Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 67 (2018)

Testing Linearity against Non-Signaling Strategies

Alessandro Chiesa
alexch@berkeley.edu
UC Berkeley

Peter Manohar
manohar@berkeley.edu
UC Berkeley

Igor Shinkar
igors@berkeley.edu
UC Berkeley

August 28, 2018

Abstract

Non-signaling strategies are collections of distributions with certain non-local correlations. They have been studied in Physics as a strict generalization of quantum strategies to understand the power and limitations of Nature's apparent non-locality. Recently, they have received attention in Theoretical Computer Science due to connections to Complexity and Cryptography.

We initiate the study of Property Testing against non-signaling strategies, focusing first on the classical problem of *linearity testing* (Blum, Luby, and Rubinfeld; JCSS 1993). We prove that any non-signaling strategy that passes the linearity test with high probability must be close to a *quasi-distribution* over linear functions.

Quasi-distributions generalize the notion of probability distributions over global objects (such as functions) by allowing negative probabilities, while at the same time requiring that "local views" follow standard distributions (with non-negative probabilities). Quasi-distributions arise naturally in the study of Quantum Mechanics as a tool to describe various non-local phenomena.

Our analysis of the linearity test relies on Fourier analytic techniques applied to quasi-distributions. Along the way, we also establish general equivalences between non-signaling strategies and quasi-distributions, which we believe will provide a useful perspective on the study of Property Testing against non-signaling strategies beyond linearity testing.

Keywords: property testing; linearity testing; non-signaling strategies; quasi-distributions

ISSN 1433-8092

Contents

1 Introduction

Property Testing studies sublinear-time algorithms for approximate decision problems. A *tester* is an algorithm that receives oracle access to an input, samples a small number of locations, queries the input at these locations, and then decides whether to accept or reject. If the input has a certain property, the tester must accept with high probability; if instead the input is far from all inputs having this property, then the tester must reject with high probability.

Seminal works in Property Testing include those of Blum, Luby, and Rubinfeld [BLR93], who studied the problem of deciding whether the input is the evaluation table of a linear function or is far from any such table, and of Rubinfeld and Sudan [RS96], who studied the analogous problem for low-degree functions. Property Testing for general decision problems was introduced in the foundational work of Goldreich, Goldwasser, and Ron [GGR98].

We initiate the study of Property Testing when the input is a *non-signaling strategy* [KT85; Ras85; PR94; PR98], which means that the input belongs to a certain class of probabilistic oracles that answer a tester's queries by sampling from a distribution that may depend on all queries. This setting stands in stark contrast to the standard one, where each query's answer is *fixed* before queries are sampled. We provide a first analysis of linearity testing against non-signaling strategies, establishing general statements and techniques about non-signaling strategies along the way.

Non-signaling strategies have been studied in Physics for over 30 years as a strict generalization of quantum strategies, in order to understand the power and limitations of Nature's apparent non-locality.[1] Informally, Quantum Mechanics is a very accurate description of Nature but it may also be an incomplete one: it has not been successfully combined with General Relativity to get a quantum theory of gravity. Nevertheless, there is wide agreement that Nature forbids instantaneous communication despite its apparent non-locality, so this *non-signaling* property must be part of *any* ultimate theory of Nature. Non-signaling strategies exactly capture this minimal requirement, thus (purportedly) capturing any physically-realizable strategy.

Non-signaling strategies also have strong connections to Complexity Theory and Cryptography. Property Testing against non-signaling strategies is likely to strengthen these connections (see Section 4 for details), and thus we believe that it should be explicitly studied.

1.1 Linearity testing

A boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is *linear* if $f(x) + f(y) = f(x+y)$ for all $x, y \in \{0,1\}^n$, where bits are added modulo two and vectors are added component-wise. The problem of *linearity testing* is to decide whether a given arbitrary boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is linear or is far from all linear functions. Blum, Luby, and Rubinfeld [BLR93] suggest a very simple 3-query tester: sample uniform and independent $x, y \in \{0,1\}^n$, and check that $f(x) + f(y) = f(x+y)$. Perhaps surprisingly, analyzing this tester is far from simple, and a tight characterization of its acceptance probability is still an open problem. Nevertheless, upper and lower bounds on the acceptance probability are known, which is sufficient for applications. Bellare, Coppersmith, Håstad, Kiwi, and Sudan [BCHKS96] have shown that the acceptance probability is at most $1 - \Delta(f)$, where $\Delta(f)$ is the fractional Hamming distance of f to the closest linear function. Many other works have studied this problem and closely related ones [SW04; BCLR08; BKSSZ10; DDGKS17]. Finally, Ito and Vidick [IV12; Vid14] analyzed linearity testing against quantum strategies. Fixed functions and quantum strategies are both special cases of non-signaling strategies, the subject of this work.

[1] "Non-locality" refers to correlations in Nature that appear non-local when interpreted using classical physics.

1.2 Non-signaling strategies

A non-signaling strategy is a collection of distributions, one per set of queries, that jointly satisfy certain restrictions. There are two distinct definitions, corresponding to whether the strategy is meant to represent a function or players in a game. Throughout most of this paper, we consider *non-signaling functions*, because the functional view fits better the setting of Property Testing; nevertheless, we also consider *non-signaling players*, and show that our results about non-signaling functions imply corresponding results about non-signaling players (see Appendices D to F).

A *k-non-signaling function* $\mathcal{F}$ extends the notion of a function $f\colon \{0,1\}^n \to \{0,1\}$ as follows: it is a collection $\{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n,|S|\leq k}$ where each $\mathcal{F}_S$ is a *distribution* over functions $f_S\colon S \to \{0,1\}$ and, for every two subsets S and T each of size at most k, the restrictions of $\mathcal{F}_S$ and $\mathcal{F}_T$ to $S \cap T$ are equal as distributions. We sometimes write "$\mathcal{F}(S) = \vec{b}$", for a subset $S \subseteq \{0,1\}^n$ and string $\vec{b} \in \{0,1\}^S$, to denote the event that the function sampled from $\mathcal{F}_S$ equals $\vec{b}$.

Observe that, given any $k \in \{1,\ldots,2^n\}$, every function $f\colon \{0,1\}^n \to \{0,1\}$ naturally induces a k-non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n,|S|\leq k}$, namely the one where each $\mathcal{F}_S$ equals the constant distribution that outputs the restriction of f to S with probability 1. More generally, every distribution over functions induces a corresponding k-non-signaling function in a similar way.

However, the set of non-signaling functions is richer, because consistency between local distributions need *not* imply a global distribution, as the following example shows. For $n = 2$ and $k = 2$, consider the non-signaling function $\{\mathcal{F}_S\}_{S\subseteq\{0,1\}^2,|S|\leq 2}$ defined as follows: $\mathcal{F}_{\{00,11\}}$ is uniform over the two functions $\left\{ \begin{smallmatrix} 00\to 0 \\ 11\to 1 \end{smallmatrix} , \begin{smallmatrix} 00\to 1 \\ 11\to 0 \end{smallmatrix} \right\}$ and, for every $\{x,y\} \neq \{00,11\}$, $\mathcal{F}_{\{x,y\}}$ is uniform over $\left\{ \begin{smallmatrix} x\to 0 \\ y\to 0 \end{smallmatrix} , \begin{smallmatrix} x\to 1 \\ y\to 1 \end{smallmatrix} \right\}$. No distribution over functions can explain the above strategy, as any f in the support of such a distribution would have to satisfy $f(00) \neq f(11)$ and $f(x) = f(y)$ for every $\{x,y\} \subseteq \{0,1\}^2 \setminus \{00,11\}$, which is impossible.

1.3 The problem and challenges

We study linearity testing against non-signaling functions, which is the following problem.

Question 1.1 (informal)**.** *Let $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n,|S|\leq k}$ be a k-non-signaling function. Suppose that with probability at least $1-\varepsilon$ (for sufficiently small $\varepsilon \geq 0$) it holds that $f(x)+f(y) = f(x+y)$, where x and y are sampled uniformly and independently from $\{0,1\}^n$ and $f\colon \{x,y,x+y\} \to \{0,1\}$ is sampled from the distribution $\mathcal{F}_{\{x,y,x+y\}}$. Can we deduce any global properties about $\mathcal{F}$?*

In order to build intuition about this question, we temporarily put aside the case when $\varepsilon > 0$, and focus on the case $\varepsilon = 0$, which already turns out to be quite subtle. In other words, let us assume for now that for *every* $x, y \in \{0,1\}^n$ and *every* f in the support of $\mathcal{F}_{\{x,y,x+y\}}$ it holds that $f(x)+f(y) = f(x+y)$. What global properties, if any, can we deduce about $\mathcal{F}$?

Ideally, we would like to characterize the set of *all* non-signaling functions that pass the linearity test with probability 1 and say that this set is related to linear functions. If $\mathcal{F}$ is restricted to answer according to a single fixed function $f\colon \{0,1\}^n \to \{0,1\}$ (as in the standard setting) then f passing the linearity test with probability 1 is *equivalent* to f being linear by definition. On the other extreme, if $\mathcal{F}$ is allowed to answer queries arbitrarily without any non-signaling property then no interesting conclusion is possible. The case of $\mathcal{F}$ being a non-signaling function sits somewhere in between these two extremes: $\mathcal{F}$ is neither a fixed function nor completely arbitrary. We present two examples to highlight the challenges that arise when seeking an answer.

Example 1. Consider the following 3-non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n,|S|\leq 3}$. For every subset $\{x, y, x+y\} \subseteq \{0,1\}^n\backslash\{0^n\}$, the random variable $f \leftarrow \mathcal{F}_{\{x,y,x+y\}}$ is such that $(f(x), f(y), f(x+y))$ is uniform over $\{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$; for every subset $\{x, y, z\} \subseteq \{0,1\}^n \setminus \{0^n\}$ with $z \neq x + y$, the random variable $f \leftarrow \mathcal{F}_{\{x,y,z\}}$ is such that $(f(x), f(y), f(z))$ is uniform over $\{0,1\}^3$. For every set $S \subseteq \{0,1\}^n$ containing 0^n, $\mathcal{F}$ samples $f \leftarrow \mathcal{F}_{S\setminus\{0^n\}}$, and outputs the function g where $g(x) = f(x)$ for $x \in S \setminus \{0^n\}$ and $g(0^n) = 0$. Note that $\mathcal{F}$ is 3-non-signaling because for every $S \subseteq \{0,1\}^n \setminus \{0^n\}$ with $|S| = 3$ the restriction of $\mathcal{F}_S$ to any two coordinates $\{x, y\} \subseteq S$ induces a uniformly boolean random function over $f\colon \{x, y\} \to \{0, 1\}$. In particular, for distinct $x, y \in \{0,1\}^n \setminus \{0^n\}$ it holds that $\mathcal{F}_{\{0^n,x,y\}}$ outputs 0 on 0^n, and random bits on x and y.

