcal{Q} \rangle) = j] = \sum_{j \in \mathbb{F}_p} \omega^{-j} \Pr[\mathrm{Tr}(\langle \alpha, \mathcal{F} \rangle) = j] = q^n \widehat{\mathcal{F}}(\alpha)$. □

Suppose that we are given a collection of local distributions $(\mathcal{F}_S)_{S \subseteq [n]_{\leq k}}$, namely, $\mathcal{F}_S$ is a distribution over functions $f \colon S \to \mathbb{F}$. We can think of each local distribution $\mathcal{F}_S$ as a function $\mathcal{F}_S \colon \mathbb{F}^S \to \mathbb{C}$, and in this way define for each local distribution $\mathcal{F}_S$ the Fourier coefficients $\widehat{\mathcal{F}_S}(\alpha)$ for each $\alpha \in \mathbb{F}^n_{\subseteq S}$. In the following lemma, we characterize when $(\mathcal{F}_S)_{S \subseteq [n]_{\leq k}}$ is k-non-signaling in terms of the Fourier spectra of the local distributions.

Lemma 4.9. *Let $(\mathcal{F}_S)_{S \subseteq [n]_{\leq k}}$ be a collection of local distributions. Then $(\mathcal{F}_S)_{S \subseteq [n]_{\leq k}}$ is a k-non-signaling function if and only if $q^{|S|} \widehat{\mathcal{F}_S}(\alpha) = q^{|R|} \widehat{\mathcal{F}_R}(\alpha)$ for every $S \subseteq [n]_{\leq k}$, $R \subseteq S$, and $\alpha \in \mathbb{F}^n_{\subseteq R}$.*

Proof. Suppose $(\mathcal{F}_S)_{S \subseteq [n]_{\leq k}}$ is a k-non-signaling function. Fix $S \subseteq [n]_{\leq k}$, $R \subseteq S$, and $\alpha \in \mathbb{F}^n_{\subseteq R}$. Since the collection of local distributions is k-non-signaling we have that $\mathcal{F}_S|_R = \mathcal{F}_R$. Therefore by Lemma 4.4 we have that $q^{|S|} \widehat{\mathcal{F}_S}(\alpha) = q^{|R|} \widehat{\mathcal{F}_R}(\alpha)$.

Now, fix $S \subseteq [n]_{\leq k}$ and $R \subseteq S$. Applying Corollary 4.6 to the distributions $\mathcal{F}_S$ and $\mathcal{F}_R$, we see that if $q^{|S|} \widehat{\mathcal{F}_S}(\alpha) = q^{|R|} \widehat{\mathcal{F}_R}(\alpha)$ for every $\alpha \in \mathbb{F}^n_{\subseteq R}$, then $\mathcal{F}_S|_R \equiv \mathcal{F}_R$. Hence, $(\mathcal{F}_S)_{S \subseteq [n]_{\leq k}}$ is k-non-signaling. □

4.3 Equivalence between non-signaling functions and quasi-distributions

We show that k-non-signaling functions and k-local quasi-distributions are equivalent. Every k-local quasi-distribution $\mathcal{Q}$ induces a k-non-signaling function $\mathcal{F}$ (Proposition 4.10). Conversely, every k-non-signaling function $\mathcal{F}$ can be described by a k-local quasi-distribution $\mathcal{Q}$ (Proposition 4.11). In fact, the set of such quasi-distributions is an affine subspace of co-dimension $\sum_{i=0}^{k} \binom{n}{i} \cdot (q-1)^i$ in $\mathbb{C}^{q^n}$. The first direction of the equivalence is elementary; the other direction is the interesting one.

The aforementioned result is a special case of a result of Abramsky and Brandenburger [AB11] that establishes an equivalence between *non-signaling empirical models* (a general notion of non-signaling experiments in the language of sheaf theory) and quasi-distributions over *global sections*. Our result strengthens this equivalence by giving an explicit characterization of the affine subspace of quasi-distributions describing a non-signaling function, by leveraging Fourier-analytic tools. This also extends to any finite field $\mathbb{F}$ the equivalence lemma for $\mathbb{F}_2$ presented in [CMS18].[5]

Proposition 4.10. *For every k-local quasi-distribution $\mathcal{Q}$ over functions $f \colon [n] \to \mathbb{F}$ there exists a k-non-signaling function $\mathcal{F} \colon [n] \to \mathbb{F}$ such that $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$.*

Proof. For every subset $S \subseteq [n]_{\leq k}$, define $\mathcal{F}_S$ to be the distribution over functions $f \colon S \to \mathbb{F}$ where $\Pr[\mathcal{F}_S \text{ outputs } f] := \widetilde{\Pr}[\mathcal{Q}(S) = f(S)]$, namely, such that $\mathcal{F}_S \equiv \mathcal{Q}|_S$. Note that $\mathcal{F}_S$ is a distribution because $\mathcal{Q}$ is k-local, so the relevant probabilities are in $[0, 1]$ and sum to 1. The definition immediately implies that $\Pr[\mathcal{F}(S) = g] = \widetilde{\Pr}[\mathcal{Q}(S) = g]$ for every string $g \in \mathbb{F}^S$, and so $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$. We are left to argue that $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq [n]_{\leq k}}$ is k-non-signaling. Let $S \subseteq [n]_{\leq k}$,

[5] The characterization further extends to functions taking values in any finite alphabet Σ (not necessarily a field) by adding an abelian group structure to Σ (for example, by identifying Σ with $\mathbb{Z}/|\Sigma|\mathbb{Z}$), and then using analogous tools from Fourier analysis over finite abelian groups.

and let $R \subseteq S$. By definition of $\mathcal{F}$ and Lemma 4.4 we have that for every $\alpha \in \mathbb{F}^R$, $q^{|S|}\widehat{\mathcal{F}_S}(\alpha) = q^{|S|}\widehat{\mathcal{Q}|_S}(\alpha) = q^{|R|}\widehat{\mathcal{Q}|_R}(\alpha) = q^{|R|}\widehat{\mathcal{F}_R}(\alpha)$. By Lemma 4.9, it follows that $\mathcal{F}$ is k-non-signaling. □

Proposition 4.11. *For every k-non-signaling function $\mathcal{F}\colon [n] \to \mathbb{F}$, there exists a k-local quasi-distribution $\mathcal{Q}$ over functions $f\colon [n] \to \mathbb{F}$ such that $\Delta_k(\mathcal{F}, \mathcal{Q}) = 0$. Moreover, the set of such $\mathcal{Q}$'s (viewed as vectors in $\mathbb{C}^{q^n}$) is the affine subspace of co-dimension $\sum_{i=0}^{k} \binom{n}{i} \cdot (q-1)^i$ in $\mathbb{C}^{q^n}$ given by $\mathcal{Q}_0 + \operatorname{span}\{\chi_\alpha : \alpha \in \mathbb{F}^n, \operatorname{wt}(\alpha) > k\}$, where $\mathcal{Q}_0$ is any solution.*

Proof. Let $\mathcal{Q}$ be a quasi-distribution over functions $f\colon [n] \to \mathbb{F}$. By Corollary 4.8, it holds that $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$ if and only if $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{Q}}(\alpha)$ for all $\alpha \in \mathbb{F}^n_{\leq k}$.

Let $\mathcal{Q}_0$ be the quasi-distribution with Fourier coefficients $\widehat{\mathcal{Q}}(\alpha) := \widehat{\mathcal{F}}(\alpha)$ for all α of weight at most k and $\widehat{\mathcal{Q}}(\alpha) := 0$ otherwise. Consider the affine subspace $\mathcal{Q}_0 + \operatorname{span}\{\chi_\alpha : \alpha \in \mathbb{F}^n, \operatorname{wt}(\alpha) > k\}$. By Corollary 4.8, every quasi-distribution $\mathcal{Q}$ in the affine subspace satisfies $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$. We note that this affine subspace has dimension $\sum_{i=0}^{k} \binom{n}{i} \cdot (q-1)^i$.

Conversely, suppose that $\mathcal{Q}$ satisfies $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$. Then by Corollary 4.8 it holds that $\widehat{\mathcal{Q}}(\alpha) = \widehat{\mathcal{F}}(\alpha)$ for all $\alpha \in \mathbb{F}^n_{\leq k}$, which implies that $\mathcal{Q}$ is in the aforementioned affine subspace. Hence, the affine subspace contains all $\mathcal{Q}$ such that $\Delta_k(\mathcal{Q}, \mathcal{F}) = 0$. □

5 Non-signaling linear codes

We wish to define what it means for a non-signaling function $\mathcal{F}\colon [n] \to \mathbb{F}$ to be "in" a linear code $\mathbf{C} \subseteq \mathbb{F}^n$. We introduce two natural definitions for the above goal. The first definition is motivated by the equivalence between non-signaling functions and quasi-distributions established in Section 4.3. The second definition is motivated by a notion of local consistency.

For each of the two definitions, we *characterize* the Fourier spectrum of non-signaling strategies that satisfy the definition, in the exact and in the robust case. Also, we prove a strong relationship between the two definitions, showing that they are *equivalent* (up to a small loss in parameters). The compelling structure that we uncover supports our choice of definitions.

For this section, we remind the reader that a linear code $\mathbf{C}$ over $\mathbb{F}$ with block length n is a linear subspace of $\mathbb{F}^n$. We equivalently also view $\mathbf{C}$ as a linear subspace of the set of all functions $f\colon [n] \to \mathbb{F}$. The dual code of $\mathbf{C}$ is the linear subspace $\mathbf{C}^\perp := \{\alpha : \langle \alpha, f \rangle = 0 \ \forall f \in \mathbf{C}\} \subseteq \mathbb{F}^n$.

5.1 Quasi-distributions supported on linear codes

The equivalence between non-signaling functions and quasi-distributions in Section 4.3 suggests a natural way to capture when a non-signaling function is "in" a given linear code.

Definition 5.1. *Given a k-non-signaling strategy $\mathcal{F}\colon [n] \to \mathbb{F}$, code $\mathbf{C} \subseteq \mathbb{F}^n$ and parameter $k' \leq k$, we say that $\mathcal{F}$ is* $(\mathbf{C}, k')$**-supported** *if there exists a k'-local quasi-distribution $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ supported on $\mathbf{C}$ such that $\Delta_{k'}(\mathcal{Q}, \mathcal{F}) = 0$.*

In light of the characterization of the Fourier spectra of quasi-distributions equivalent to a given non-signaling function in Section 4.3, it is natural to ask if the Fourier spectrum of a quasi-distribution supported on $\mathbf{C}$ has a special structure. In the following lemma, we characterize the Fourier spectrum of quasi-distributions supported on a given linear code $\mathbf{C}$. Informally, we show that the condition "Fourier coefficients are constants on cosets of $\mathbf{C}^\perp$" is necessary and sufficient.

Lemma 5.2. *Let $\mathbf{C} \subseteq \mathbb{F}^n$ be a linear code. A quasi-distribution $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ is supported on $\mathbf{C}$ if and only if $\widehat{\mathcal{Q}}(\alpha) = \widehat{\mathcal{Q}}(\alpha')$ for all $\alpha, \alpha' \in \mathbb{F}^n$ such that $\alpha - \alpha' \in \mathbf{C}^\perp$.*

The foregoing statement immediately gives us a corollary about non-signaling functions.

Corollary 5.3. *A k-non-signaling strategy $\mathcal{F}\colon [n] \to \mathbb{F}$ is $(\mathbf{C}, k')$-supported if and only if for all $\alpha, \alpha' \in \mathbb{F}^n_{\leq k}$ such that $\alpha - \alpha' \in \mathbf{C}^\perp$ it holds that $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{F}}(\alpha')$.*

Next, we wish to study the Fourier spectrum of a quasi-distribution $\mathcal{Q}$ that is merely *close* to being supported on $\mathbf{C}$. For this case, we give the following "robust" version of Lemma 5.2.

Lemma 5.4. *Let $\mathbf{C} \subseteq \mathbb{F}^n$ be a linear code, and let $\mathcal{Q}$ be a quasi-distribution.*

- *Suppose that there exists a quasi-distribution $\mathcal{Q}'$ supported on $\mathbf{C}$ such that $\Delta_k(\mathcal{Q}, \mathcal{Q}') \leq \delta$. Then for all $\alpha, \alpha' \in \mathbb{F}^n_{\leq k}$ and $\alpha - \alpha' \in \mathbf{C}^\perp$ it holds that $\left|\widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}(\alpha')\right| \leq \frac{2\delta}{q^n}$.*
- *Conversely, suppose that for all $\alpha, \alpha' \in \mathbb{F}^n_{\leq k}$ and $\alpha - \alpha' \in \mathbf{C}^\perp$ it holds that $\left|\widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}(\alpha')\right| \leq \frac{2\delta}{q^n}$. Then there exists a quasi-distribution $\mathcal{Q}'$ supported on $\mathbf{C}$ such that $\Delta_k(\mathcal{Q}, \mathcal{Q}') \leq q^{k/2} \cdot 2\delta$.*

We note that in Lemma 5.4, neither quasi-distribution is required to be local.

5.1.1 Proof of Lemma 5.2

Define the affine spaces

$$V_1 = \left\{ \mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C} \text{ s.t. } \sum_{f \in \mathbf{C}} \mathcal{Q}(f) = 1 \text{ and } \mathcal{Q}(f) = 0 \ \forall f \notin \mathbf{C} \right\} \ ,$$

$$V_2 = \left\{ \mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C} \text{ s.t. } \widehat{\mathcal{Q}}(0^n) = \frac{1}{q^n} \text{ and } \widehat{\mathcal{Q}}(\alpha) = \widehat{\mathcal{Q}}(\alpha+\gamma) \ \forall \alpha \in \mathbb{F}^n, \gamma \in \mathbf{C}^\perp \right\} \ .$$

It suffices to prove that $V_1 = V_2$. First we show that $\dim(V_1) = \dim(V_2)$. The dimension of V_1 is $|\mathbf{C}| - 1$ because the $|\mathbf{C}|$ free terms are subject to a single linear constraint. The dimension of V_2 is $q^n / \left|\mathbf{C}^\perp\right| - 1$ because the Fourier coefficients are constant on each coset of $\mathbf{C}^\perp$, and on each coset they can take on an arbitrary value; the one exception is the coset $\mathbf{C}^\perp$, on which the Fourier coefficients must be $\frac{1}{q^n}$. Recalling that $q^n = |\mathbf{C}| \cdot |\mathbf{C}^\perp|$, we deduce that $\dim(V_1) = \dim(V_2)$.

Next we show that $V_1 \subseteq V_2$. Fix $\mathcal{Q} \in V_1$. Since $\sum_f \mathcal{Q}(f) = 1$, we have $\widehat{\mathcal{Q}}(0^n) = \frac{1}{q^n} \sum_f \mathcal{Q}(f) \cdot \omega^0 = \frac{1}{q^n}$. Moreover, for any $\alpha \in \mathbb{F}^n$ and $\gamma \in \mathbf{C}^\perp$,

$$\widehat{\mathcal{Q}}(\alpha+\gamma) = \frac{1}{q^n} \cdot \sum_f \mathcal{Q}(f) \cdot \omega^{-\mathrm{Tr}(\langle \alpha+\gamma f \rangle)} = \frac{1}{q^n} \cdot \sum_f \mathcal{Q}(f) \cdot \omega^{-\mathrm{Tr}(\langle \alpha, f \rangle)} \cdot \omega^{-\mathrm{Tr}(\langle \gamma, f \rangle)} \ .$$

Since $\mathcal{Q} \in V_1$, if $\mathcal{Q}(f) \neq 0$ then $f \in \mathbf{C}$ and hence $\omega^{\mathrm{Tr}(\langle \gamma, f \rangle)} = \omega^{\mathrm{Tr}(0)} = 1$. Therefore,

$$\widehat{\mathcal{Q}}(\alpha+\gamma) = \frac{1}{q^n} \cdot \sum_f \mathcal{Q}(f) \cdot \omega^{-\mathrm{Tr}(\langle \alpha, f \rangle)} = \widehat{\mathcal{Q}}(\alpha) \ .$$

Thus $V_1 \subseteq V_2$. Since $\dim(V_1) = \dim(V_2)$ and $V_1 \subseteq V_2$, we conclude that $V_1 = V_2$.

5.1.2 Proof of Lemma 5.4

Suppose $\mathcal{Q}\colon \mathbb{F}^n \to \mathbb{C}$ is a quasi-distribution such that there exists a quasi-distribution $\mathcal{Q}'$ supported on $\mathbf{C}$ with $\Delta_k(\mathcal{Q}, \mathcal{Q}') \leq \delta$. Fix $\alpha \in \mathbb{F}^n_{\leq k}$, so that $S = \mathrm{supp}(\alpha)$ has $|S| \leq k$. Since $\Delta_k(\mathcal{Q}, \mathcal{Q}') \leq \delta$, we have that $\sum_{g \in \mathbb{F}^S} \left| \widetilde{\Pr}[\mathcal{Q}(S) = g] - \widetilde{\Pr}[\mathcal{Q}'(S) = g] \right| \leq \delta$. Therefore,

$$\begin{aligned}
\left| \widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}'(\alpha) \right| &\leq \frac{1}{q^n} \sum_{j \in \mathbb{F}_p} |\omega^{-j}| \left| \widetilde{\Pr}[\mathrm{Tr}(\langle \alpha, \mathcal{Q} \rangle) = j] - \widetilde{\Pr}[\mathrm{Tr}(\langle \alpha, \mathcal{Q}' \rangle) = j] \right| \\
&= \frac{1}{q^n} \sum_{j \in \mathbb{F}_p} \sum_{g \in \mathbb{F}^S : \mathrm{Tr}(\langle \alpha, g \rangle) = j} \left| \widetilde{\Pr}[\mathcal{Q}(S) = g] - \widetilde{\Pr}[\mathcal{Q}'(S) = g] \right| \\
&\leq \frac{1}{q^n} \sum_{g \in \mathbb{F}^S} \left| \widetilde{\Pr}[\mathcal{Q}(S) = g] - \widetilde{\Pr}[\mathcal{Q}'(S) = g] \right| \leq \frac{\delta}{q^n} \ .
\end{aligned}$$

By Lemma 5.2, we know that for every $\alpha, \alpha' \in \mathbb{F}^n$ such that $\alpha - \alpha' \in \mathbf{C}^\perp$ it holds that $\left| \widehat{\mathcal{Q}}'(\alpha) - \widehat{\mathcal{Q}}'(\alpha') \right| = 0$. Hence, for every $\alpha, \alpha' \in \mathbb{F}^n_{\leq k}$ such that $\alpha - \alpha' \in \mathbf{C}^\perp$ it holds that

$$\left| \widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}(\alpha') \right| \leq \left| \widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}'(\alpha) \right| + \left| \widehat{\mathcal{Q}}'(\alpha) - \widehat{\mathcal{Q}}'(\alpha') \right| + \left| \widehat{\mathcal{Q}}'(\alpha') - \widehat{\mathcal{Q}}(\alpha') \right|$$

$$\leq \frac{\delta}{q^n} + 0 + \frac{\delta}{q^n} = \frac{2\delta}{q^n} \ .$$

Now, suppose that $\mathcal{Q}$ is a quasi-distribution such that $\left|\widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}(\alpha')\right| \leq \frac{2\delta}{q^n}$ for all $\alpha, \alpha' \in \mathbb{F}^n_{\leq k}$ such that $\alpha - \alpha' \in \mathbf{C}^\perp$. For each $\alpha \in \mathbb{F}^n$, let γ_α be an element of the coset $\alpha + \mathbf{C}^\perp$ of minimal weight (ties are broken arbitrarily). Define $\mathcal{Q}'$ to be the quasi-distribution where $\widehat{\mathcal{Q}'}(\alpha) := \widehat{\mathcal{Q}}(\gamma_\alpha)$ if $\mathrm{wt}(\gamma_\alpha) \leq k$ and 0 otherwise. By construction, for any $\alpha, \alpha' \in \mathbb{F}^n$ such that $\alpha - \alpha' \in \mathbf{C}^\perp$ it holds that $\widehat{\mathcal{Q}'}(\alpha) = \widehat{\mathcal{Q}'}(\alpha')$, so $\mathcal{Q}'$ is supported on $\mathbf{C}$ by Lemma 5.2. Let $\alpha \in \mathbb{F}^n_{\leq k}$. By construction, we know that $\left|\widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}'}(\alpha)\right| \leq \left|\widehat{\mathcal{Q}}(\alpha) - \widehat{\mathcal{Q}}(\gamma_\alpha)\right| + \left|\widehat{\mathcal{Q}}(\gamma_\alpha) - \widehat{\mathcal{Q}'}(\alpha)\right| \leq \frac{2\delta}{q^n} + 0 = \frac{2\delta}{q^n}$, since $\alpha - \gamma_\alpha \in \mathbf{C}^\perp$ and $\mathrm{wt}(\gamma_\alpha) \leq \mathrm{wt}(\alpha) \leq k$. Therefore, by Lemma 4.7 we have that $\Delta_k(\mathcal{Q}, \mathcal{Q}') \leq q^{k/2} \cdot 2\delta$.

5.2 Locally-explainable non-signaling functions

We introduce another natural definition that captures when a non-signaling function $\mathcal{F}$ is "in" a given linear code $\mathbf{C} \subseteq \mathbb{F}^n$. This time we take the perspective of local consistency, namely, we shall require that the output of $\mathcal{F}$ is always consistent with a codeword in $\mathbf{C}$.

Definition 5.5. *Given a k-non-signaling strategy $\mathcal{F}\colon [n] \to \mathbb{F}$, code $\mathbf{C} \subseteq \mathbb{F}^n$, and parameter $k' \leq k$, we say that $\mathcal{F}$ is* $(\mathbf{C}, k')$**-explainable** *if for every set $S \subseteq [n]_{\leq k'}$ it holds that $\Pr[\mathcal{F}(S) \in \mathbf{C}|_S] = 1$.*

Note that $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable if and only if $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathbf{C}^\perp_{\leq k'}$. The non-trivial direction of the equivalence is implied by the following lemma.

Lemma 5.6. *Let $\mathbf{C} \subseteq \mathbb{F}^n$ be a linear code, $S \subseteq [n]_{\leq k}$, and $g\colon S \to \mathbb{F}$. If $\langle \alpha, g \rangle = 0$ for every $\alpha \in \mathbf{C}^\perp_{\subseteq S}$, then there is a codeword $f \in \mathbf{C}$ such that $f|_S = g$.*

Proof. Since $\mathbf{C} \subseteq \mathbb{F}^n$ is a linear code, there is a *pivotal set* $P \subseteq [n]$ of size $|P| = \dim(\mathbf{C})$ such that for all $y\colon P \to \mathbb{F}$ there is a unique codeword $f \in \mathbf{C}$ satisfying $f|_P = y$. Such P need not be unique.