Clearly, $\mathcal{F}$ passes the linearity test with probability 1. Observe that we can alternatively describe its answers according to the following procedure: upon receiving a subset $S \subseteq \{0,1\}^n$, $\mathcal{F}$ samples a uniformly random *linear* function $f\colon \{0,1\}^n \to \{0,1\}$ (independent of S) and returns the restriction of f to S. We can thus explain $\mathcal{F}$ via the uniform distribution over linear functions.

Generalizing from the above example, any non-signaling function that is induced by sampling a linear function from *any* distribution (not just the uniform one) and answering accordingly will pass the linearity test with probability 1. Note that a distribution over linear functions is given by non-negative real numbers $(p_\alpha)_{\alpha\in\{0,1\}^n}$ such that $\sum_{\alpha\in\{0,1\}^n} p_\alpha = 1$, where p_α is the probability of sampling the function $\langle\alpha, \cdot\rangle$. If $\mathcal{F}$ answers according to $(p_\alpha)_{\alpha\in\{0,1\}^n}$, then $\Pr[\mathcal{F}(x) = b] = \sum_{\alpha:\langle\alpha,x\rangle=b} p_\alpha$ for every $x \in \{0,1\}^n$ and $b \in \{0, 1\}$; a similar formula holds for more inputs.

The above discussion suggests a natural conjecture: every non-signaling function that passes the linearity test with probability 1 can be explained by some distribution over linear functions. In fact, this conjecture *is* true if the non-signaling strategy is restricted to be a quantum strategy [IV12; Vid14]. But the set of non-signaling strategies is strictly larger. Below we show that, perhaps surprisingly, these additional strategies make this conjecture false.

Example 2. Consider the following 3-non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n,|S|\leq 3}$. For every subset $\{x, y, x + y\} \subseteq \{0,1\}^n \setminus \{0^n\}$, $\mathcal{F}_{\{x,y,x+y\}}$ is the following distribution

$$\Pr_{f\leftarrow\mathcal{F}_{\{x,y,x+y\}}}[f(x, y, x + y) = (a_1, a_2, a_3)] = \begin{cases} 1/7 & \text{if } (a_1, a_2, a_3) = (0, 0, 0) \\ 2/7 & \text{if } (a_1, a_2, a_3) \in \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\} \end{cases};$$

for every subset $\{x, y, z\} \subseteq \{0,1\}^n \setminus \{0^n\}$ with $z \neq x + y$, $\mathcal{F}_{\{x,y,z\}}$ is the following distribution

$$\Pr_{f\leftarrow\mathcal{F}_{\{x,y,z\}}}[f(x, y, z) = (a_1, a_2, a_3)] = \begin{cases} 0 & \text{if } (a_1, a_2, a_3) = (0, 0, 0) \\ 1/7 & \text{if } (a_1, a_2, a_3) \neq (0, 0, 0) \end{cases}.$$

If an input set S contains 0^n, $\mathcal{F}_S$ assigns 0^n to 0 and answers the rest according to $\mathcal{F}_{S\setminus\{0^n\}}$. Note that $\mathcal{F}$ is 3-non-signaling because for distinct and non-zero x and y, the distribution of $\mathcal{F}_{\{x,y\}}$ is

$$\Pr_{f\leftarrow\mathcal{F}_{\{x,y\}}}[f(x, y) = (a_1, a_2)] = \begin{cases} 1/7 & \text{if } (a_1, a_2) = (0, 0) \\ 2/7 & \text{if } (a_1, a_2) \neq (0, 0) \end{cases}.$$

In particular, for distinct and non-zero x and y, the distribution of $\mathcal{F}_{\{x,y,0^n\}}$ is

$$\Pr_{f\leftarrow\mathcal{F}_{\{x,y,0^n\}}}[f(x, y, 0^n) = (a_1, a_2, 0)] = \begin{cases} 1/7 & \text{if } (a_1, a_2) = (0, 0) \\ 2/7 & \text{if } (a_1, a_2) \in \{(1, 0), (0, 1), (1, 1)\} \end{cases}.$$

Observe that $\mathcal{F}$ passes the linearity test with probability 1. However, unlike before, a distribution over linear functions that explains $\mathcal{F}$ *does not exist*. Namely, there is no probability vector $(p_\alpha)_{\alpha\in\{0,1\}^n}$ with non-negative entries and $\sum_{\alpha\in\{0,1\}^n} p_\alpha = 1$ such that $\Pr[\mathcal{F}(x) = b] = \sum_{\alpha:\langle\alpha,x\rangle=b} p_\alpha$ for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$. In fact, when trying to solve this linear system of equations with $(p_\alpha)_{\alpha\in\{0,1\}^n}$ as the variables, we obtain a solution vector in which some of the entries are *negative*.

The above example is problematic because it seems to suggest that a clean characterization of the set of all non-signaling functions passing the linearity test does not exist. Indeed, it shows that this set is strictly richer than the set of all distributions over linear functions.

1.4 Negative probabilities and quasi-distributions

In order to resolve the difficulty encountered in Example 2, we *embrace* negative probabilities (and probabilities greater than 1), and consider the notion of a *quasi-distribution* over boolean functions.

Definition 1.2 (informal)**.** *A* quasi-distribution *is a vector of real numbers $\mathcal{Q} = \{q_f\}_{f\colon \{0,1\}^n\to\{0,1\}}$ such that $\sum_{f\colon \{0,1\}^n\to\{0,1\}} q_f = 1$. Similarly, a* quasi-distribution over linear functions *is a quasi-distribution $\mathcal{Q} = \{q_f\}_{f\colon \{0,1\}^n\to\{0,1\}}$ such that $q_f = 0$ for all f that are not linear functions; in this case, we also allow ourselves to represent the quasi-distribution by a vector $(q_\alpha)_{\alpha\in\{0,1\}^n}$, where each q_α is associated with the linear function $\langle\alpha,\cdot\rangle$.*

A function f in a quasi-distribution $\mathcal{Q} = \{q_f\}_f$ is thus "sampled" with "probability" q_f, which means that for every subset $S \subseteq \{0,1\}^n$ and string $\vec{b} \in \{0,1\}^S$ the event "$\mathcal{Q}(S) = \vec{b}$" has *quasi-probability* given by $\widetilde{\Pr}[\,\mathcal{Q}(S) = \vec{b}\,] := \sum_{f \text{ s.t. } f(S)=\vec{b}} q_f$.

This may seem nonsensical, because quasi-probabilities are not restricted to be in $[0,1]$. But this shall soon make sense. In the words of Paul Dirac [Dir42, p.8]: "*Negative energies and probabilities should not be considered as nonsense. They are well-defined concepts mathematically, like a negative sum of money, since the equations which express the important properties of energies and probabilities can still be used when they are negative. Thus negative energies and probabilities should be considered simply as things which do not appear in experimental results.*"

This viewpoint, which plays a central role in our work, is borrowed from Physics, where it is used to describe physical phenomena [Dir42; Fey87], including non-signaling ones [AB11; AS13].

While the non-signaling function $\mathcal{F}$ in Example 2 cannot be explained by any distribution over linear functions, it *can* be explained by a *quasi*-distribution over linear functions. Concretely, letting q_α represent the probability of "sampling" the function $\langle\alpha,\cdot\rangle$, we solve the following system of linear equations in the variables $(q_\alpha)_{\alpha\in\{0,1\}^n}$:

$$\sum_{\alpha\in\{0,1\}^n} q_\alpha = 1 \quad \text{and} \quad \forall\, x \in \{0,1\}^n \;\; \forall\, b \in \{0,1\} \sum_{\alpha:\langle\alpha,x\rangle=b} q_\alpha = \Pr[\mathcal{F}(x) = b] \;\; .$$

The solution to this system is $q_{\vec{0}} = 1 - \frac{8}{7}\frac{2^n-1}{2^n} < 0$ and $q_\alpha = \frac{8}{7}\cdot\frac{1}{2^n}$ for all $\alpha \neq \vec{0}$. We stress that the solution has a negative entry. One can then verify that the quasi-distribution obtained above not only matches $\mathcal{F}$ on events involving one input (which is by construction) but also on events involving two inputs: $\Pr[\mathcal{F}(x_1) = b_1\,,\, \mathcal{F}(x_2) = b_2] = \sum_{\alpha:\langle\alpha,x_1\rangle=b_1\,,\,\langle\alpha,x_2\rangle=b_2} q_\alpha$ for all $x_1, x_2 \in \{0,1\}^n$ and $b_1, b_2 \in \{0,1\}$. Similarly, the same holds for events involving three inputs.

Crucially, the quasi-probabilities of events that involve a small enough set of inputs "magically" add up to *non-negative* probabilities because, in particular, they describe distributions of $\mathcal{F}$. In

other words, like in Dirac's observation above, the negative probabilities "do not appear in experimental results"; in our case the experiment is querying $\mathcal{F}$, and a quasi-distribution is merely a convenient mathematical abstraction to describe it.

The foregoing considerations directly lead to the following observation.

Observation 1.3. *If $\mathcal{Q} = (q_f)_{f\colon \{0,1\}^n \to \{0,1\}}$ is a quasi-distribution that induces a probability distribution on every event of at most k inputs, then $\mathcal{Q}$ induces a k-non-signaling function.*

Furthermore, if $\mathcal{Q}$ is supported on linear functions only, then the corresponding k-non-signaling function passes the linearity test with probability 1*.*

The first part of the observation suggests using k as a measure of a quasi-distribution's locality: we say that a quasi-distribution $\mathcal{Q} = (q_f)_f$ is *k-local* if for every k inputs $x_1, \ldots, x_k \in \{0,1\}^n$ and k outputs $b_1, \ldots, b_k \in \{0,1\}$ it holds that $\sum_{f: f(x_1)=b_1, \ldots, f(x_k)=b_k} q_f \geq 0$. Thus $\mathcal{Q}$ behaves like a collection of (standard) distributions on all events that involve at most k inputs and, moreover, these distributions jointly satisfy the k-non-signaling property.

The second part of the observation shows the existence of a class of non-signaling functions that pass the linearity test with probability 1 that is *much richer* than the class of distribution over linear functions. Are there any other types of non-signaling functions that pass the linearity test with probability 1, or are these all of them? Moreover, how does this answer change when we merely require that a non-signaling function pass the linearity test with probability at least $1 - \varepsilon$? We now discuss our results, which will provide answers to these questions.