Let $P^* \subseteq [n]$ be a pivotal set such that $|P^* \cap S|$ is maximal, and let $P_S := P^* \cap S$. Define $f'\colon P^* \to \mathbb{F}$ by letting $f'(i) = g(i)$ for all $i \in P_S$, and letting $f'(j)$ be arbitrary for all $j \in P^* \setminus P_S$. Since P^* is a pivotal set, there exists a unique $f \in \mathbf{C}$ such that $f|_{P^*} = f'$.

It remains to show that $f|_S = g$. Let $i \in S$. If $i \in P_S$, then $f(i) = f'(i) = g(i)$, as required. Suppose that $i \notin P_S$. Since P^* is maximal, there exists $\alpha \in \mathbf{C}^\perp$ such that $\alpha_i = 1$ and $\mathrm{supp}(\alpha) \subseteq P_S \cup \{i\} \subseteq S$. Indeed, if no such α exists then for any codeword $h \in \mathbf{C}$, $h(i)$ is not determined by $\{h(j) : j \in P_S\}$. Hence, the set $P_S \cup \{i\}$ can be extended into a pivotal set for $\mathbf{C}$, which contradicts the maximality of P^*. Therefore, such an α exists. Since $\langle \alpha, f \rangle = 0$ and $\langle \alpha, g \rangle = 0$, we get that $0 = \langle \alpha, f \rangle - \langle \alpha, g \rangle = f(i) + \sum_{j \in P_S} \alpha_j f(j) - g(i) - \sum_{j \in P_S} \alpha_j g(j) = f(i) + \sum_{j \in P_S} \alpha_j g(j) - g(i) - \sum_{j \in P_S} \alpha_j g(j) = f(i) - g(i)$, and therefore $f(i) = g(i)$. We conclude that $f|_S = g$, as required. □

We provide a characterization of the Fourier spectrum of $\mathbf{C}$-explainable non-signaling functions, both in the exact and in the robust cases, as captured by the respective lemmas below. Both lemmas make crucial use of Lemma 4.3.

Lemma 5.7. *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function. Then $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable if and only if $\widehat{\mathcal{F}}(\alpha) = \frac{1}{q^n}$ for every $\alpha \in \mathbf{C}^\perp_{\leq k'}$.*

Proof. We know that $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable if and only if for every $\alpha \in \mathbf{C}^{\perp}_{\leq k'}$ it holds that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$. By Lemma 4.3, we know that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ if and only if $\widehat{\mathcal{F}}(a\alpha) = \frac{1}{q^n}$ for every $a \in \mathbb{F}$, as M is invertible and maps the distribution $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ and $\Pr[\langle \alpha, \mathcal{F} \rangle = b] = 0$ for all other b to the vector 1^q. We conclude the proof by noting that if $\alpha \in \mathbf{C}^{\perp}_{\leq k'}$ then $a\alpha \in \mathbf{C}^{\perp}_{\leq k'}$ for any $a \in \mathbb{F}$. □

Lemma 5.8. *Let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function, and let $\alpha \in \mathbb{F}^n_{\leq k}$.*

- *If $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \varepsilon$, then $|\widehat{\mathcal{F}}(a\alpha) - \frac{1}{q^n}| \leq \frac{2\varepsilon}{q^n}$ for every $a \in \mathbb{F}$.*
- *If $|\widehat{\mathcal{F}}(a\alpha) - \frac{1}{q^n}| \leq \frac{\varepsilon}{q^n}$ for every $a \in \mathbb{F}$, then $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \varepsilon$.*

Proof. Suppose that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \varepsilon$. This immediately implies that, for every $a \in \mathbb{F}$, $\Pr[\langle a\alpha, \mathcal{F} \rangle = 0] \geq 1 - \varepsilon$. Therefore,

$$\begin{aligned}
\left| q^n \widehat{\mathcal{F}}(a\alpha) - 1 \right| &= \left| -1 + \sum_{b \in \mathbb{F}} \omega^{-\mathrm{Tr}(ab)} \Pr[\langle a\alpha, \mathcal{F} \rangle = b] \right| \\
&\leq |-1 + \Pr[\langle a\alpha, \mathcal{F} \rangle = 0]| + \sum_{b \neq 0} |\omega^{-\mathrm{Tr}(ab)}| \, |\Pr[\langle a\alpha, \mathcal{F} \rangle = b]| \\
&\leq \varepsilon + \sum_{b \neq 0} \Pr[\langle a\alpha, \mathcal{F} \rangle = b] \\
&= \varepsilon + (1 - \Pr[\langle a\alpha, \mathcal{F} \rangle = 0]) \leq 2\varepsilon \ .
\end{aligned}$$

This proves the first direction.

For the second direction, let $v \in \mathbb{C}^q$ be the vector where $v_b = \Pr[\langle \alpha, \mathcal{F} \rangle = b]$ and let $w \in \mathbb{C}^q$ be the vector where $w_a = q^n \widehat{\mathcal{F}}(a\alpha)$. Note that $Mv = w$, where M is the matrix from Lemma 4.3. Suppose that $|\widehat{\mathcal{F}}(a\alpha) - \frac{1}{q^n}| \leq \frac{\varepsilon}{q^n}$ for every $a \in \mathbb{F}$, so that $|w_a - 1| \leq \varepsilon$ for every $a \in \mathbb{F}$. Then, we have that $\|w - 1^q\|^2_{\ell_2} \leq q\varepsilon^2$, so that $\|w - 1^q\|_{\ell_2} \leq \varepsilon\sqrt{q}$. Let $u \in \mathbb{C}^q$ be the vector where $u_0 = 1$ and $u_b = 0$ for all other $b \in \mathbb{F}$. Observe that $Mu = 1^q$. Since $\frac{1}{\sqrt{q}} M$ is unitary, we have that $\|\frac{1}{\sqrt{q}} M(v - u)\|_{\ell_2} = \|\frac{1}{\sqrt{q}}(w - 1^q)\|_{\ell_2} \leq \frac{1}{\sqrt{q}} \cdot \varepsilon\sqrt{q} = \varepsilon$. Therefore, $|v_b - u_b| \leq \varepsilon$ for all $b \in \mathbb{F}$. In particular, $|v_0 - 1| \leq \varepsilon$, so that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \varepsilon$. □

5.3 The relationship between the two definitions

We have given two natural definitions of what it means for a non-signaling function to be in a linear code. Which of the two definitions is more "correct"? Lemma 5.2 and Lemma 5.7 show that Definition 5.1 implies Definition 5.5, in the sense that if $\mathcal{F}$ is $(\mathbf{C}, k')$-supported then $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable. We prove that, conversely, Definition 5.5 implies Definition 5.1 up to a factor of 2 in the locality k'. We conclude that the two definitions are essentially equivalent.

Lemma 5.9. *Let $\mathbf{C} \subseteq \mathbb{F}^n$ be a linear code, and let $\mathcal{F}\colon [n] \to \mathbb{F}$ be a k-non-signaling function.*

- *If $\mathcal{F}$ is $(\mathbf{C}, k')$-supported then $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable.*
- *If $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable then $\mathcal{F}$ is $(\mathbf{C}, k'/2)$-supported.*

Remark 5.10. For specific choices of $\mathbf{C}$ one can achieve stronger versions of the above lemma. For example, when $\mathbf{C}$ is the Hadamard code (all linear functions), one can prove the lemma with $k' - 1$ in place of $k'/2$. Also, *some* gap in locality is necessary: taking again $\mathbf{C}$ to be the Hadamard

code, there exists a non-signaling function $\mathcal{F}$ that is $(\mathbf{C}, k)$-explainable and $(\mathbf{C}, k-1)$-supported but *not* $(\mathbf{C}, k)$-supported. (The foregoing statements are shown implicitly in [CMS18].)

Proof. Lemma 5.2 and Lemma 5.7 imply the first direction, as any $(\mathbf{C}, k')$-supported k-non-signaling function $\mathcal{F}$ satisfies $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{F}}(0^n) = \frac{1}{q^n}$ for every $\alpha \in \mathbf{C}^{\perp}_{\leq k'}$, implying that $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable.

We now prove the second direction. Fix $\alpha \in \mathbf{C}^{\perp}_{\leq k'}$, and let $S := \{i \in [n] : \alpha_i \neq 0\}$. Note that $|S| \leq k'$ since $|S| = \mathrm{wt}(\alpha)$. We first show that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$. Indeed, since $\mathcal{F}$ is $(\mathbf{C}, k')$-explainable, we have that

$$\begin{aligned}\Pr[\langle \alpha, \mathcal{F} \rangle = 0] &\geq \Pr[\langle \alpha, \mathcal{F} \rangle = 0 \wedge \exists f \in \mathbf{C} \text{ s.t. } \mathcal{F}(S) = f|_S] \\ &= \Pr[\langle \alpha, f \rangle = 0 \wedge \exists f \in \mathbf{C} \text{ s.t. } \mathcal{F}(S) = f|_S] \\ &= \Pr[\exists f \in \mathbf{C} \text{ s.t. } \mathcal{F}(S) = f|_S] = 1 \ ,\end{aligned}$$

and so $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$.

Now, for any $\alpha, \alpha' \in \mathbb{F}^n_{\leq k'/2}$ with $\alpha - \alpha' \in \mathbf{C}^{\perp}$ we get that for any $b \in \mathbb{F}$,

$$\Pr[\langle \alpha, \mathcal{F} \rangle = b] = \Pr[\langle \alpha', \mathcal{F} \rangle + \langle \alpha - \alpha', \mathcal{F} \rangle = b] = \Pr[\langle \alpha', \mathcal{F} \rangle = b] \ ,$$

since $\Pr[\langle \alpha - \alpha', \mathcal{F} \rangle = 0] = 1$ as $\alpha - \alpha' \in \mathbf{C}^{\perp}$ with $\mathrm{wt}(\alpha - \alpha') \leq k'$. This shows that the vectors $(\Pr[\langle \alpha, \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$ and $(\Pr[\langle \alpha', \mathcal{F} \rangle = b])_{b \in \mathbb{F}}$ are the same. Thus, $\widehat{\mathcal{F}}(\alpha) = \widehat{\mathcal{F}}(\alpha')$, by the definition of $\mathcal{F}$'s Fourier coefficients. By Lemma 5.2, it follows that $\mathcal{F}$ is $(\mathbf{C}, k'/2)$-supported. □

6 Local characterizations and Cayley hypergraphs

We prove Theorem 3 in this section. For this section, we let $k' \leq k$ be an integer. We let $\mathbf{C} \subseteq \mathbb{F}^n$ be a linear code, and $T \subseteq \mathbb{F}^n$ be a set of constraints. Given a k-non-signaling function $\mathcal{F}$, we say that $\mathcal{F}$ satisfies a constraint $\alpha \in \mathbb{F}^n_{\leq k}$ if $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$.

Definition 6.1. *We let* $\mathsf{Consistent}(T, k)$ *denote the set of k-non-signaling functions $\mathcal{F}$ where* $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ *for every $\alpha \in T$. That is,* $\mathsf{Consistent}(T, k)$ *is the set of k-non-signaling functions that are consistent with T.*

We note that by Lemma 5.7, $\mathsf{Consistent}(\mathbf{C}^\perp_{\leq k'}, k)$ is the set of k-non-signaling functions that are $(\mathbf{C}, k')$-explainable.

With the above definition, the definition of local characterization can be rephrased as follows.

Definition 6.2. *For $\ell \leq k' \leq k$, a set of constraints $T \subseteq \mathbf{C}^\perp_{\leq \ell}$ is a ℓ-local characterization of $(\mathbf{C}, k', k)$ if* $\mathsf{Consistent}(T, k)$ *equals the set of k-non-signaling functions that are $(\mathbf{C}, k')$-explainable, i.e. that* $\mathsf{Consistent}(T, k) = \mathsf{Consistent}(\mathbf{C}^\perp_{\leq k'}, k)$.