2 Our results

Quasi-distributions arose rather naturally when reasoning about non-signaling functions. This is not a coincidence, because these two notions are equivalent.

Theorem 1 (informal)**.** *Local quasi-distributions and non-signaling functions are equivalent:*

1. *every k-local quasi-distribution induces a corresponding k-non-signaling function; conversely,*
2. *every k-non-signaling function has a k-local quasi-distribution that describes it. (In fact, this quasi-distribution is not unique: the set of all such quasi-distributions is an affine subspace.)*

See Section 8 (specifically, Theorem 8 and Theorem 9) for precise statements of the two items.

The first item is just Observation 1.3. The second item is proved via Fourier analytic techniques applied to a quasi-probability vector. Informally, the Fourier coefficients of quasi-probability vectors are indexed by subsets of $\{0,1\}^n$, and can be grouped into *levels* according to their size. We prove that the only coefficients that matter for the k-non-signaling function are those in the levels for sizes at most k, while all others change the weights in the quasi-probability vector but do not affect the induced k-non-signaling function.

The foregoing equivalence is a special case of a result of Abramsky and Brandenburger [AB11] that establishes an equivalence between *non-signaling empirical models* and quasi-distributions over *global sections*. Our result strengthens this equivalence by using novel Fourier analytic techniques to give an explicit characterization of the affine subspace of quasi-distributions that explain a non-signaling function. Moreover, these techniques play a crucial role in our study of linearity testing, and extend naturally to the case of non-signaling *players* (see Appendix F.2). We believe that the mathematical structure uncovered by our Fourier analytic techniques is of independent interest.

Having established the equivalence of local quasi-distributions and non-signaling functions, we return to the problem of linearity testing against non-signaling functions. Our first theorem in this direction is a characterization of the set of non-signaling functions that pass the linearity test with probability 1: this set consists of local quasi-distributions over linear functions (essentially).

Theorem 2 (informal)**.** *Let $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n, |S|\leq k}$ be a k-non-signaling function such that*

$$\Pr_{\substack{x,y\leftarrow\{0,1\}^n \\ f\leftarrow\mathcal{F}_{\{x,y,x+y\}}}}[f(x)+f(y)=f(x+y)] = 1 \ .$$

There is a unique $(k-1)$-local quasi-distribution $\mathcal{L}$ over linear functions describing $\mathcal{F}$ on all input sets of size $\leq k-1$ ($\mathcal{L}_S$ and $\mathcal{F}_S$ are equal as distributions for every set $S \subseteq \{0,1\}^n$ with $|S| \leq k-1$).

See Theorem 11 in Section 10 for the precise statement. (A minor technicality of the theorem is that $\mathcal{L}$ is only $(k-1)$-local and only matches $\mathcal{F}$ on at most $k-1$ inputs; the discussion after Theorem 11 explains why this is the best we can hope for.) To prove the theorem we define a quasi-distribution $\mathcal{L}$ over linear functions by solving a certain system of linear equations that ensures that $\mathcal{L}$ and $\mathcal{F}$ match on single inputs, i.e., that $\widetilde{\Pr}[\mathcal{L}(x) = b] = \Pr[\mathcal{F}(x) = b]$ for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$. We then need to establish that $\mathcal{L}$ and $\mathcal{F}$ match on all sets of at most $k-1$ inputs. We do so in two steps: we first use linearity to show that $\mathcal{L}$ and $\mathcal{F}$ match on all parity events (i.e., $\widetilde{\Pr}\left[\sum_{i\in T}\mathcal{L}(x_i) = b\right] = \Pr\left[\sum_{i\in T}\mathcal{F}(x_i) = b\right]$ for all $x_1,\ldots,x_s \in \{0,1\}^n$ and $b \in \{0,1\}$ with $s \leq k-1$); then we use Fourier analysis to extend this claim to all allowed input sets.

We finally return to our original question (Question 1.1). Suppose that a non-signaling function $\mathcal{F}$ passes the linearity test with probability $1-\varepsilon$ for sufficiently small $\varepsilon \geq 0$ (possibly with $\varepsilon > 0$ so Theorem 2 does not apply). What can we learn about $\mathcal{F}$? Recall that if $\mathcal{F}$ answers according to a fixed function $f\colon \{0,1\}^n \to \{0,1\}$ (as in standard linearity testing), then we may conclude that f is ε-close to some linear function [BLR93; BCHKS96]. The foregoing discussion for the case of $\varepsilon = 0$ leads to a natural conjecture: *non-signaling functions that pass the linearity test with high probability are local quasi-distributions over functions that are close to linear.* Our next theorem implies that this conjecture is true, but in a non-interesting way. That is, it holds even without the hypothesis: *every* k-non-signaling function can be expressed as a quasi-distribution over functions with support of size at most k (namely, over functions that are non-zero for at most k inputs).

Theorem 3 (informal)**.** *Every k-non-signaling function $\mathcal{F}$ can be expressed as a k-local quasi-distribution $\mathcal{Q}$ over functions with support of size at most k.*

The above theorem is quite counterintuitive. On one hand, if $\mathcal{F}$ is described by a distribution over functions that are close to linear, then $\mathcal{F}$ passes the linearity test with high probability. But this simple fact does *not* extend to the case where $\mathcal{F}$ is a *quasi*-distribution over functions that are close to linear. For example, the all-ones function never passes the linearity test, yet Theorem 3 implies that it can be expressed as a quasi-distribution over functions with support of size at most k, i.e., functions that are $\frac{k}{2^n}$-close to the all-zeros function (a linear function)!

We prove Theorem 3 via a greedy approach: given the non-signaling function $\mathcal{F}$, we iteratively consider small-support functions from heaviest to lightest and, in each iteration, assign to these functions certain quasi-probabilities computed from $\mathcal{F}$. See Theorem 10 (in Section 9) for details.

Since our last conjecture turned out to be false, we again look for inspiration in the standard setting in order to formulate another conjecture. Taking a different view, linearity testing tells

us that if a function $f\colon \{0,1\}^n \to \{0,1\}$ passes the linearity test with high probability then we know that there exists a linear function L such that for *every* $x \in \{0,1\}^n$ it holds that $L(x) = f(x+y) - f(y)$ with high probability over a random $y \in \{0,1\}^n$. Put another way, the answers to any given query (or, more generally, a set of queries) given by the self-correction of f and by L are close in statistical distance.

The foregoing observation suggests a conjecture: *if a non-signaling function passes the linearity test with high probability, then its self-correction is close to a quasi-distribution over linear functions.*

The self-correction $\hat{\mathcal{F}}$ of a non-signaling function $\mathcal{F}$ is naturally defined: on input $x \in \{0,1\}^n$, $\hat{\mathcal{F}}$ samples a random $y \in \{0,1\}^n$ and outputs $\mathcal{F}(x+y) - \mathcal{F}(y)$; a similar procedure applies if $\hat{\mathcal{F}}$ receives multiple inputs. Note that if $\mathcal{F}$ is k-non-signaling then $\hat{\mathcal{F}}$ is $\hat{k}$-non-signaling with $\hat{k} := \lfloor k/2 \rfloor$.

The notion of distance is also naturally defined: the distance between two non-signaling functions is the maximum statistical distance between the distributions induced on every subset S; the equivalence of non-signaling functions and quasi-distributions (Theorem 1) extends this definition to apply between two quasi-distributions, or between a non-signaling function and a quasi-distribution.

The following theorem shows that the conjecture above is in fact true.

Theorem 4 (informal)**.** *Let $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq \{0,1\}^n, |S| \le k}$ be a k-non-signaling function such that*

$$\Pr_{\substack{x,y \leftarrow \{0,1\}^n \\ f \leftarrow \mathcal{F}_{\{x,y,x+y\}}}} [f(x) + f(y) = f(x+y)] \ge 1 - \varepsilon \quad \text{for some } \varepsilon \ge 0 \ .$$

There is a $(\hat{k}-1)$-local quasi-distribution $\mathcal{L}$ over linear functions that is $O_{\hat{k}}(\varepsilon)$-close to $\hat{\mathcal{F}}$ on all input sets of size $\le \hat{k}-1$. That is, the maximum statistical distance between $\mathcal{L}_S$ and $\hat{\mathcal{F}}_S$, across all sets $S \subseteq \{0,1\}^n$ with $|S| \le \hat{k}-1$, is $O_{\hat{k}}(\varepsilon)$.

See Theorem 12 (in Section 11) for details. Our proof differs significantly from prior proofs of linearity testing in the standard setting. Informally, we start the proof by noting that $\hat{\mathcal{F}}$ satisfies $\Pr_{\hat{f} \leftarrow \hat{\mathcal{F}}_{\{x,y,x+y\}}} \Pr[\hat{f}(x) + \hat{f}(y) = \hat{f}(x+y)] \ge 1 - \hat{\varepsilon}$ for *every* $x, y \in \{0,1\}^n$ and $\hat{\varepsilon} := 4\varepsilon$. (By assumption, $\mathcal{F}$ merely satisfies such a statement for *random* $x, y \in \{0,1\}^n$.) The next step is similar to a step in the proof of Theorem 2: we define a quasi-distribution $\mathcal{L}$ over linear functions by solving a system of linear equations that ensures that $\mathcal{L}$ and $\hat{\mathcal{F}}$ match on single inputs, i.e., that $\Pr[\mathcal{L}(x) = b] = \Pr[\mathcal{F}(x) = b]$ for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$. We are left to argue that $\mathcal{L}$ and $\hat{\mathcal{F}}$ *almost* match on all sets of at most $\hat{k}-1$ inputs, i.e., that the distributions $\mathcal{L}_S$ and $\hat{\mathcal{F}}_S$ are statistically close for $|S| < \hat{k}$. As before, we do so in two steps: we first use linearity to show that $\mathcal{L}$ and $\hat{\mathcal{F}}$ *almost* match on all parity events (i.e., $\Pr[\sum_{i \in T} \hat{\mathcal{F}}(x_i) = b] \approx \widetilde{\Pr}[\sum_{i \in T} \mathcal{L}(x_i) = b]$ for all $x_1, \ldots, x_s \in \{0,1\}$ for $s \le \hat{k}-1$), and then we use a quantitative Fourier analytic claim (Lemma 5.1) to extend this claim to the remaining query sets.

Finally, we use the foregoing results about non-signaling *functions* to prove analogous statements about non-signaling *players*.