In this language, [CMS18] shows that $T = \{e_x + e_y - e_{x+y} : x, y \in \{0,1\}^n\}$ is a 3-local characterization of $(\mathbf{C}, k-1, k)$, where $\mathbf{C}$ is the Hadamard code.

We briefly recall the definition of a Cayley hypergraph introduced in Section 1.2

Definition 6.3. *Given a set $T \subseteq \mathbf{C}^\perp$, the* **Cayley hypergraph** $\Gamma_k(\mathbf{C}^\perp, T)$ *is the hypergraph with vertices $V = \{\alpha \in \mathbf{C}^\perp : \mathrm{wt}(\alpha) \leq k\}$, edges $E = \{(\alpha, \alpha + \gamma) : \alpha \in V, \gamma \in T, |\mathrm{supp}(\alpha) \cup \mathrm{supp}(\gamma)| \leq k\} \cup \{(\alpha, b\alpha) : b \in \mathbb{F} \setminus \{0\}\}$, and hyperedges $H = \{(\alpha, \beta, \alpha + \beta) : |\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)| \leq k\}$.*

Definition 6.4 (Path in Cayley hypergraph)**.** *Let $\alpha \in \mathbb{F}^n$. A path from 0^n to α in $\Gamma_k(\mathbf{C}^\perp, T)$ is a sequence $(\alpha_1, \ldots, \alpha_r)$ of vertices such that $\alpha_1 = 0^n$, $\alpha_r = \alpha$, and for each $i > 1$ one of the following three cases holds: 1. (edges) there exists $j < i$ such that (α_j, α_i) is an edge, or 2. (hyperedges) there exists $j_1, j_2 < i$ such that $(\alpha_{j_1}, \alpha_{j_2}, \alpha_i)$ is a hyperedge.*

We write $T \vdash_k \alpha$ (using the symbol $\vdash$ from mathematical logic) if there is a path from 0^n to α in $\Gamma_k(\mathbf{C}^\perp, T)$. The notation is motivated by the fact that a path in $\Gamma_k(\mathbf{C}^\perp, T)$ can be equivalently viewed as a logical deduction of α from T. We note that if $T \vdash_k \alpha$, then it must be the case that $\alpha \in \mathrm{span}(T)$, but the converse is not necessarily the case (in fact, Theorem 1 is simply an example where this fails).

Theorem 3 is stated formally as the theorem below.

Theorem 5. *For $\ell \leq k' \leq k$, a set of constraints $T \subseteq \mathbf{C}^\perp_{\leq \ell}$ is a ℓ-local characterization of $(\mathbf{C}, k', k)$ if and only if $T \vdash_k \mathbf{C}^\perp_{\leq k'}$.*

The proof of Theorem 5 relies on the notion of a k-local subspace, which we define below.

Definition 6.5. *A k-local subspace $\mathcal{V}$ is a subset of $\mathbb{F}^n_{\leq k}$ where $\mathcal{V}_{\subseteq S} \subseteq \mathbb{F}^n$ is a linear subspace for every $S \subseteq [n]_{\leq k}$.*

We prove Theorem 5 by showing the following three lemmas.

Lemma 6.6. *If $T \vdash_k \alpha$, then* $\mathsf{Consistent}(T, k) = \mathsf{Consistent}(T \cup \{\alpha\}, k)$.

Lemma 6.7. *For every k-local subspace $\mathcal{V} \subseteq \mathbb{F}^n_{\leq k}$, there exists a k-non-signaling function $\mathcal{F}$ such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathcal{V}$, and $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = \frac{1}{|\mathbb{F}|}$ otherwise.*

Lemma 6.8. *$\{\alpha \in \mathbb{F}^n : T \vdash_k \alpha\} \subseteq \mathbb{F}^n_{\leq k}$ is a k-local subspace.*

Proof of Theorem 5. Suppose that $T \vdash_k \mathbf{C}^{\perp}_{\leq k'}$. Then by Lemma 6.6 we have that $\mathsf{Consistent}(T, k) = \mathsf{Consistent}(T \cup \mathbf{C}^{\perp}_{\leq k'}, k)$. Since $T \subseteq \mathbf{C}^{\perp}_{\leq \ell}$ and $\ell \leq k'$, we get that $T \subseteq \mathbf{C}^{\perp}_{\leq k'}$. Hence, $\mathsf{Consistent}(T, k) = \mathsf{Consistent}(T \cup \mathbf{C}^{\perp}_{\leq k'}, k) = \mathsf{Consistent}(\mathbf{C}^{\perp}_{\leq k'}, k)$, as required.

Conversely, suppose that T is an ℓ-local characterization of $(\mathbf{C}, k', k)$. By Lemma 6.7 and Lemma 6.8, there exists a k-non-signaling function $\mathcal{F}$ such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in \mathbb{F}^n_{\leq k}$ such that $T \vdash_k \alpha$, and $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = \frac{1}{|\mathbb{F}|}$ otherwise. Since $T \vdash_k \alpha$ for every $\alpha \in T$, it follows that $\mathcal{F} \in \mathsf{Consistent}(T, k)$, which implies that $\mathcal{F} \in \mathsf{Consistent}(\mathbf{C}^{\perp}_{\leq k'}, k)$ as T is an ℓ-local characterization of $(\mathbf{C}, k', k)$. This implies that $T \vdash_k \alpha$ for all $\alpha \in \mathbf{C}^{\perp}_{\leq k'}$, since for all such α it holds that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$, and thus $T \vdash_k \alpha$. $T \vdash_k \mathbf{C}^{\perp}_{\leq k'}$, as required. □

6.1 Proof of Lemma 6.6

It is clear that from the definition that $\mathsf{Consistent}(T, k) \supseteq \mathsf{Consistent}(T \cup \{\alpha\}, k)$ for all $\alpha \in \mathbb{F}^n$. Below we prove the containment in the other direction. Suppose that $T \vdash_k \alpha$, and let $(\alpha_1 = 0^n, \alpha_2, \ldots, \alpha_r = \alpha)$ be a path from 0^n to α in $\Gamma_k(\mathbf{C}^{\perp}, T)$. Let $\mathcal{F} \in \mathsf{Consistent}(T, k)$, that is, $\mathcal{F}$ is a k-non-signaling function such that $\forall \gamma \in T$, $\Pr[\langle \gamma, \mathcal{F} \rangle = 0] = 1$. We prove by induction that for $i \in [r]$ it holds that $\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = 1$.

For the base case of $i = 1$ it must be the case that $\alpha_1 = 0^n$. Therefore, $\Pr[\langle \alpha_1, \mathcal{F} \rangle = 0] = 1$. For the induction step let $i > 1$, and consider the following three cases.

1. There exists $j < i$ and $b \in \mathbb{F} \setminus \{0^n\}$ such that $\alpha_i = b\alpha_j$. Then,

$$\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = \Pr[b\langle \alpha_j, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_j, \mathcal{F} \rangle = 0] = 1 \ ,$$

   where the last equality uses the induction hypothesis.

2. There exist $j < i$ and $\gamma \in T$ such that $\alpha_i = \alpha_j + \gamma$ with $|\mathrm{supp}(\alpha_j) \cup \mathrm{supp}(\gamma)| \leq k$. Since $\mathcal{F} \in \mathsf{Consistent}(T, k)$ we have that $\Pr[\langle \gamma, \mathcal{F} \rangle = 0] = 1$, as $\gamma \in T$. Therefore,

$$\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_j, \mathcal{F} \rangle + \langle \gamma, \mathcal{F} \rangle = 0] \geq \Pr[\langle \alpha_j, \mathcal{F} \rangle = 0 \wedge \langle \gamma, \mathcal{F} \rangle = 0] = 1 \ ,$$

   as required. Note that $\Pr[\langle \alpha_j, \mathcal{F} \rangle = 0 \wedge \langle \gamma, \mathcal{F} \rangle = 0]$ is well-defined since $|\mathrm{supp}(\alpha_{j_1}) \cup \mathrm{supp}(\gamma)| \leq k$.

3. There exist $j_1, j_2 < i$ such that $\alpha_i = \alpha_{j_1} + \alpha_{j_2}$ and $|\mathrm{supp}(\alpha_{j_1}) \cup \mathrm{supp}(\alpha_{j_2})| \leq k$. By the induction hypothesis we know that $\Pr[\langle \alpha_{j_1}, \mathcal{F} \rangle = 0] = 1$ and $\Pr[\langle \alpha_{j_2}, \mathcal{F} \rangle = 0] = 1$. Thus,

$$\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_{j_1}, \mathcal{F} \rangle + \langle \alpha_{j_2}, \mathcal{F} \rangle = 0] \geq \Pr[\langle \alpha_{j_1}, \mathcal{F} \rangle = 0 \wedge \langle \alpha_{j_2}, \mathcal{F} \rangle = 0] = 1 \ ,$$

   and therefore $\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = 1$. Again, we require $|\mathrm{supp}(\alpha_{j_1}) \cup \mathrm{supp}(\alpha_{j_2})| \leq k$ in order for the last probability to be well-defined.

In particular, this implies that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_r, \mathcal{F} \rangle = 0] = 1$, and hence $\mathcal{F} \in \mathsf{Consistent}(T \cup \{\alpha\}, k)$. Therefore $\mathsf{Consistent}(T, k) \subseteq \mathsf{Consistent}(T \cup \{\alpha\}, k)$, which completes the proof of Lemma 6.6.

6.2 Proof of Lemma 6.7

We define $\mathcal{F}$ specifying its local distributions $\mathcal{F}_S$ for each $S \subseteq [n]_{\leq k}$. We define the function $\mathcal{F}_S \colon \mathbb{F}^S \to \mathbb{C}$ by specifying its (local) Fourier coefficients as follows. We set the Fourier coefficient $\widehat{\mathcal{F}_S}(\alpha)$ to be $\frac{1}{q^{|S|}}$ if $\alpha \in \mathcal{V}$, and 0 otherwise.

We now show that each $\mathcal{F}_S$ is a distribution. For any $f \colon S \to \mathbb{F}$ we have

$$\mathcal{F}_S(f) = \sum_{\alpha \in \mathbb{F}^S} \widehat{\mathcal{F}_S}(\alpha)\chi_\alpha(f) = \sum_{\alpha \in \mathcal{V}_{\subseteq S}} \frac{1}{q^{|S|}}\chi_\alpha(f) = \frac{1}{q^{|S|}} \sum_{\alpha \in \mathcal{V}_{\subseteq S}} \omega^{\mathrm{Tr}(\langle \alpha, f \rangle)} \ .$$

For each $b \in \mathbb{F}$, let $\mathcal{V}_b \subseteq \mathcal{V}_{\subseteq S}$ be the set of $\alpha \in \mathcal{V}_{\subseteq S}$ where $\langle \alpha, f \rangle = b$. Let $\pi \colon \mathcal{V}_{\subseteq S} \to \mathbb{F}$ be the map where $\pi(\alpha) = \langle \alpha, f \rangle$. Since $\mathcal{V}_{\subseteq S}$ is a subspace, π is a homomorphism. It follows that either $\mathcal{V}_0 = \mathcal{V}_{\subseteq S}$ or $|\mathcal{V}_b| = |\mathcal{V}_0|$ for every $b \in \mathbb{F}$. In the first case, $\sum_{\alpha \in \mathcal{V}_{\subseteq S}} \omega^{\mathrm{Tr}(\langle \alpha, f \rangle)} = |\mathcal{V}_{\subseteq S}| \geq 0$. In the second case,

$$\sum_{\alpha \in \mathcal{V}_{\subseteq S}} \omega^{\mathrm{Tr}(\langle \alpha, f \rangle)} = \sum_{b \in \mathbb{F}} \sum_{\alpha \in \mathcal{V}_b} \omega^{\mathrm{Tr}(b)} = \sum_{b \in \mathbb{F}} |\mathcal{V}_b| \, \omega^{\mathrm{Tr}(b)} = |\mathcal{V}_0| \sum_{b \in \mathbb{F}} \omega^{\mathrm{Tr}(b)} = 0 \ .$$

This implies that in either case, $\mathcal{F}_S(f) \geq 0$, and so $\mathcal{F}_S$ is a distribution.

We now show that the collection of local distributions $\{\mathcal{F}_S\}_{S \subseteq [n]_{\leq k}}$ is indeed non-signaling. This follows from Lemma 4.9. If $\alpha \in \mathcal{V}$ then we have that $q^{|S|}\widehat{\mathcal{F}_S}(\alpha) = 1 = q^{|R|}\widehat{\mathcal{F}_R}(\alpha)$ for every $S, R \in [n]_{\leq k}$ such that $\mathrm{supp}(\alpha) \subseteq S \cap R$, and otherwise we have $q^{|S|}\widehat{\mathcal{F}_S}(\alpha) = 0 = q^{|R|}\widehat{\mathcal{F}_R}(\alpha)$. Thus, the collection of local distributions is a k-non-signaling function $\mathcal{F}$.

It remains to show that $\mathcal{F}$ satisfies the desired property. Observe that for every α, $q^n \widehat{\mathcal{F}}(\alpha) = q^{|\mathrm{supp}(\alpha)|}\widehat{\mathcal{F}}_{\mathrm{supp}(\alpha)}(\alpha) = 1$ if $\alpha \in \mathcal{V}$, and otherwise $\widehat{\mathcal{F}}(\alpha) = 0$. By Lemma 4.3 it follows that $\mathcal{F}$ has the desired properties.

6.3 Proof of Lemma 6.8

Let $\mathcal{V} = \{\alpha \in \mathbb{F}^n : T \vdash_k \alpha\}$. We show that $\mathcal{V}$ is a k-local subspace. Let $S \subseteq [n]_{\leq k}$. We need to show that $\mathcal{V}_{\subseteq S}$ is a linear subspace of $\mathbb{F}^n$. We first observe that 0^n is always in the set, as $T \vdash_k 0^n$ always.

Let $\alpha \in \mathcal{V}_{\subseteq S}$ and let $b \in \mathbb{F} \setminus \{0\}$. Then we have that $T \vdash_k \alpha$ which implies that $T \vdash_k b\alpha$. Since $\mathrm{supp}(b\alpha) = \mathrm{supp}(\alpha) \subseteq S$, it follows that $b\alpha \in \mathcal{V}_{\subseteq S}$.

Let $\alpha, \beta \in \mathcal{V}_{\subseteq S}$. Then, since $|\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)| \leq |S| \leq k$ we have that $(\alpha, \beta, \alpha + \beta)$ is a hyperedge in Γ_k. Thus, since $T \vdash_k \{\alpha, \beta\}$ it follows that $T \vdash_k \alpha + \beta$. Since $\mathrm{supp}(\alpha + \beta) \subseteq \mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta) \subseteq S$, it follows that $\alpha + \beta \in \mathcal{V}_{\subseteq S}$.

We have thus shown that $\mathcal{V}_{\subseteq S}$ is a linear subspace of $\mathbb{F}^n$, which completes the proof.

7 Non-testability of bivariate polynomials

In this section, we prove Theorem 1 and Theorem 2. The proof strategies for both theorems are nearly identical, and rely on Theorem 3.

7.1 The case of the row/column test

We let $\mathbf{C}$ be the linear code of bivariate polynomials $P\colon \mathbb{F}^2 \to \mathbb{F}$ of degree at most d in each variable, and let T be the set of α's in $\mathbf{C}^\perp$ where the support of α is contained in exactly one row or column.

We define the *rank* of an element in $\mathbf{C}^\perp$ to be

$$\mathsf{rank}_T(\alpha) := \min_{T' \subseteq T : \alpha \in \mathrm{span}(T')} \left|T'\right| \quad .$$

Note that since $\mathrm{span}(T) = \mathbf{C}^\perp$, the rank of α is well-defined for all $\alpha \in \mathbf{C}^\perp$.

We let $T_0 = T_{\leq d+2}$ denote the subset of T that only contains elements whose support is contained in exactly one row or column, and of weight $d+2$. With this notation, the non-signaling row/column bivariate low-degree test (i) samples $\alpha \leftarrow T_0$ uniformly at random, and (ii) checks that $\langle \alpha, \mathcal{F} \rangle = 0$.

The main theorem we prove is stated below, and is the formal statement of Theorem 1.

Theorem 6. *For every k with $2d+2 \leq k < \frac{7}{32}(d+2)^2$, there exists a k-non-signaling function such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in T_0$, and yet $\Delta_{2d+2}(\mathcal{F}, \mathcal{F}') \geq (1 - \frac{1}{|\mathbb{F}|})$ for every $(2d+2)$-non-signaling function $\mathcal{F}'$ that is $(\mathbf{C}, 2d+2)$-explainable.*

We begin the proof of Theorem 6 by showing the following lemma. This lemma follows from earlier statements, and outlines a sufficient condition to prove Theorem 6

Lemma 7.1. *Suppose that there exists $\alpha^* \in \mathbf{C}^\perp$ with $\mathrm{wt}(\alpha^*) = 2d+2$ such that for every $k < \frac{7}{32}(d+2)^2$ it holds that $T \not\vdash_k \alpha^*$. Then for every k with $2d+2 \leq k < \frac{7}{32}(d+2)^2$ there exists a k-non-signaling function $\mathcal{F}$ such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in T_0$, and yet $\Delta_{2d+2}(\mathcal{F}, \mathcal{F}') \geq 1 - \frac{1}{|\mathbb{F}|}$ for every $(2d+2)$-non-signaling function $\mathcal{F}'$ that is $(\mathbf{C}, 2d+2)$-explainable.*

Proof. Applying Lemma 6.7 and Lemma 6.8, for every k with $2d+2 \leq k < \frac{7}{32}(d+2)^2$, we get that there exists a k-non-signaling function $\mathcal{F}$ such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in T_0$ and $\Pr[\langle \alpha^*, \mathcal{F} \rangle = 0] = \frac{1}{|\mathbb{F}|}$. Let $\mathcal{F}'$ be a $(2d+2)$-non-signaling function that is $(\mathbf{C}, 2d+2)$-explainable. Since for every $S \subseteq \mathbb{F}^2$ with $|S| \leq 2d+2$ we have that $\Pr[\mathcal{F}'(S) \in \mathbf{C}|_S] = 1$ and $\alpha^* \in \mathbf{C}^\perp$ has $\mathrm{wt}(\alpha^*) = 2d+2$, it follows that $\Pr[\langle \alpha^*, \mathcal{F}' \rangle = 0] = 1$. Therefore, $\Delta_{2d+2}(\mathcal{F}, \mathcal{F}') \geq |\Pr[\langle \alpha^*, \mathcal{F} \rangle = 0] - \Pr[\langle \alpha^*, \mathcal{F}' \rangle = 0]| = 1 - \frac{1}{|\mathbb{F}|}$. □

Therefore, by Lemma 7.1 it suffices to find such an α^*. We let $\alpha^* \in \mathbf{C}^\perp$ be any constraint where $\mathrm{supp}(\alpha)$ has size $2d+2$ and is contained on the diagonal of $\mathbb{F}^{n \times n}$, i.e. $\{(a,a) : a \in \mathbb{F}\} \subseteq \mathbb{F}^{n \times n}$. We note that α^* is one of the constraints that checks that $P(t,t)$ is a univariate polynomial of degree at most $2d$ in t.

We show that α^* satisfies the desired properties in two main lemmas. We first show the following generic lemma, which gives us a way to prove that $T \not\vdash_k \alpha^*$.

Lemma 7.2 (Interval cut Lemma)**.** *Fix $\alpha \in \mathbf{C}^\perp$. Suppose that there exists $r \in \mathbb{R}$ with $2 \leq r \leq \mathsf{rank}_T(\alpha)$ such that for every $\beta \in \mathbf{C}^\perp$ with $\mathsf{rank}_T(\beta) \in [r/2, r)$ it holds that $T \not\vdash_k \beta$. Then $T \not\vdash_k \alpha$.*

We then show that every $\alpha \in \mathbf{C}^\perp$ of rank in $[(d+2)/4, (d+2)/2]$ must have large weight, implying that they are not reachable from 0^n in $\Gamma_k(\mathbf{C}^\perp, T)$ when k is small.

Lemma 7.3. *For every $\beta \in \mathbf{C}^\perp$ with $\mathsf{rank}_T(\beta) \in [(d+2)/4, (d+2)/2]$ it holds that $\mathrm{wt}(\beta) \geq \frac{7}{32}(d+2)^2$. In particular, if $k < \frac{7}{32}(d+2)^2$ then $T \not\vdash_k \beta$.*

With the above two lemmas, we now finish the proof of Theorem 6.

Proof of Theorem 6. Let $k < \frac{7}{32}(d+2)^2$. We first observe that $\mathsf{rank}_T(\alpha^*) \geq 2d+2$, as every element of T contains at most one non-zero point on the diagonal. Since $k < \frac{7}{32}(d+2)^2$, Lemma 7.3 implies that $T \not\vdash_k \beta$ for every β with $\mathsf{rank}_T(\beta) \in [(d+2)/4, (d+2)/2]$. Thus, by Lemma 7.2 it follows that $T \not\vdash_k \alpha^*$. Hence, α^* satisfies the assumptions of Lemma 7.1, and so applying Lemma 7.1 completes the proof of Theorem 6. □

Next we turn to the proofs of Lemma 7.2 and Lemma 7.3.

Proof of Lemma 7.2. First, observe that by definition of rank, $\mathsf{rank}_T(\alpha_1 + \alpha_2) \leq \mathsf{rank}_T(\alpha_1) + \mathsf{rank}_T(\alpha_2)$. By the assumption of the lemma, there exists $r \in \mathbb{R}$ with $2 \leq r \leq \mathsf{rank}_T(\alpha)$ such that for every $\beta \in \mathbf{C}^\perp$ with $\mathsf{rank}_T(\beta) \in [r/2, r)$ it holds that $T \not\vdash_k \beta$. We need to show that $T \not\vdash_k \alpha$.

Suppose toward a contradiction that $T \vdash_k \alpha$. Then there exists a path $(\alpha_1, \ldots, \alpha_t = \alpha)$ in $\Gamma_k(\mathbf{C}^\perp, T)$ from 0^n to α. Let S_1 be the set of α_i's such that $\mathsf{rank}_T(\alpha_i) < r/2$, and let S_2 be the set of α_i's such that $\mathsf{rank}_T(\alpha_i) \geq r$. Note that $S_1 \cup S_2 = \{\alpha_1, \ldots, \alpha_t\}$, as otherwise there would exist some i such that α_i has rank in $[r/2, r)$, which would contradict the assumption that $T \vdash_k \alpha_i$ for all $i \in [t]$.