Recall that a *k-non-signaling player* $\mathcal{P}$ extends the notion of k non-communicating players (possibly sharing randomness) as follows: it is a collection $(\mathcal{P}_{(x_1,\ldots,x_k)})_{(x_1,\ldots,x_k) \in \{0,1\}^{k \cdot n}}$ where each $\mathcal{P}_{(x_1,\ldots,x_k)}$ is a *distribution* over functions $f\colon [k] \to \{0,1\}$ (the players' k answers to the k inputs) and, for every two input vectors $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ that agree on a subset $I \subseteq [k]$ of entries, the restrictions of $\mathcal{P}_{(x_1,\ldots,x_k)}$ and $\mathcal{P}_{(y_1,\ldots,y_k)}$ to entries in I are equal as distributions. Non-signaling players are a richer class than non-communicating players (and quantum-entangled ones) [PR94].

Now the linearity test, given a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{(x_1,\ldots,x_k)\in\{0,1\}^{k\cdot n}}$, samples random vectors $x, y \in \{0,1\}^n$ and distinct players $i_1, i_2, i_3 \in [k]$, sends the three queries $x, y, x+y$ to the players $\mathcal{P}_{i_1}, \mathcal{P}_{i_2}, \mathcal{P}_{i_3}$, and checks that $\mathcal{P}_{i_1}(x) + \mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)$.

Theorem 5 (informal)**.** *Let $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{(x_1,\ldots,x_k)\in\{0,1\}^{k\cdot n}}$ be a k-non-signaling player.*

1. *Suppose that*
$$\Pr_{\substack{x,y\leftarrow\{0,1\}^n\\ i_1,i_2,i_3\leftarrow[k]\\ \mathcal{P}}}[\mathcal{P}_{i_1}(x) + \mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)] = 1 \ .$$
There exists a $(k-2)$-local quasi-distribution $\mathcal{L}$ over linear functions that describes $\mathcal{P}$.

2. *Suppose that*
$$\Pr_{\substack{x,y\leftarrow\{0,1\}^n\\ i_1,i_2,i_3\leftarrow[k]\\ \mathcal{P}}}[\mathcal{P}_{i_1}(x) + \mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)] \geq 1-\varepsilon \ .$$
There exists a $(\hat{k}-1)$-local quasi-distribution $\mathcal{L}$ over linear functions that is $O_{\hat{k}}(\varepsilon)$-close to $\hat{\mathcal{P}}$, where $\hat{\mathcal{P}}$ is the (appropriately defined) self-correction of $\mathcal{P}$.

See Theorems 13 and 14 for details. The proof of these theorems show how to reduce to the case of non-signaling functions, which we have already established (in Theorems 2 and 4 respectively).

We conclude this section via a brief comparison to the case of quantum strategies. Ito and Vidick [IV12; Vid14] show that any quantum strategy that passes the linearity test with high probability is close to a *distribution* over linear functions. Our results instead show that, in our setting, we can only hope for a conclusion involving a *quasi-distribution* over linear functions. This qualitative difference is due to the fact that non-signaling strategies are a richer class than quantum strategies.

3 Techniques

We highlight some of the techniques that we use by providing proof sketches of some of our results. We first discuss the ideas behind the equivalence between non-signaling functions and local quasi-distributions (Section 3.1) and then how we analyze the linearity test (Section 3.2). After that, we explain how we derive corresponding results about non-signaling players (Section 3.3).

3.1 Non-signaling functions and local quasi-distributions are equivalent

Our Theorem 1 states that non-signaling functions and local quasi-distributions are equivalent. One direction of this equivalence, namely that every k-local quasi-distribution induces a corresponding k-non-signaling function, is a simple observation. Below we focus on the other, more interesting direction, which is: given a k-non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq\{0,1\}^n, |S|\leq k}$, how do we construct a quasi-distribution $\mathcal{Q} = \{q_f\}_{f\colon \{0,1\}^n\to\{0,1\}}$ that matches $\mathcal{F}$ on all sets of at most k queries?

We construct $\mathcal{Q}$ by specifying its *Fourier coefficients*. We view $\mathcal{Q} = (q_f)_{f\colon \{0,1\}^n\to\{0,1\}}$ as a function $q\colon \{0,1\}^{\{0,1\}^n} \to \mathbb{R}$ by setting $q(f) := q_f \in \mathbb{R}$, and then write $\mathcal{Q}$ via its Fourier expansion:

$$q(\cdot) = \sum_{T\subseteq\{0,1\}^n} \widehat{q}(T)\chi_T(\cdot) \quad \text{where} \quad \begin{cases} \chi_T(f) := (-1)^{\sum_{x\in T} f(x)} \\ \widehat{q}(T) := \langle q, \chi_T\rangle = \frac{1}{2^{2^n}} \sum_{f\colon D\to\{0,1\}} q(f)\chi_T(f) \end{cases} .$$

We set the 2^{2^n} Fourier coefficients as follows:

$$\widehat{q}(T) := \begin{cases} \frac{1}{2^{2^n}} & \text{if } T = \emptyset \\ \frac{2}{2^{2^n}} \left(\Pr[\sum_{x \in T} \mathcal{F}(x) = 0] - \frac{1}{2} \right) & \text{if } 1 \leq |T| \leq k \\ 0 & \text{if } |T| > k \end{cases} .$$

We have to argue that the above choice of $\mathcal{Q}$ does describe $\mathcal{F}$. First, we show that $\mathcal{F}$ and $\mathcal{Q}$ match on all *parity events* of size at most k, i.e., for all $S \subseteq \{0,1\}^n$ with $|S| \leq k$

$$\Pr\left[\sum_{x \in S} \mathcal{F}(x) = 1\right] = \sum_{f : \sum_{x \in S} f(x) = 1} q_f = \widetilde{\Pr}\left[\sum_{x \in S} \mathcal{Q}(x) = 1\right] .$$

Recall (see Section 1.4) that $\widetilde{\Pr}[\cdot]$ denotes the quasi-probability for an event about a quasi-distribution.

Second, we prove that $\Pr[\mathcal{F}(S) \in E] = \widetilde{\Pr}[\mathcal{Q}(S) \in E]$ for every subset $S \subseteq \{0,1\}^n$ and event $E \subseteq \{0,1\}^S$. We build on the previous step by observing that any event can be expressed as a linear combination of parity events: there exist real numbers $\{c_T\}_T$ depending on E such that

$$\Pr[\mathcal{Q}(S) \in E] = \sum_{T \subseteq S} c_T \cdot \widetilde{\Pr}\left[\sum_{x \in T} \mathcal{Q}(x) = 0\right] . \tag{1}$$

In fact, the real numbers $\{c_T\}_T$ are closely related to the Fourier coefficients of the indicator function of E, and this relation is a consequence of the fact that the functions $\{\chi_T(\cdot)\}_T$ depend only on the parities of their inputs. See Lemma 5.1 for details.

The above is merely one quasi-distribution that explains $\mathcal{F}$. We can find other such quasi-distributions by noting that changing $\widehat{q}(T)$ for $|T| > k$ yields quasi-distributions that still match $\mathcal{F}$. Essentially, if $|T| > k$ then $\chi_T(\cdot)$ does not affect the induced distributions on sets of at most k inputs. We then argue that these are the only solutions possible. See Section 8 for details.

3.2 Testing linearity against non-signaling functions

We discuss the ideas behind our analysis of linearity test against non-signaling functions (that is, behind Theorem 2 and Theorem 4). We first explain why known proofs in the standard setting do not easily extend to our setting, and then we describe the approach that we took.

3.2.1 Difficulties of prior approaches

We begin with a helpful exercise for which difficulties do *not* arise: consider the task of analyzing the linearity test against a *distribution* $\mathcal{D}$ over boolean functions. Namely, if $\Pr[f(x) + f(y) = f(x+y)] \geq 1 - \varepsilon$ for $f \leftarrow \mathcal{D}$ and $x, y \leftarrow \{0,1\}^n$ then what can we conclude about $\mathcal{D}$? This case is not hard to analyze: we separately apply known results on linearity testing to each function in the support of $\mathcal{D}$, and conclude that most of $\mathcal{D}$ is concentrated on nearly-linear functions. Indeed, by Markov's inequality, with probability $1 - \sqrt{\varepsilon}$ over a choice of $f \leftarrow \mathcal{D}$ it holds that $\Pr_{x,y}[f(x) + f(y) = f(x+y)] \geq 1 - \sqrt{\varepsilon}$ and thus that f is $\sqrt{\varepsilon}$-close to a linear function. This conclusion explains why $\mathcal{D}$ passes the linearity test with high probability.

However, when considering the linearity test against a non-signaling function, the situation changes significantly, as we now explain.

The Fourier analytic approach. One of the classical proofs of linearity testing in the standard setting follows a Fourier analytic approach [BCHKS96]. Unfortunately, we do not see how to use this approach directly on a non-signaling function $\mathcal{F}$, because computing Fourier coefficients requires access to an entire function while $\mathcal{F}$ only provides local views. We could instead rely on the equivalence between non-signaling functions and local quasi-distributions, and apply Fourier analysis to the functions in a quasi-distribution $\mathcal{Q} = (q_f)_{f\colon \{0,1\}^n \to \{0,1\}}$ that describes $\mathcal{F}$. Namely, we could rewrite the probability $\Pr[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)]$ as $\sum_f q_f \Pr[f(x) + f(y) = f(x+y)]$, and then reason about the Fourier coefficients of every f. We do not see how to make this work either, because the coefficients $\{q_f\}_f$ can be positive or negative (and even unbounded), which in particular forbids Markov-type arguments. It is also not clear what kind of conclusion we could expect about the Fourier coefficients about *all* functions.

The combinatorial approach. Another classical proof of linearity testing in the standard setting follows a combinatorial approach (e.g., [BLR93; BCLR08]): given the function $f\colon \{0,1\}^n \to \{0,1\}$, define its correction $g\colon \{0,1\}^n \to \{0,1\}$ to be $g(x) := \mathrm{maj}_{y \in \{0,1\}^n} f(x+y) - f(y)$, and show that it is close to f; then show that g is linear as, for every $x \in \{0,1\}^n$, a vast majority of y's yield $g(x)$. This approach also seems to fail in our setting: the foregoing correcting procedure relies on taking majority over *all* $y \in \{0,1\}^n$, but a non-signaling function only accepts up to k inputs at a time.

It is not surprising that prior approaches do not seem to apply to our setting: they were developed to show that a function f passing the linearity test with high probability is nearly-linear. But we already know that every non-signaling function can be described by a quasi-distribution over nearly-linear functions, so we are not interested in conclusions about nearly-linear functions. Instead, we aim to show that (the self-correction of) a non-signaling function passing the linearity test with high probability is close to a quasi-distribution over *linear* functions. We next discuss our approach to establish such a conclusion.

3.2.2 Our approach

Let us once more first focus on the case where a k-non-signaling function $\mathcal{F}$ passes the linearity test with probability 1, namely, $\Pr[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] = 1$ for every $x, y \in \{0,1\}^n$. Our first step is to show that there exists a quasi-distribution $\mathcal{L}$ over linear functions that matches $\mathcal{F}$ on single inputs, namely, $\widetilde{\Pr}[\mathcal{L}(x) = b] = \Pr[\mathcal{F}(x) = b]$ for every $x \in \{0,1\}^n$ and $b \in \{0,1\}$. Viewing $\mathcal{L}$ as a vector $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$ where each α is associated with the linear function $\langle \alpha, \cdot \rangle$, we know that $\mathcal{L}$ must be a solution to the following system of linear equations:

$$\forall\, x \in \{0,1\}^n\,, \qquad \sum_{\alpha : \langle \alpha, x \rangle = 0} \ell_\alpha = \Pr[\mathcal{F}(x) = 0] \ .$$

Note that it suffices to consider constraints only involving $\Pr[\mathcal{F}(x) = 0]$ because $\Pr[\mathcal{F}(x) = 1] = 1 - \Pr[\mathcal{F}(x) = 0]$. Also, $\mathcal{L}$ is a quasi-distribution because $\sum_\alpha \ell_\alpha = \Pr[\mathcal{F}(0^n) = 0] = \Pr_{x \leftarrow \{0,1\}^n}[\mathcal{F}(0^n) + \mathcal{F}(x) = \mathcal{F}(x)] = 1$ (as $\mathcal{F}$ always passes the linearity test). This system has a unique solution, which thus defines the quasi-distribution $\mathcal{L}$. We remark that it is no coincidence that quasi-distributions supported on LIN are uniquely defined by their probabilities on sets of size 1: in Appendix A we prove that a quasi-distribution is supported on LIN if and only if all of its Fourier coefficients are determined by the coefficients only for sets of size 1.

Next, we need to argue that $\mathcal{L}$ and $\mathcal{F}$ match on larger sets of inputs. We first argue that they match on all parity events, similarly to the idea behind the equivalence between non-signaling func-

tions and quasi-distributions discussed above (in Section 3.1). Specifically, we use the assumption on linearity to show that for every subset $S \subseteq \{0,1\}^n$ with $|S| < k$ it holds that

$$\widetilde{\Pr}\left[\sum_{x \in S} \mathcal{L}(x) = 0\right] = \Pr\left[\sum_{x \in S} \mathcal{F}(x) = 0\right] \ .$$

After that, using Eq. (1), we conclude that $\mathcal{L}$ and $\mathcal{F}$ match on all sets S of less than k inputs: we express each event $E \subseteq \{0,1\}^S$ as a linear combination of parity events for both $\mathcal{F}$ and $\mathcal{L}$,

$$\Pr\left[\mathcal{F}(S) \in E\right] = \sum_{T \subseteq S} c_T \cdot \Pr\left[\sum_{x \in T} \mathcal{F}(x) = 0\right] \ ,$$

and similarly

$$\widetilde{\Pr}\left[\mathcal{L}(S) \in E\right] = \sum_{T \subseteq S} c_T \cdot \widetilde{\Pr}\left[\sum_{x \in T} \mathcal{L}(x) = 0\right] \ .$$

The above shows that matching on parity events implies matching on all sets of less than k inputs.

Let us now relax the assumption that $\mathcal{F}$ passes the linearity test with probability 1 to merely that it passes the test with high probability, say at least $1 - \varepsilon$ for $\varepsilon > 0$. We first consider $\hat{\mathcal{F}}$, which is the $\hat{k}$-non-signaling self-correction of $\mathcal{F}$ (with $\hat{k} := k/2$), and observe that there exists $\hat{\varepsilon} = 4\varepsilon$ such that $\hat{\mathcal{F}}$ satisfies, for *every* $x, y \in \{0,1\}^n$,

$$\Pr_{\hat{f} \leftarrow \hat{\mathcal{F}}_{\{x,y,x+y\}}} [\hat{f}(x) + \hat{f}(y) = \hat{f}(x+y)] \geq 1 - \hat{\varepsilon} \ .$$

Note that, by assumption, $\mathcal{F}$ merely satisfies such a statement for *random* $x, y \in \{0,1\}^n$.

The next step is similar to the "$\varepsilon = 0$" case discussed above: we define a quasi-distribution $\mathcal{L}$ over linear functions by solving the system of linear equations that ensures that $\mathcal{L}$ and $\hat{\mathcal{F}}$ match on all single inputs, i.e., that $\widetilde{\Pr}[\mathcal{L}(x) = b] = \Pr[\hat{\mathcal{F}}(x) = b]$ for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$.

We then argue that $\mathcal{L}$ and $\hat{\mathcal{F}}$ *almost* match on sets of less than $\hat{k}$ inputs, i.e., that the distributions $\mathcal{L}_S$ and $\hat{\mathcal{F}}_S$ are statistically close for every $S \subseteq \{0,1\}^n$ with $|S| < \hat{k}$. We do so, again, in two steps. First, we use the almost linearity of $\hat{\mathcal{F}}$ to show that $\mathcal{L}$ and $\hat{\mathcal{F}}$ *almost* match on all parity events. Specifically, we show that for every subset $T \subseteq \{0,1\}^n$ with $|T| < \hat{k}$ and $b \in \{0,1\}$,

$$\left| \Pr\left[\sum_{x \in T} \hat{\mathcal{F}}(x) = b\right] - \widetilde{\Pr}\left[\sum_{x \in T} \mathcal{L}(x) = b\right] \right| < (|T| - 1)\hat{\varepsilon} \ .$$

Then, we use Eq. (1) to extend this claim to all events on these query sets: for every subset $S \subseteq \{0,1\}^n$ with $|S| < \hat{k}$ and event $E \subseteq \{0,1\}^S$

$$\left| \Pr[\hat{\mathcal{F}}(S) \in E] - \widetilde{\Pr}[\mathcal{L}(S) \in E] \right| < \sum_{T \subseteq S} |c_T| \cdot (|T| - 1) \cdot \hat{\varepsilon} \ .$$

Crucially, unlike the case of $\varepsilon = 0$, here we need *quantitative* bounds on the coefficients $\{c_T\}_T$ in order to derive an upper bound. We prove such bounds in Lemma 5.1.

Finally, while $\mathcal{L}$ is close to $\hat{\mathcal{F}}$ (see Definition 7.5 for how to extend the notion of statistical distance to our setting), it is possible that $\mathcal{L}$ does not induce a distribution on all subsets $S \subseteq \{0,1\}^n$

with $|S| < \hat{k}$, because it could be that $\widetilde{\Pr}[\mathcal{L}(S) \in E]$ is negative for some S and $E \subseteq \{0,1\}^S$. However, since $\Pr[\hat{\mathcal{F}}(S) \in E]$ is a probability (i.e., a number between 0 and 1), for all subsets $S \subseteq \{0,1\}^n$ with $|S| < \hat{k}$ it holds that $\widetilde{\Pr}[\mathcal{L}(S) \in E] \in [-\varepsilon', 1+\varepsilon']$ for $\varepsilon' := (|S|-1) \cdot \sqrt{|E|} \cdot \hat{\varepsilon}$. We then show that $\mathcal{L}$ can be corrected to obtain a $(\hat{k}-1)$-local quasi-distribution $\mathcal{L}'$ that is close to $\mathcal{L}$ (see Corollary 7.9). By triangle inequality this implies that $\mathcal{L}'$ is also close to $\hat{\mathcal{F}}$.

See Section 11 for details.

3.3 Extending the analysis to non-signaling players

We make a "black-box" use of our results on testing linearity against non-signaling *functions* to derive corresponding results on testing linearity against non-signaling *players* (defined in Appendix D). Recall that, given a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{(x_1,\ldots,x_k)\in\{0,1\}^{k\cdot n}}$, the linearity test is now as follows: sample $x, y \in \{0,1\}^n$ and (distinct) $i_1, i_2, i_3 \in [k]$ uniformly at random, send the three queries $x, y, x+y$ to the players $\mathcal{P}_{i_1}, \mathcal{P}_{i_2}, \mathcal{P}_{i_3}$ respectively, and check that $\mathcal{P}_{i_1}(x)+\mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)$.

We prove that if $\mathcal{P}$ *always* passes the linearity test, then there exists a quasi-distribution $\mathcal{L}$ over linear functions that matches $\mathcal{P}$.

We first argue that $\mathcal{P}$ must be (almost) *symmetric*, that is, $\mathcal{P}$'s answers depend only on the set of asked queries but not also on which players answer these queries. In more detail, we show that, for every subset $I \subseteq [k]$ of $|I| = k-1$ players, it holds that $\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{P}(\pi(\vec{x})) = \pi(\vec{b})]$ for every permutation $\pi\colon I \to I$, inputs $\vec{x} = (x_i)_{i\in I} \in (\{0,1\}^n)^I$, and answers $\vec{b} = (b_i)_{i\in I} \in \{0,1\}^I$.

We then define a $(k-1)$-non-signaling function $\mathcal{F}$ that matches $k-1$ players of $\mathcal{P}$ in the natural way (we define $\Pr[\mathcal{F}(x_1) = b_1, \ldots, \mathcal{F}(x_{k-1}) = b_{k-1}] := \Pr[\mathcal{P}_1(x_1) = b_1, \ldots, \mathcal{P}_{k-1}(x_{k-1}) = b_k]$). By the aforementioned symmetry of $\mathcal{P}$, it does not matter which $k-1$ players we use to define $\mathcal{F}$.

We then argue that $\mathcal{F}$ always passes the linearity test. Our earlier results imply that there exists a quasi-distribution $\mathcal{L}$ over linear functions that matches $\mathcal{F}$ on all subsets of at most $k-2$ queries. By definition of $\mathcal{F}$ this implies that $\mathcal{L}$ *also* matches the players $\mathcal{P}_1, \ldots, \mathcal{P}_{k-2}$, and, using the symmetry of $\mathcal{P}$, we conclude that $\mathcal{L}$ also matches *every* subset of $k-2$ players.

We now relax the assumption that $\mathcal{P}$ passes the linearity test with probability 1 to merely that it passes the test with probability $1-\varepsilon$ for a small enough $\varepsilon > 0$.