Since $\mathsf{rank}_T(\alpha) \geq r$ it follows that $\alpha \in S_2$, and hence $S_2 \neq \emptyset$. Let ℓ be the smallest index such that $\alpha_\ell \in S_2$. We have that $\alpha_\ell \neq 0^n$ since $\alpha_\ell \in S_2$, and there does not exist $i < \ell$ and $b \in \mathbb{F} \setminus \{0\}$ such that $\alpha_\ell = b\alpha_i$, as then $\mathsf{rank}_T(\alpha_i) = \mathsf{rank}_T(\alpha_\ell) \geq r$, thus contradicting the minimality of ℓ. Suppose that there exists $i < \ell$ and $\gamma \in T$ such that $\alpha_\ell = \alpha_i + \gamma$. By the minimality of ℓ, we must have that $\alpha_i \in S_1$, and hence $r \leq \mathsf{rank}_T(\alpha_\ell) \leq \mathsf{rank}_T(\alpha_i) + \mathsf{rank}_T(\gamma) < r/2 + 1 \leq r/2 + r/2 = r$, which is also a contradiction. Therefore, there must either exist $j_1, j_2 < \ell$ such that $\alpha_\ell = \alpha_{j_1} + \alpha_{j_2}$. By the minimality of ℓ, we must have that $\alpha_{j_1}, \alpha_{j_2} \in S_1$, and hence $r \leq \mathsf{rank}_T(\alpha_\ell) \leq \mathsf{rank}_T(\alpha_{j_1}) + \mathsf{rank}_T(\alpha_{j_1}) < r/2 + r/2 = r$, which is, again, a contradiction. In all cases we have reached a contradiction to the assumption that $T \vdash_k \alpha$, which completes the proof of Lemma 7.2. □

Remark 7.4. We note that in the foregoing proof we only required that rank_T is subadditive, i.e., that $\mathsf{rank}_T(\alpha_1 + \alpha_2) \leq \mathsf{rank}_T(\alpha_1) + \mathsf{rank}_T(\alpha_2)$, $\mathsf{rank}_T(\alpha) = 1$ for every $\alpha \in T$, and $\mathsf{rank}_T(0^n) = 0$. Thus, the Interval Cut Lemma holds for any such subadditive function.

Proof of Lemma 7.3. Let $\beta \in \mathbf{C}^\perp$ be such that $\mathsf{rank}_T(\beta) = r \in [\frac{d+2}{4}, \frac{d+2}{2}]$. We show that $\mathrm{wt}(\beta) \geq \frac{7}{32}(d+2)^2$. Since $\beta \in \mathrm{span}(T)$, we can write $\beta = \sum_{i=1}^{s} \beta_i + \sum_{i'=1}^{t} \beta'_{i'}$ with $s + t = r$, where each $\beta_i \in T$ is a constraint whose support is contained in exactly one row, and each $\beta'_{i'} \in T$ is a constraint whose support is contained in exactly one column. Note that there are no $i \neq j \in [s]$ such that $\mathrm{supp}(\beta_i)$ and $\mathrm{supp}(\beta_j)$ are contained in the same row, as otherwise we could use $\beta_{i,j} = \beta_i + \beta_j$ instead of the two terms, which contradicts the assumption that $\mathsf{rank}_T(\beta) = r$. Similarly, there are no $i' \neq j' \in [t]$ such that $\mathrm{supp}(\beta'_{i'})$ and $\mathrm{supp}(\beta'_{j'})$ are contained in the same column.

Observe that for any $i \in [s], i' \in [t]$ it holds that $\left|\mathrm{supp}(\beta_i) \cap \mathrm{supp}(\beta'_{i'})\right| \leq 1$. Therefore, $\mathrm{wt}(\beta) = \mathrm{wt}(\sum_{i=1}^{s} \beta_i + \sum_{i'=1}^{t} \beta'_{i'}) \geq \sum_{i=1}^{s} \mathrm{wt}(\beta_i) + \sum_{i=1}^{t} \mathrm{wt}(\beta'_{i'}) - 2st$. The term $-2st$ comes from the fact

that if $\left|\mathrm{supp}(\beta_i) \cap \mathrm{supp}(\beta'_{i'})\right| = 1$, then the two constraints may cancel each other on the intersection point, and we have counted this point twice: once in $\mathrm{wt}(\beta_i)$ and once in $\mathrm{wt}(\beta'_{i'})$. Therefore, using that fact that $s + t = r$ and that $\mathrm{wt}(\beta_i), \mathrm{wt}(\beta'_{i'})$ are at least $d + 2$ for every $i \in [s], i' \in [t]$ we get

$$\mathrm{wt}(\beta) \geq \sum_{i=1}^{s} \mathrm{wt}(\beta_i) + \sum_{i=1}^{t} \mathrm{wt}(\beta'_{i'}) - 2st \geq (s+t)(d+2) - 2st \geq r(d+2) - r^2/2 \ ,$$

where the last inequality uses the fact that $st = s(r-s)$ is maximized when $s = t = r/2$. Finally, the function $f(r) = r(d+2) - r^2/2$ for $r \in [\frac{d+2}{4}, \frac{d+2}{2}]$ is minimized when $r = \frac{d+2}{4}$, and hence

$$\mathrm{wt}(\beta) \geq r(d+2) - r^2/2 \geq \frac{(d+2)^2}{4} - \frac{(d+2)^2}{32} = \frac{7}{32}(d+2)^2 \ ,$$

as required. □

7.2 The case of the random lines test

We now prove Theorem 2. The random lines test for total degree d works as follows. Given a function $f\colon \mathbb{F}^2 \to \mathbb{F}$, the test: (1) samples a random line L from the set of all lines in $\mathbb{F}^2$; (2) samples a random subset $S \subseteq L$ of size $d+2$; (3) checks that $f|_S$ is a univariate polynomial of degree d. Similar to before, we let $\mathbf{C}$ be the set of bivariate polynomials of total degree d and let T be the subset of $\mathbf{C}^\perp$ containing all α's where $\mathrm{supp}(\alpha)$ is contained on a line. We let $T_0 = T_{\leq d+2}$. The random lines test is equivalent to sampling a random $\alpha \in T_0$ and checking that $\langle \alpha, f \rangle = 0$.

Formally, we prove the following theorem, which is the analogue of Theorem 1 for the random lines test.

Theorem 7. *For every k with $2d+2 \leq k < \frac{3}{16}(d+2)^2$, there exists a k-non-signaling function such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1$ for every $\alpha \in T_0$, and yet $\Delta_{2d+2}(\mathcal{F}, \mathcal{F}') \geq (1 - \frac{1}{|\mathbb{F}|})$ for every $(2d+2)$-non-signaling function $\mathcal{F}'$ that is $(\mathbf{C}, 2d+2)$-explainable.*

The proof of Theorem 1 for the row/column test implies that in order to show Theorem 7, it suffices to show the following lemma.

Lemma 7.5. *There exists $\alpha^* \in \mathbf{C}^\perp$ where $\mathrm{wt}(\alpha^*) = 2d+2$ and $\mathsf{rank}_T(\alpha^*) \geq (d+2)/2$, and for every $\alpha \in \mathbf{C}^\perp$ with $\mathsf{rank}_T(\alpha) \in [(d+2)/4, (d+2)/2)$ it holds that $\mathrm{wt}(\alpha) \geq \frac{3}{16}(d+2)^2$.*

Proof. For any bivariate polynomial $P(x,y)$ of degree d, the polynomial $P(t,t^2)$ has degree $\leq 2d$. Therefore, there exists at least one $\alpha^* \in \mathbf{C}^\perp$ that checks that $P(t,t^2)$ has degree $\leq 2d$. In particular, this α^* has $\mathrm{wt}(\alpha^*) = 2d+2$ and has support contained on the curve $x^2 - y = 0$. Since the curve $x^2 - y = 0$ is irreducible in $\mathbb{F}[x,y]$, any line L intersects the curve on at most 2 distinct points. It follows that $\mathsf{rank}_T(\alpha^*) \geq (2d+2)/2 = d+1$, as any constraint $\beta \in T$ can only have at most 2 points on the curve $x^2 - y = 0$.

Let $\beta \in \mathbf{C}^\perp$ be such that $\mathsf{rank}_T(\beta) = r \in [(d+2)/4, (d+2)/2]$. Then there exist lines $L_1, \ldots, L_r$ such that $\beta = \sum_{i=1}^{r} \beta_i$ where $\mathrm{supp}(\beta_i) \subseteq L_i$. The L_i's must be distinct, as otherwise we could add two constraints contained in the same line and we would then get $\mathsf{rank}_T(\beta) < r$. We have that $\mathrm{wt}(\beta_i) \geq d+2$ for each i. Hence, $\mathrm{wt}(\beta) \geq r(d+2) - 2\binom{r}{2}$, since each β_i contributes at least $d+2$ to the weight, and there are at most $\binom{r}{2}$ intersection points as each of the r lines is distinct. It follows that $\mathrm{wt}(\beta) \geq r(d+2) - r^2 \geq \frac{3}{16}(d+2)^2$ as $r \in [(d+2)/4, (d+2)/2]$, which completes the proof. □

8 On robust local characterizations

In this section we prove Theorem 4. In Section 8.1 we prove part 1 of the theorem, and in Section 8.2 we prove part 2. Finally, in Section 8.3 we show that Theorem 4 is tight for the repetition code and is tight up to a constant factor for the Hadamard code.

8.1 Part 1 of Theorem 4

We prove part 1 of Theorem 4. In order to do this, we must first formally define nsrank_T. We define

$$\mathsf{nsrank}_T(\alpha) := \min_P \mathsf{cost}_P(\alpha) \ ,$$

where the minimum is taken over all paths P from 0^n to α in $\Gamma_k(\mathbf{C}^\perp, T)$, and $\mathsf{cost}_P(\alpha)$ is defined according to the following definition:

Definition 8.1. *Let $P = (\alpha_1, \ldots, \alpha_r)$ be a path from 0^n to α in $\Gamma_k(\mathbf{C}^\perp, T)$ as in Definition 6.4. For each $i \in [r]$, we define $\mathsf{cost}_P(\alpha_i)$ recursively as follows.*

1. *(Base case) $\mathsf{cost}_P(\alpha_1) = \mathsf{cost}_P(0^n) = 0$.*
2. *(Edge type 1) if there exists $j < i$ with $(\alpha_j, \alpha_i) \in E$ such that $\alpha_i = b\alpha_j$ for some $b \in \mathbb{F} \setminus \{0\}$, then $\mathsf{cost}_P(\alpha_i) = \mathsf{cost}_P(\alpha_j)$.*
3. *(Edge type 2) if there exists $j < i$ with $(\alpha_j, \alpha_i) \in E$ such that $\alpha_i = \alpha_j + \gamma$ for some $\gamma \in T$, then $\mathsf{cost}_P(\alpha_i) = \mathsf{cost}_P(\alpha_j) + 1$.*
4. *(Hyperedge) if there exists $j_1, j_2 < i$ with $(\alpha_{j_1}, \alpha_{j_2}, \alpha_i) \in H$, then $\mathsf{cost}_P(\alpha_i) = \mathsf{cost}_P(\alpha_{j_1}) + \mathsf{cost}_P(\alpha_{j_2})$.*

If more than one of the above cases hold for a particular α_i, then $\mathsf{cost}_P(\alpha_i)$ is defined to be the minimum over all possible cases.

Intuitively, the function $\mathsf{cost}_P(\cdot)$ is counting the number of edges of the form $(\alpha, \alpha + \gamma)$ with $\gamma \in T$ that are used in the path P, only one can use hyperedges and they cost more. The cost of taking a hyperedge $(\alpha, \beta, \alpha + \beta)$ is equal to the cost to reach α plus the cost to reach β.