Similarly to the case of non-signaling functions, we define a self-correction $\hat{\mathcal{P}}$ of $\mathcal{P}$ in the natural way: it is a $\hat{k}$-non-signaling player (for $\hat{k} := k/2$) that, given a query $(x_1, \ldots, x_{\hat{k}}) \in \{0,1\}^{\hat{k}\times n}$, samples $w_1, \ldots, w_{\hat{k}} \in \{0,1\}^n$ and a permutation $\pi\colon [k] \to [k]$ uniformly at random, and answers each x_i with $\mathcal{P}_{\pi(2i)}(x_i + w_i) + \mathcal{P}_{\pi(2i+1)}(w_i)$.

We show that $\hat{\mathcal{P}}$ is (fully) symmetric and that, for every $x, y \in \{0,1\}^n$ and distinct $i_1, i_2, i_3 \in [\hat{k}]$, $\Pr[\hat{\mathcal{P}}_{i_1}(x) + \hat{\mathcal{P}}_{i_2}(y) = \hat{\mathcal{P}}_{i_3}(x+y)] > 1-\hat{\varepsilon}$ for $\hat{\varepsilon} := 4\varepsilon$. This is analogous to the average-case-to-worst-case statement that we showed for non-signaling functions. We define a $\hat{k}$-non-signaling function $\hat{\mathcal{F}}$ that matches $\hat{\mathcal{P}}$ similarly to the above (by letting $\Pr[\hat{\mathcal{F}}(x_1) = b_1, \ldots, \hat{\mathcal{F}}(x_{\hat{k}}) = b_{\hat{k}}] := \Pr[\hat{\mathcal{P}}_1(x_1) = b_1, \ldots, \hat{\mathcal{P}}_{\hat{k}}(x_{\hat{k}}) = b_{\hat{k}}]$), and show that it satisfies the analogous worst-case property, that is, $\Pr[\hat{\mathcal{F}}(x) + \hat{\mathcal{F}}(y) = \hat{\mathcal{F}}(x+y)] \geq 1-\hat{\varepsilon}$ for every $x, y \in \{0,1\}^n$. Our earlier results imply that there exists a quasi-distribution $\mathcal{L}$ over linear functions that is close to $\hat{\mathcal{F}}$, and thus also close to $\hat{\mathcal{P}}$.

See Appendix E for details.

4 Discussion and open problems

The study of non-signaling strategies in Physics is motivated by the goal of understanding the power and limitations of Nature's apparent non-locality [KT85; Ras85; PR94; PR98; Bar07]. Prior work has explored many topics, including the inter-convertibility between quantum strategies and non-signaling strategies [CGMP05; BP05; BLMPPR05; JM05; BM06]; communication complexity with non-signaling strategies [van13; BBLMTU06]; non-local computation [LPSW07]; using non-signaling strategies to achieve key distribution, oblivious transfer, and bit commitments [BHK05; WW05; BCUWW06; SPG06; SGP06]; and many others [MAG06; Hol09; CR17].

More recently, researchers have established connections with Complexity Theory and Cryptography. Property Testing against non-signaling strategies, the subject of our work, is likely to lead to a deeper understanding of these.

4.1 Powers and limitations of non-local strategies

Understanding the computational complexity of computing or approximating the value of certain classes of games is a fundamental problem in Complexity Theory. Games are typically phrased in terms of one or more *non-communicating* players that interact with a probabilistic polynomial-time Referee (with polynomial randomness), who decides at the end of the game if the players win or not. The complexity of these games is well-understood.

- Results on *Interactive Proofs* (IPs) [LFKN92; Sha92] imply that approximating the value of single-player games is PSPACE-complete, when given enough rounds.
- Results on *Multi-prover Interactive Proofs* (MIPs) [BFL91] imply that approximating the value of multi-player games is NEXP-complete, even with only two players.
- Results on *Probabilistically Checkable Proofs* (PCPs) [BFLS91; FGLSS96; AS98; ALMSS98] imply that, if the player's strategy is non-adaptive (the player merely answers queries from the Referee) then approximating the game's value is NEXP-complete, even if the Referee asks only a constant number of queries and receives answers over a constant-size alphabet.

However, if the players can use any non-signaling strategy to win the game, *much less is known.*

If there are only *two* players, then approximating the game's value is PSPACE-complete [IKM09; Ito10]. If the game has k players then its value can be computed in time $\mathsf{poly}(2^{kr}, |\Sigma|^k)$, where r is the Referee's randomness complexity and Σ is each player's answer's alphabet [DLNNR04], which means that this computation lies in EXP. This is *very unlike* the case of non-communicating players.

However, hardness results for this problem in the case of three or more players have been elusive. Recently, Kalai, Raz, and Rothblum [KRR13; KRR14] established EXP-hardness for the case of polynomially-many provers, via a reduction from deterministic-time languages.

Theorem 6 ([KRR13; KRR14])**.** *Let L be a language decidable in time $T\colon \mathbb{N} \to \mathbb{N}$. There exists a constant $c > 0$ such that, for any function $\lambda\colon \mathbb{N} \to \mathbb{N}$ with $\lambda \geq \log^c T$, L has a $(\lambda \log^c T)$-prover MIP with soundness error $2^{-\lambda}$ against non-signaling players. The verifier runs in time $n\lambda^2 \log^c T$ and the provers in time $\mathsf{poly}(T, \lambda)$; each query and answer consists of $\lambda \log^c T$ bits.*

The above theorem is proved by constructing a PCP verifier that is secure against non-signaling functions (Definition 6.1), which can then be compiled into an MIP verifier that is secure against

non-signaling players (Definition D.1). The proof is a technical tour-de-force showing that a modification of the "classical" PCP verifier in [BFL91; BFLS91] is secure against non-signaling functions.

The huge gap between the EXP-completeness for polynomially-many provers and the PSPACE-completeness for two provers motivates a natural question:

> *Is there a non-signaling analogue of the PCP Theorem?* I.e., does EXP have $O(1)$-query PCPs over a $O(1)$-size alphabet that are secure against non-signaling functions? (Equivalently, $O(1)$-prover MIPs over a $O(1)$-size alphabet that are secure against non-signaling players?)

We believe that initiating a study of Property Testing against non-signaling strategies will drive progress on this question. In particular, linearity testing is one of the ingredients of the (classical) PCP Theorem, and linearity testing against non-signaling strategies may be a good place to start.

We also believe that Property Testing against non-signaling strategies may play a significant *simplifying role*, which could itself drive progress on this and other questions. Indeed, the analysis of classical PCP constructions (including [BFL91; BFLS91]) is carried out in two conceptually simple steps: first argue soundness assuming that the PCP is a low-degree function, and then rely on low-degree testing and self-correction to ensure that the PCP is close to a low-degree function [RS96; RS97; AS03]. The study of this latter step as a standalone problem in the area of Property Testing has enabled much progress on PCP research. In contrast, while the analysis in [KRR13; KRR14] does analyze low-degree tests by proving certain average-case-to-worst-case statements, it *does not prove any local-to-global phenomena* for the property of "low-degreeness".

We prove a first local-to-global phenomenon for Property Testing against non-signaling strategies. However, whether Property Testing is feasible beyond the case of linearity testing (our focus) and whether it plays a beneficial and simplifying role in PCP research are fascinating open problems.

4.2 Hardness of approximation

Feige et al. [FGLSS96] showed a fundamental connection between MIPs/PCPs and the hardness of approximating values of constraint satisfaction problems. Kalai, Raz, and Regev [KRR16] recently established a similar connection, this time between *non-signaling* MIPs/PCPs and the hardness of approximating values of *linear programs*. While the first connection considers approximation algorithms that are bounded in time, the second connection considers approximation algorithms that are bounded in *space*. We recall [KRR16]'s result and its relation to our results.

Theorem 7 ([KRR16])**.** *Let L be a language with a 1-round k-prover MIP with soundness error ϵ against non-signaling players in which: (i) the verifier has time complexity T, space complexity S, and randomness complexity r; (ii) the prover's answers are symbols in Σ.*

Then there exists a family of polyhedra $\{H_n\}_{n\in\mathbb{N}}$ and a $\mathsf{poly}(2^{kr}, |\Sigma|^k, T)$-time $\mathsf{poly}(k, r, S)$-space reduction $\mathscr{R}$ such that: (i) For every instance $x \in \{0,1\}^*$, $\mathscr{R}(x)$ is a linear program with polyhedron $H_{|x|}$ and with $\mathsf{poly}(2^{kr}, |\Sigma|^k)$ variables and constraints. (ii) If $x \in L$, then the value of the linear program $\mathscr{R}(x)$ is 1. (iii) If $x \notin L$, then the value of the linear program $\mathscr{R}(x)$ at most ϵ.

The above result, when combined with the non-signaling MIPs for deterministic-time languages of [KRR13; KRR14] (see Section 4.1), implies that a $2^{\log^{o(1)}(n)}$-space approximation algorithm for linear programming is unlikely, even when given unbounded computation based on the polyhedron. (Since that would imply, in particular, that every problem in P can be solved in $2^{\log^{o(1)}(n)}$-space.)

The above conclusion, however, appears sub-optimal because both 2^{kr} and $|\Sigma|^k$ are super-polynomial in the construction of [KRR13; KRR14]. Ideally, we would like a construction where

$r = O(\log n)$ and $k = O(1)$, which again (as discussed in Section 4.1) leads to the question of whether there is a non-signaling analogue of the PCP Theorem. We conjecture that the study of Property Testing against non-signaling strategies is again very relevant.

4.3 One-round delegation of computation

Delegation of computation is a fundamental goal in Cryptography that involves designing protocols that enable a weak verifier to outsource expensive computations to a powerful but untrusted prover.

A key efficiency measure is round complexity (the number of back-and-forth messages between the verifier and prover). Aiello et al. [ABOR00] suggested a cryptographic method to transform any 1-round MIP into a 1-round delegation protocol, but did not provide a proof of security. Later on, Dwork et al. [DLNNR04] showed that this method is not secure in the general case, by exhibiting a 1-round MIP for which the transformation yields a delegation protocol that can be fooled.

Nevertheless, Kalai, Raz, and Rothblum [KRR13] proved that if the 1-round MIP used in the method is sound against non-signaling players then the resulting delegation protocol *cannot* be fooled (namely, is secure). More precisely, the 1-round MIP must be sound not only against all players that are non-signaling but also against all players that are *almost* non-signaling (see Appendix C), where "almost" denotes a certain parameter that depends on the security reduction.

By invoking this method on the MIP of [KRR13; KRR14] (which *is* secure against almost non-signaling players), one obtains a delegation protocol for all polynomial-time functions in which the prover runs in polynomial time and the verifier in polylogarithmic time.

Yet, the seemingly sub-optimal parameters of the MIP of [KRR13; KRR14] suggest that there is room to improve efficiency by invoking the method on more efficient MIPs. For example:

> *Is there an <u>almost</u> non-signaling analogue of the PCP Theorem?*
> Namely, does EXP have $O(1)$-query PCPs (equivalently, $O(1)$-prover MIPs) over a $O(1)$-size alphabet that are secure against almost non-signaling strategies?