We note that $\mathsf{nsrank}_T(\alpha)$ implicitly depends on k. In fact, when $k = n$ we have that $\mathsf{nsrank}_T(\alpha) = \mathsf{rank}_T(\alpha)$, which motivates nsrank as a non-signaling analogue of rank.

Using the definition above, we prove part 1 of Theorem 4. Suppose that $\mathcal{F}$ is a k-non-signaling function such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \varepsilon$ for every $\alpha \in T$. Let $\alpha \in \mathbb{F}^n_{\leq k}$ be such that $T \vdash_k \alpha$. We show that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{nsrank}_T(\alpha)\varepsilon$.

Let $P = (\alpha_1, \ldots, \alpha_r)$ be a path from 0^n to α in $\Gamma_k(\mathbf{C}^\perp, T)$ such that $\mathsf{cost}_P(\alpha)$ is minimal, i.e., such that $\mathsf{nsrank}_T(\alpha) = \min_P \mathsf{cost}_P(\alpha)$. Let $\mathsf{cost}_P(\alpha_i)$ be the non-negative integers assigned to each $\alpha_i \in P$. We prove that for all $i \in [r]$ it holds that $\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_i)\varepsilon$. The proof is by induction on i.

For the base case of $i = 1$ indeed holds $\Pr[\langle \alpha_1, \mathcal{F} \rangle = 0] = 1 = 1 - \mathsf{cost}_P(\alpha_1)\varepsilon$. For the induction step let $i > 1$, and consider the following three cases.

1. If α_i is reached using an edge of the form $(\alpha_j, \alpha_i = b\alpha_j)$ for some $b \in \mathbb{F} \setminus \{0\}$ and $j < i$, then $\mathsf{cost}_P(\alpha_i) = \mathsf{cost}_P(\alpha_j)$. By the induction hypothesis $\Pr[\langle \alpha_j, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_j)\varepsilon$, and hence

$$\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = \Pr[\langle b\alpha_j, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_j, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_j)\varepsilon = 1 - \mathsf{cost}_P(\alpha_i)\varepsilon \ .$$

2. If α_i is reached using an edge of the form $(\alpha_j, \alpha_i = \alpha_j + \gamma)$ for some $\gamma \in T$ and $j < i$, then by the induction hypothesis $\Pr[\langle \alpha_j, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_j)\varepsilon$, and hence

   $$\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_j + \gamma, \mathcal{F} \rangle = 0] \geq \Pr[\langle \alpha_j, \mathcal{F} \rangle = 0 \wedge \langle \gamma, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_j)\varepsilon - \varepsilon = 1 - \mathsf{cost}_P(\alpha_i)\varepsilon \ ,$$

   by union bound. Therefore, also in this case $\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_i)\varepsilon$.

3. Otherwise, α_i is reached using a hyperedge $(\alpha_{j_1}, \alpha_{j_2}, \alpha_i = \alpha_{j_1} + \alpha_{j_2})$, then

   $$\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] = \Pr[\langle \alpha_{j_1} + \alpha_{j_2}, \mathcal{F} \rangle = 0] \geq \Pr[\langle \alpha_{j_1}, \mathcal{F} \rangle = 0 \wedge \langle \alpha_{j_2}, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_{j_1})\varepsilon - \mathsf{cost}_P(\alpha_{j_2})\varepsilon \ ,$$

   by the induction hypothesis and union bound. Since $\mathsf{cost}_P(\alpha_i) = \mathsf{cost}_P(\alpha_{j_1}) + \mathsf{cost}_P(\alpha_{j_2})$, it follows that $\Pr[\langle \alpha_i, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_i)\varepsilon$, as required.

By induction, we conclude that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] \geq 1 - \mathsf{cost}_P(\alpha_r)\varepsilon = 1 - \mathsf{nsrank}_T(\alpha)\varepsilon$, which completes the proof.

8.2 Part 2 of Theorem 4

We prove part 2 of Theorem 4 by showing the following lemma.

Lemma 8.2. *Let $\mathsf{cost}\colon \mathbb{F}^n \to \mathbb{Z}_{\geq 0}$ be a function such that for every $\alpha \in \mathbb{F}^n$, if $\alpha = \sum_{i=1}^n \alpha_i e_i$, then $\mathsf{cost}(\alpha) = \sum_{i:\alpha_i \neq 0} \mathsf{cost}(e_i)$. Let $M\colon \mathbb{F}^n \to \mathbb{F}^n$ be a linear transformation. Let $\mathcal{W}$ be a k-local subspace, and let $\varepsilon \geq 0$ be such that $1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon \geq 0$ for every $\alpha \in \mathcal{W}$. Then there exists a k-non-signaling function $\mathcal{F}$ such that $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = 1 - \mathsf{cost}(M\alpha)\varepsilon$ for every $\alpha \in \mathcal{W}$, and $\Pr[\langle \alpha, \mathcal{F} \rangle = 0] = \frac{1}{|\mathbb{F}|}$ otherwise.*

Part 2 of Theorem 4 follows from Lemma 8.2 by setting $\mathsf{cost}(e_i) = 1$ for each $i \in [n]$, and letting M be the identity matrix.

Note that the assumptions on cost in Lemma 8.2 imply that $\mathsf{cost}(0^n) = 0$, and for every $\alpha \in \mathbb{F}^n$ and $b \in \mathbb{F} \setminus \{0\}$, we have that $\mathsf{cost}(\alpha) = \mathsf{cost}(b\alpha)$. In addition, if we let $\pi_i\colon \mathbb{F}^n \to \mathbb{F}$ be the projection map $\alpha \mapsto \alpha_i$, and let $h_i\colon \mathbb{F}^n \to \mathbb{Z}$ be the map which sends $\alpha \mapsto 1$ if $\alpha_i \neq 0$ and $\alpha \mapsto 0$ otherwise, then $\mathsf{cost}(\alpha) = \sum_{i=1}^n h_i(\alpha)\mathsf{cost}(e_i)$.

The following lemma will be used in the proof. We delay the proof of the lemma until after the proof of Lemma 8.2.

Lemma 8.3. *Let $\mathcal{V} \subseteq \mathbb{F}^n$ be a linear subspace. Then for every subspace $\mathcal{V}_0 \subseteq \mathcal{V}$ of co-dimension 1 it holds that $\frac{1}{q-1}\sum_{\alpha \in \mathcal{V} \setminus \mathcal{V}_0} \mathsf{cost}(\alpha) - \sum_{\alpha \in \mathcal{V}_0} \mathsf{cost}(\alpha) \geq 0$.*

Proof of Lemma 8.2. As in the proof of Lemma 6.7, we define each $\mathcal{F}_S$ first as a function $\mathbb{F}^S \to \mathbb{C}$ by specifying its Fourier coefficients. In particular, we set $\widehat{\mathcal{F}_S} = \frac{1}{q^{|S|}} \cdot (1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon)$ if $\alpha \in \mathcal{W}$, and 0 otherwise.

We now finish the proof assuming that each $\mathcal{F}_S$ is in fact a distribution. By Lemma 4.9, it follows that the collection of local distributions $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq [n]_{\leq k}}$ is k-non-signaling, and by Lemma 4.3 it follows that $\mathcal{F}$ has the desired properties, completing the proof.

It remains to show that each $\mathcal{F}_S$ is a distribution. Since $\mathsf{cost}(0^n) = 0$, we have that $\widehat{\mathcal{F}_S}(0^S) = \frac{1}{q^{|S|}}$, and hence $\sum_{f \in \mathbb{F}^S} \mathcal{F}_S(f) = 1$. So, it remains to show that $\mathcal{F}_S(f) \geq 0$ for each $f \in \mathbb{F}^S$.

Let $\mathcal{V} = \mathcal{W}_{\subseteq S}$. Note that by definition of $\mathcal{F}_S$ we have that

$$\mathcal{F}_S(f) = \sum_{\alpha \in \mathbb{F}^S} \widehat{\mathcal{F}_S}(\alpha)\chi_\alpha(f) = \sum_{\alpha \in \mathcal{V}} \left(1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon\right) \cdot \frac{1}{q^{|S|}} \omega^{-\mathrm{Tr}(\langle \alpha, f\rangle)} \ ,$$

since $\widehat{\mathcal{F}_S}(\alpha) = 0$ when $\alpha \notin \mathcal{V}$. For any $\alpha \in \mathcal{V}$, if $\langle \alpha, f\rangle = 0$ then $\sum_{b \in \mathbb{F}\setminus\{0\}} \omega^{-\mathrm{Tr}(\langle b\alpha, f\rangle)} = q-1$. Otherwise, $\sum_{b \in \mathbb{F}\setminus\{0\}} \omega^{-\mathrm{Tr}(\langle b\alpha, f\rangle)} = -1$.

Let $\mathcal{V}_0 \subseteq \mathcal{V}$ be the subspace containing all $\alpha \in \mathcal{V}$ such that $\langle \alpha, f\rangle = 0$. Since $\mathsf{cost}(M\alpha) = \mathsf{cost}(M(b\alpha))$ for all $b \in \mathbb{F} \setminus \{0\}$, the above computation shows that

$$q^{|S|}\mathcal{F}_S(f) = \sum_{\alpha \in \mathcal{V}_0} \left(1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon\right) + \frac{-1}{q-1} \cdot \sum_{\alpha \in \mathcal{V}\setminus\mathcal{V}_0} \left(1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon\right) \ .$$

There are two cases. If $\mathcal{V}_0 = \mathcal{V}$, then $q^{|S|}\mathcal{F}_S(f) = \sum_{\alpha \in \mathcal{V}_0} \left(1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon\right) \geq 0$ by assumption. If $\mathcal{V}_0 \subsetneq \mathcal{V}$, then $\mathcal{V}_0$ is a subspace of co-dimension 1, as it is specified by one linear constraint. Let $\gamma \in \mathcal{V} \setminus \mathcal{V}_0$. Then

$$\begin{aligned} q^{|S|}\mathcal{F}_S(f) &= \sum_{\alpha \in \mathcal{V}_0} \left(1 - \frac{q}{q-1}\mathsf{cost}(M\alpha)\varepsilon + \frac{-1}{q-1} \cdot \sum_{b \in \mathbb{F}\setminus\{0\}} 1 - \frac{q}{q-1}\mathsf{cost}(M(\alpha + b\gamma))\varepsilon\right) \\ &= \frac{q}{q-1}\varepsilon \cdot \sum_{\alpha \in \mathcal{V}_0} \left(-\mathsf{cost}(M\alpha) + \frac{1}{q-1} \cdot \sum_{b \in \mathbb{F}\setminus\{0\}} \mathsf{cost}(M(\alpha + b\gamma))\right) \ . \end{aligned}$$

If $M\gamma = 0^n$, then we have that $\mathsf{cost}(M\alpha) = \mathsf{cost}(M(\alpha + b\gamma))$ for every $b \in \mathbb{F}$, which implies that the above sum is 0. Hence, $\mathcal{F}_S(f) \geq 0$ in this case. If $M\gamma \neq 0^n$, then $M\mathcal{V}_0 \subsetneq M\mathcal{V}$ is a subspace of co-dimension 1. The remainder of the proof follows from Lemma 8.3 applied to the subspaces $M\mathcal{V}_0 \subseteq M\mathcal{V}$. □