The study of Property Testing against almost non-signaling strategies is likely a first step.

While almost non-signaling strategies are not our focus, we do prove that almost non-signaling strategies are within the reach of tools that we use for exact non-signaling ones. In Appendix C we show that every almost non-signaling function is "reasonably close" to a corresponding (exact) non-signaling function. The proof of this statement uses Fourier analysis, and the intuition behind it is similar to how almost-feasible solutions to Sherali–Adams relaxations are "smoothened" into feasible ones [RS09]. The generic lemma enables us, e.g., to extend Theorem 4 to the case of almost non-signaling strategies. Whether a whitebox analysis of linearity testing against almost non-signaling strategies can improve upon such a blackbox extension is an interesting open problem.

5 Preliminaries

For a finite domain D, we denote by U_D the set of all boolean functions $f\colon D \to \{0,1\}$; when D is clear from context, we may omit the subscript in U_D. When $D = \{0,1\}^n$, a function $f \in U_{\{0,1\}^n}$ is *linear* if $f(x) + f(y) = f(x+y)$ for all $x, y \in \{0,1\}^n$; LIN is the set of all such linear functions.

5.1 Fourier analysis of boolean functions

We use standard notation for Fourier analysis of boolean functions (see [O'D14] for more details). For a domain D of size N, we consider functions $f\colon \{0,1\}^D \to \mathbb{R}$. The inner product of two functions $g_1, g_2\colon \{0,1\}^D \to \mathbb{R}$ is $\langle g_1, g_2\rangle := \frac{1}{2^N}\sum_{x\in\{0,1\}^D} g_1(x)g_2(x)$. For a subset $T \subseteq D$, $\chi_T\colon \{0,1\}^D \to \mathbb{R}$ is the parity function $\chi_T(x) = (-1)^{\sum_{i\in T} x_i}$. It is not hard to verify that the set of functions $\{\chi_T\}_{T\subseteq D}$ is an orthonormal basis of the space of all functions from $\{0,1\}^D$ to $\mathbb{R}$. In particular, every function $f\colon \{0,1\}^D \to \mathbb{R}$ can be written as

$$f(\cdot) = \sum_{T\subseteq D} \widehat{f}(T)\chi_T(\cdot) \ ,$$

where $\widehat{f}(T) = \langle f, \chi_T\rangle = \frac{1}{2^N}\sum_{x\in\{0,1\}^D} f(x)\chi_T(x)$. In particular, by Parseval's identity for any two functions $f, g\colon \{0,1\}^D \to \mathbb{R}$ we have

$$\frac{1}{2^N}\sum_{x\in\{0,1\}^D} f(x)g(x) = \sum_{T\subseteq D} \widehat{f}(T)\widehat{g}(T) \ ,$$

which implies Plancherel's identity

$$\frac{1}{2^N}\sum_{x\in\{0,1\}^D} f(x)^2 = \sum_{T\subseteq D} \widehat{f}(T)^2 \ .$$

For a set $E \subseteq \{0,1\}^s$, its indicator function $\mathbf{1}_E\colon \{0,1\}^s \to \{0,1\}$ is defined as

$$\mathbf{1}_E = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{otherwise} \end{cases} \ .$$

Note that by Plancherel's identity we have $\sum_{T\subseteq[s]} \widehat{\mathbf{1}_E}(T)^2 = \mathbb{E}[\mathbf{1}_E] = \frac{|E|}{2^s}$. In particular, this implies $\|\widehat{\mathbf{1}_E}\|_1 = \sum_{T\subseteq[s]} |\widehat{\mathbf{1}_E}(T)| \le \sqrt{\sum_{T\subseteq[s]} \widehat{\mathbf{1}_E}(T)^2} \cdot \sqrt{\sum_{T\subseteq[s]} 1} \le \sqrt{\frac{|E|}{2^s}} \cdot 2^{s/2} = \sqrt{|E|}$.

5.2 Expressing boolean events as sums of parities

We state two lemmas that express the probability of certain events as probabilities about the *parities* of related events.

Lemma 5.1. *Let $X_1, \ldots, X_s$ be boolean random variables. Then, for every event $E \subseteq \{0,1\}^s$ it holds that*

$$\Pr[(X_1 \ldots, X_s) \in E] = \sum_{T\subseteq[s]} c_T \cdot \Pr\left[\sum_{i\in T} X_i = 0\right] \ ,$$

where $c_\emptyset = 2\cdot\widehat{\mathbf{1}_E}(\emptyset) - \mathbf{1}_E(\vec{0})$, and $c_T = 2\cdot\widehat{\mathbf{1}_E}(T)$ for all $T \neq \emptyset$. In particular, c_T's depend only on E and $\sum_{T\subseteq[s]} |c_T| \le 3\|\widehat{\mathbf{1}_E}\|_1 \le 3\sqrt{|E|}$.

Corollary 5.2. *Let $X_1, \ldots, X_s$ be boolean random variables. Then, for every $\vec{b} = (b_1, \ldots, b_s) \in \{0,1\}^s$ it holds that*

$$\Pr[X_1 = b_1, \ldots, X_s = b_s] = -1 + \frac{1}{2^{s-1}} \sum_{T \subseteq [s]} \Pr\left[\sum_{i \in T} X_i = \sum_{i \in T} b_i\right] \ .$$

Proof of Lemma 5.1. Define $p\colon \{0,1\}^s \to \mathbb{R}$ as $p(\vec{a}) = \Pr[X_1 = a_1, \ldots, X_s = a_s]$, and write $p = \sum_{T \subseteq [s]} \hat{p}(T) \cdot \chi_T$. We have

$$\begin{aligned}
\hat{p}(T) &= \mathbb{E}[p(\vec{a}) \cdot \chi_T(\vec{a})] \\
&= \frac{1}{2^s} \left(\sum_{\vec{a}: \sum_{i \in T} \vec{a}_i = 0} p(\vec{a}) - \sum_{\vec{a}: \sum_{i \in T} \vec{a}_i = 1} p(\vec{a}) \right) \\
&= \frac{1}{2^s} \left(2 \sum_{\vec{a}: \sum_{i \in T} \vec{a}_i = 0} p(\vec{a}) - 1 \right) \\
&= \frac{1}{2^s} \left(2 \Pr\left[\sum_{i \in T} X_i = 0\right] - 1 \right)
\end{aligned}$$

Let $E \subseteq \{0,1\}^s$ be an event, and let $\mathbf{1}_E\colon \{0,1\}^s \to \{0,1\}$ be its indicator function. Then, by Parseval's identity we have

$$\Pr[(X_1 \ldots, X_s) \in E] = \sum_{\vec{a} \in \{0,1\}^s} p(\vec{a}) \cdot \mathbf{1}_E(\vec{a}) = 2^s \cdot \sum_{T \subseteq [s]} \hat{p}(T) \cdot \widehat{\mathbf{1}_E}(T) \ .$$

By plugging in the formula $\hat{p}(T) = \frac{1}{2^s}\left(2 \Pr[\sum_{i \in T} X_i = 0] - 1\right)$, and using $\Pr[\sum_{i \in \emptyset} X_i = 0] = 1$ we get

$$\Pr[(X_1 \ldots, X_s) \in E] = \sum_{T \subseteq [s]} \left(2 \Pr\left[\sum_{i \in T} X_i = 0\right] - 1 \right) \cdot \widehat{\mathbf{1}_E}(T) = \sum_{T \subseteq [s]} c_T \cdot \Pr\left[\sum_{i \in T} X_i = 0\right] \ ,$$

where $c_\emptyset = 2 \cdot \widehat{\mathbf{1}_E}(\emptyset) - \sum_{T \subseteq [s]} \widehat{\mathbf{1}_E}(T)$, and $c_T = 2 \cdot \widehat{\mathbf{1}_E}(T)$ for all $T \neq \emptyset$. Since $\mathbf{1}_E(\cdot) = \sum_{T \subseteq [s]} \widehat{\mathbf{1}_E}(T) \chi_T(\cdot)$, it follows that $\mathbf{1}_E(\vec{0}) = \sum_{T \subseteq [s]} \widehat{\mathbf{1}_E}(T)$, as required.

Thus, by the argument in Section 5.1 we have $\sum_{T \subseteq [s]} |c_T| \leq 3 \sum_{T \subseteq [s]} |\widehat{\mathbf{1}_E}(T)| \leq 3\sqrt{|E|}$. □

Proof of Corollary 5.2. Let $E = \{\vec{b}\}$ be the singleton event. It is easy to verify that $\widehat{\mathbf{1}_E}(T) = (-1)^{\sum_{i \in T} b_i} \cdot 2^{-s}$. Therefore, by Lemma 5.1 we have

$$\Pr[X_1 = b_1, \ldots, X_s = b_s] = \sum_{T \subseteq [s]} c_T \cdot \Pr\left[\sum_{i \in T} X_i = 0\right] \ ,$$

where $c_\emptyset = 2 \cdot \widehat{\mathbf{1}_E}(\emptyset) - \mathbf{1}_E(\vec{0}) = \frac{1}{2^{s-1}} - \mathbf{1}_E(\vec{0})$, and $c_T = (-1)^{\sum_{i \in T} b_i} \cdot 2^{-s+1}$ for all $T \neq \emptyset$. By substituting $\Pr\left[\sum_{i \in T} X_i = 0\right]$ with $1 - \Pr\left[\sum_{i \in T} X_i = 1\right]$ for all $T \subseteq [s]$ such that $\sum_{i \in T} b_i = 1$ we

get

$$\begin{aligned}\Pr[X_1 = b_1, \ldots, X_s = b_s] &= \sum_{T \subseteq [s]} c_T \cdot \Pr\left[\sum_{i \in T} X_i = 0\right] \\ &= \left(-\mathbf{1}_E(0) - \sum_{T : \sum_{i \in T} b_i = 1} \frac{1}{2^{s-1}}\right) + \frac{1}{2^{s-1}} \sum_{T \subseteq [s]} \Pr\left[\sum_{i \in T} X_i = \sum_{i \in T} b_i\right] \\ &= -1 + \frac{1}{2^{s-1}} \sum_{T \subseteq [s]} \Pr\left[\sum_{i \in T} X_i = \sum_{i \in T} b_i\right] \ ,\end{aligned}$$

as required. □

5.3 A linear system

Below we prove that a certain linear system of equations, which we will use later, has a unique solution. This linear system is the inverse of the Hadamard–Walsh matrix.