We now prove Lemma 8.3

Proof of Lemma 8.3. Let $\mathcal{V}_0 \subseteq \mathcal{V}$ be a subspace of co-dimension 1. Since $\mathcal{V}_0 \neq \mathcal{V}$, there exists an element $\gamma \in \mathcal{V} \setminus \mathcal{V}_0$. We have that

$$\begin{aligned} &\frac{1}{q-1} \sum_{\alpha \in \mathcal{V}\setminus\mathcal{V}_0} \mathsf{cost}(\alpha) - \sum_{\alpha \in \mathcal{V}_0} \mathsf{cost}(\alpha) = \sum_{\alpha \in \mathcal{V}_0} \left(-\mathsf{cost}(\alpha) + \frac{1}{q-1} \sum_{b \neq 0} \mathsf{cost}(\alpha + b\gamma)\right) \\ &= \sum_{i=1}^{n} \mathsf{cost}(e_i) \sum_{\alpha \in \mathcal{V}_0} \left(-h_i(\alpha) + \frac{1}{q-1} \sum_{b \neq 0} h_i(\alpha + b\gamma)\right) \ . \end{aligned}$$

Let $i \in [n]$. Observe that if $\gamma_i = 0$, then $-h_i(\alpha) + \frac{1}{q-1}\sum_{b \neq 0} h_i(\alpha + b\gamma) = 0$ for every $\alpha \in \mathcal{V}_0$. Let $i \in [n]$ such that $\gamma_i \neq 0$. Observe that if $h_i(\alpha) = 0$, then $-h_i(\alpha) + \frac{1}{q-1}\sum_{b \neq 0} h_i(\alpha + b\gamma) = 1$, as $h_i(\alpha + b\gamma) = 1$ for every $b \in \mathbb{F} \setminus \{0\}$ as $\gamma_i \neq 0$, and $h_i(\alpha) = 0$. If $h_i(\alpha) = 1$, then $-h_i(\alpha) + \frac{1}{q-1}\sum_{b \neq 0} h_i(\alpha + b\gamma) = -\frac{1}{q-1}$, as then there exists a unique $b^* \in \mathbb{F} \setminus \{0\}$ such that $h_i(\alpha + b^*\gamma) = 0$ and $h_i(\alpha + b\gamma) = 1$ for all other b.

Now, either $h_i(\alpha) = 0$ for every $\alpha \in \mathcal{V}_0$, or $h_i(\alpha) = 1$ for some $\alpha \in \mathcal{V}_0$. In the first case, we have that $\sum_{\alpha\in\mathcal{V}_0}\left(-h_i(\alpha) + \frac{1}{q-1}\sum_{b\neq 0} h_i(\alpha+b\gamma)\right) = |\mathcal{V}_0| \geq 0$, as each term in the sum is 1. The second case is more complicated. If $h_i(\alpha) = 1$ for some $\alpha \in \mathcal{V}_0$, then we have that $\sum_{\alpha\in\mathcal{V}_0}\left(-h_i(\alpha) + \frac{1}{q-1}\sum_{b\neq 0} h_i(\alpha+b\gamma)\right) = |\{\alpha \in \mathcal{V}_0 : h_i(\alpha) = 0\}| - \frac{1}{q-1}|\{\alpha \in \mathcal{V}_0 : h_i(\alpha) = 1\}|$. In this case, the linear homomorphism $\pi_i \colon \mathcal{V}_0 \to \mathbb{F}$ has $\pi_i(\alpha) \neq 0$ for some $\alpha \in \mathcal{V}_0$, which implies that $|\{\alpha \in \mathcal{V}_0 : \pi(\alpha) = 0\}| = |\{\alpha \in \mathcal{V}_0 : \pi(\alpha) = b\}|$ for every $b \in \mathbb{F}$. In particular, $|\{\alpha \in \mathcal{V}_0 : h_i(\alpha) = 0\}| = \frac{1}{q-1}|\{\alpha \in \mathcal{V}_0 : h_i(\alpha) = 1\}|$. This implies that $\sum_{\alpha\in\mathcal{V}_0}\left(-h_i(\alpha) + \frac{1}{q-1}\sum_{b\neq 0} h_i(\alpha+b\gamma)\right) = 0$. Hence,

$$\frac{1}{q-1}\sum_{\alpha\in\mathcal{V}\setminus\mathcal{V}_0}\mathsf{cost}(\alpha) - \sum_{\alpha\in\mathcal{V}_0}\mathsf{cost}(\alpha) = \sum_{i=1}^{n}\mathsf{cost}(e_i)\sum_{\alpha\in\mathcal{V}_0}\left(-h_i(\alpha) + \frac{1}{q-1}\sum_{b\neq 0} h_i(\alpha+b\gamma)\right) \geq 0 \ ,$$

as $\sum_{\alpha\in\mathcal{V}_0}\left(-h_i(\alpha) + \frac{1}{q-1}\sum_{b\neq 0} h_i(\alpha+b\gamma)\right) \geq 0$ for each $i \in n$. □

8.3 On the tightness of Theorem 4

We now show that Theorem 4 is tight when $\mathbf{C}$ is the repetition code and is tight up to a factor of 3 when $\mathbf{C}$ is the Hadamard code. We begin by stating the following proposition.

Proposition 8.4. *Let T be a set of local constraints, and let $k \geq 0$. Then,*

- $\mathsf{nsrank}_T(\alpha) \geq \mathsf{rank}_T(\alpha)$.
- $\mathsf{nsrank}_T \geq \mathrm{wt}(\alpha)/\ell$, *where* $\ell = \max_{\alpha\in T}\mathrm{wt}(\alpha)$.

The first statement follows immediately from the fact that any path of length r in the Cayley hypergraph can be mapped to a path of length $\leq r$ in the Cayley graph. The second statement follows immediately from the first one and the fact that if $\mathsf{rank}_T(\alpha) = r$ then $\mathrm{wt}(\alpha) \leq r\ell$.

Let $\mathbf{C}$ be the Hadamard code and $T = \{e_x + e_y - e_{x+y} : x, y \in \mathbb{F}^n\}$. In [CMS18] it is shown implicitly that $\mathsf{nsrank}_T(\alpha) \leq \mathrm{wt}(\alpha) - 2$. The above shows that $\mathsf{nsrank}_T(\alpha) \geq \mathrm{wt}(\alpha)/3$. This implies that for the Hadamard code, Theorem 4 is tight up to a factor of 3.

We now show the following lemma, which implies that Theorem 4 is tight for the repetition code.

Lemma 8.5. *If $\mathbf{C} = \{0^n, 1^n\} \subseteq \{0,1\}^n$ is the repetition code and $T = \{e_i + e_j : i, j \in [n]\}$ is the canonical test, then* $\mathsf{nsrank}_T(\alpha) = \mathrm{wt}(\alpha)/2$.

Proof. Observe that $\mathbf{C}^\perp = \{\alpha \in \{0,1\}^n : \sum_{i=1}^n \alpha_i = 0\}$. Note that in particular, $\mathrm{wt}(\alpha)$ is even for every $\alpha \in \mathbf{C}^\perp$. Let $\alpha \in \mathbf{C}^\perp$, and let $i_1, \ldots, i_\ell$ be the set of indices in $[n]$ such that $\alpha_{i_j} \neq 0$. Then $\alpha = (e_{i_1} + e_{i_2}) + (e_{i_3} + e_{i_4}) + \cdots + (e_{i_{\ell-1}} + e_{i_\ell}) = \alpha_1 + \cdots + \alpha_{\ell/2}$. Observe that if $T \vdash_k \alpha$, then $\mathrm{wt}(\alpha) \leq k$. Hence, the above gives a path in the Cayley hypergraph to α of length $\ell/2$, and so $\mathsf{nsrank}_T(\alpha) \leq \ell/2$. The earlier proposition implies that $\mathsf{nsrank}_T(\alpha) = \ell/2$, completing the proof. □

Acknowledgements

We are grateful to Thomas Vidick for suggesting using irreducible curves to extend our non-testability result about the row/column test to the random lines test.

References

[AB11] Samson Abramsky and Adam Brandenburger. "The sheaf-theoretic structure of non-locality and contextuality". In: *New Journal of Physics* 13.11 (2011), p. 113036.

[ALMSS98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. "Proof verification and the hardness of approximation problems". In: *Journal of the ACM* 45.3 (1998). Preliminary version in FOCS '92., pp. 501–555.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. "Self-Testing/Correcting with Applications to Numerical Problems". In: *Journal of Computer and System Sciences* 47.3 (1993), pp. 549–595.

[CMS18] Alessandro Chiesa, Peter Manohar, and Igor Shinkar. "Testing Linearity against Non-Signaling Strategies". In: *Proceedings of the 33rd Annual Conference on Computational Complexity*. CCC '18. 2018, 17:1–17:37.

[CMS19] Alessandro Chiesa, Peter Manohar, and Igor Shinkar. "Probabilistic Checking Against Non-Signaling Strategies from Linearity Testing". In: *Proceedings of the 10th Innovations in Theoretical Computer Science Conference*. ITCS '19. 2019, 25:1–25:17.

[GS06] Oded Goldreich and Madhu Sudan. "Locally testable codes and PCPs of almost-linear length". In: *Journal of the ACM* 53 (4 2006). Preliminary version in STOC '02., pp. 558–655.

[GVZ14] Parikshit Gopalan, Salil P. Vadhan, and Yuan Zhou. "Locally testable codes and Cayley graphs". In: *Proceedings of the 5th Innovations in Theoretical Computer Science Conference*. ITCS '14. 2014, pp. 81–92.

[KRR13] Yael Kalai, Ran Raz, and Ron Rothblum. "Delegation for Bounded Space". In: *Proceedings of the 45th ACM Symposium on the Theory of Computing*. STOC '13. 2013, pp. 565–574.

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. "How to delegate computations: the power of no-signaling proofs". In: *Proceedings of the 46th ACM Symposium on Theory of Computing*. STOC '14. Full version available at `https://eccc.weizmann.ac.il/report/2013/183/`. 2014, pp. 485–494.

[KRR16] Yael Tauman Kalai, Ran Raz, and Oded Regev. "On the Space Complexity of Linear Programming with Preprocessing". In: *Proceedings of the 7th Innovations in Theoretical Computer Science Conference*. ITCS '16. 2016, pp. 293–300.

[KT92] Leonid A Khalfin and Boris S Tsirelson. "Quantum/classical correspondence in the light of Bell's inequalities". In: *Foundations of physics* 22.7 (1992), pp. 879–948.

[NV18] Anand Natarajan and Thomas Vidick. "Low-Degree Testing for Quantum States, and a Quantum Entangled Games PCP for QMA". In: *Proceedings of the 59th IEEE Symposium on Foundations of Computer Science*. FOCS '18. 2018, pp. 731–742.

[PR94] Sandu Popescu and Daniel Rohrlich. "Quantum nonlocality as an axiom". In: *Foundations of Physics* 24.3 (1994), pp. 379–385.

[PS94] Alexander Polishchuk and Daniel A. Spielman. "Nearly-linear size holographic proofs". In: *Proceedings of the 26th ACM Symposium on Theory of Computing*. STOC '94. 1994, pp. 194–203.

[RS96] Ronitt Rubinfeld and Madhu Sudan. "Robust Characterizations of Polynomials with Applications to Program Testing". In: *SIAM Journal on Computing* 25.2 (1996), pp. 252–271.

[Ras85] Peter Rastall. "Locality, Bell's theorem, and quantum mechanics". In: *Foundations of Physics* 15.9 (1985), pp. 963–972.

[SA90] Hanif D. Sherali and Warren P. Adams. "A Hierarchy of Relaxations between the Continuous and Convex Hull Representations for Zero-One Programming Problems". In: *SIAM Journal on Discrete Mathematics* 3.3 (1990), pp. 411–430.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il