Lemma 5.3. *For every positive integer n and real numbers $\{c_\beta\}_{\beta \in \{0,1\}^n}$, the system of 2^n linear equations over $\mathbb{R}$ in 2^n variables $\{z_\alpha\}_{\alpha \in \{0,1\}^n}$ given by*

$$\left\{ \forall \beta \in \{0,1\}^n \quad \sum_{\substack{\alpha \in \{0,1\}^n \\ \text{s.t. } \langle \alpha, \beta \rangle = 0}} z_\alpha = c_\beta \right\}$$

has a unique solution.

Proof. Let A be the $2^n \times 2^n$ boolean matrix corresponding to the system of linear equations, that is, such that $Az = c$. Note that the (β, α)-th entry of A is equal to $1 - \langle \alpha, \beta \rangle$, and in particular, the row in A corresponding to $\beta = 0^n$ is the all-ones row. Define H to be the matrix obtained from A by performing the following elementary row operations: for every $\beta \neq 0^n$, multiply row β by 2 and then subtract the all-ones row (corresponding to $\beta = 0^n$).

Note that the (β, α)-th entry of H is equal to $(-1)^{\langle \alpha, \beta \rangle}$. (The matrix H is sometimes called the Hadamard–Walsh matrix.) Indeed, this holds trivially for the row $\beta = 0^n$ as $H_{\beta,\alpha} = (-1)^{\langle \alpha, 0^n \rangle} = 1$, and for $\beta \neq 0^n$ we have $H_{\beta,\alpha} = 2(1 - \langle \alpha, \beta \rangle) - 1 = 1 - 2\langle \alpha, \beta \rangle = (-1)^{\langle \alpha, \beta \rangle}$. Since H was obtained from A by performing elementary row operations, A is invertible if and only if H is invertible. Observe that H is indeed invertible because the rows of H are mutually orthogonal since for every two distinct β and γ in $\{0,1\}^n$ it holds that

$$\langle \text{row } \beta, \text{row } \gamma \rangle = \sum_\alpha (-1)^{\langle \alpha, \beta \rangle} (-1)^{\langle \alpha, \gamma \rangle} = \sum_\alpha (-1)^{\langle \alpha, \beta \rangle + \langle \alpha, \gamma \rangle} = \sum_\alpha (-1)^{\langle \alpha, \beta + \gamma \rangle} = 0 \ ,$$

where the last equality holds because $\beta + \gamma \neq 0^n$. □

6 Non-signaling functions

We define *non-signaling functions*, introduce useful notation for them, and prove a simple lemma about them. The notions described here are used throughout the paper.

Definition 6.1 (non-signaling functions)**.** *A* k**-non-signaling (boolean) function** *over a finite domain* D *is a collection* $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq D, |S| \leq k}$ *where (i) each* $\mathcal{F}_S$ *is a distribution over functions* $f\colon S \to \{0,1\}$*, and (ii) for every two subsets* S *and* T *each of size at most* k*, the restrictions of* $\mathcal{F}_S$ *and* $\mathcal{F}_T$ *to* $S \cap T$ *are equal as distributions. (If* $S = \emptyset$ *then* $\mathcal{F}_S$ *always outputs the empty string.)*

Remark 6.2. Cryptographic applications (Section 4.3) motivate the study of *almost* non-signaling functions. In Appendix C we prove that these are well-approximated by non-signaling functions.

Given a set $S \subseteq D$ of size $|S| \leq k$ and a string $\vec{b} \in \{0,1\}^S$, we define

$$\Pr[\,\mathcal{F}(S) = \vec{b}\,] := \Pr_{f \leftarrow \mathcal{F}_S}[\,f(S) = \vec{b}\,] \ .$$

The non-signaling property in this notation is the following: for every two subsets $S, T \subseteq D$ of sizes $|S|, |T| \leq k$ and every string $\vec{b} \in \{0,1\}^{S \cap T}$, $\Pr[\,\mathcal{F}(S)|_{S\cap T} = \vec{b}\,] = \Pr[\,\mathcal{F}(T)|_{S\cap T} = \vec{b}\,]$.

Sometimes it is more convenient to consider a *vector* of inputs (rather than a *set*), and so we define notation for this case. Given a vector $\langle x_1, \ldots, x_s\rangle$ with entries in D and a vector $\langle b_1, \ldots, b_s\rangle$ with entries in $\{0,1\}$ (with $s \in \{1, \ldots, k\}$), we define $\Pr[\mathcal{F}(\langle x_1, \ldots, x_s\rangle) = \langle b_1, \ldots, b_s\rangle]$ and $\Pr[\mathcal{F}(x_1) = b_1, \ldots, \mathcal{F}(x_s) = b_s]$ to be the probability

$$\Pr_{f \leftarrow \mathcal{F}_{\{x_1,\ldots,x_s\}}}[\,f(x_1) = b_1, \ldots, f(x_s) = b_s\,] \ .$$

Note that $\{x_1, \ldots, x_s\}$ is an unordered set and its size may be less than s, because the entries of the vector $\langle x_1, \ldots, x_s\rangle$ may not be distinct. We abuse notation and still use symbols such as S and $\vec{b}$ to denote vectors as above. We stress that we use an ordering on S merely to match each element of S to the corresponding element in $\vec{b}$; the event remains unchanged if one permutes the entries of S and $\vec{b}$ according to the same permutation.

Remark 6.3 (Sherali–Adams hierarchy)**.** We note that k-non-signaling functions are solutions to the linear program arising from the k-relaxation in the Sherali–Adams hierarchy [SA90]. The variables are of the form $X_{S,\vec{b}}$ (for all $S \subseteq D$ of size at most k and $\vec{b} \in \{0,1\}^S$) and express $\Pr[\,\mathcal{F}(S) = \vec{b}\,]$. Consistency across subsets S and T is expressed using the natural linear constraints.[2]

We conclude with a useful lemma.

Lemma 6.4. *Let* $\mathcal{F}$ *be a* k*-non-signaling function over a domain* D*, let* S_1, S_2 *be subsets of* D *with* $|S_1 \cup S_2| \leq k$*, and let* $g_1\colon \{0,1\}^{S_1} \to \{0,1\}^r$ *and* $g_2\colon \{0,1\}^{S_2} \to \{0,1\}^r$ *be functions. If* $\Pr_{\mathcal{F}}[\,g_1(\mathcal{F}(S_1)) = g_2(\mathcal{F}(S_2))\,] \geq 1 - \varepsilon$*, then for every* $\vec{b} \in \{0,1\}^r$ *it holds that*

$$\left|\Pr_{\mathcal{F}}[\,g_1(\mathcal{F}(S_1)) = \vec{b}\,] - \Pr_{\mathcal{F}}[\,g_2(\mathcal{F}(S_2)) = \vec{b}\,]\right| \leq \varepsilon \ .$$

In particular, if $\varepsilon = 0$ *then* $\Pr_{\mathcal{F}}[\,g_1(\mathcal{F}(S_1)) = \vec{b}\,] = \Pr_{\mathcal{F}}[\,g_2(\mathcal{F}(S_2)) = \vec{b}\,]$ *for every* $\vec{b} \in \{0,1\}^r$*.*

[2] In fact it suffices to only have variables of the form $X_{S,1^S}$ as all other probabilities can be computed from these.

Proof. By direct computation:

$$
\begin{aligned}
&\left|\Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) = \vec{b}\,] - \Pr_{\mathcal{F}}[\, g_2(\mathcal{F}(S_2)) = \vec{b}\,]\right| \\
= &\left|\Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) = \vec{b} \wedge g_2(\mathcal{F}(S_2)) = \vec{b}\,] + \Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) = \vec{b} \wedge g_2(\mathcal{F}(S_2)) \neq \vec{b}\,]\right. \\
&\left. - \Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) = \vec{b} \wedge g_2(\mathcal{F}(S_2)) = \vec{b}\,] - \Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) \neq \vec{b} \wedge g_2(\mathcal{F}(S_2)) = \vec{b}\,]\right| \\
= &\left|\Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) = \vec{b} \wedge g_2(\mathcal{F}(S_2)) \neq \vec{b}\,] - \Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) \neq \vec{b} \wedge g_2(\mathcal{F}(S_2)) = \vec{b}\,]\right| \\
\leq &\Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) = \vec{b} \wedge g_2(\mathcal{F}(S_2)) \neq \vec{b}\,] + \Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) \neq \vec{b} \wedge g_2(\mathcal{F}(S_2)) = \vec{b}\,] \\
\leq &\Pr_{\mathcal{F}}[\, g_1(\mathcal{F}(S_1)) \neq g_2(\mathcal{F}(S_2))] \leq \varepsilon \ .
\end{aligned}
$$

Note that we are implicitly using the fact that $|S_1 \cup S_2| \leq k$ whenever we have S_1 and S_2 in the same probability event because we are querying $\mathcal{F}$ on all inputs in $S_1 \cup S_2$ at once. □

7 Quasi-distributions

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

Definition 7.1 (quasi-distributions)**.** *Let D be a finite domain, and denote by U_D the set of all boolean functions of the form $f\colon D \to \{0,1\}$. A* **quasi-distribution** *$\mathcal{Q}$ over a subset $G \subseteq U_D$ is a set of real numbers $\{q_f\}_{f \in U_D}$ such that $\sum_{f \in U_D} q_f = 1$ and $q_f = 0$ for every $f \notin G$.*

Definition 7.2 (quasi-probability)**.** *Given a quasi-distribution $\mathcal{Q} = \{q_f\}_{f \in U_D}$, a subset $S \subseteq D$, and a string $\vec{b} \in \{0,1\}^S$, we define the* **quasi-probability** *of the event "$\mathcal{Q}(S) = \vec{b}$" to be the following (possibly negative) real number*

$$\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] := \sum_{f \in U_D \text{ s.t. } f(S) = \vec{b}} q_f \ .$$

As in the case of non-signaling functions, it is sometimes more convenient to consider a *vector* of inputs rather than a *set*. Given a vector $\langle x_1, \ldots, x_s \rangle$ with entries in D and a vector $\langle b_1, \ldots, b_s \rangle$ with entries in $\{0,1\}$, we define $\Pr[\mathcal{Q}(\langle x_1, \ldots, x_s \rangle) = \langle b_1, \ldots, b_s \rangle]$ and $\Pr[\mathcal{Q}(x_1) = b_1, \ldots, \mathcal{Q}(x_s) = b_s]$ to be the (possibly negative) real number $\sum_{f \in U_D \text{ s.t. } \forall i \, f(x_i) = b_i} q_f$. We abuse notation and still use symbols such as S and $\vec{b}$ to denote vectors as above.

Since a quasi-distribution $\mathcal{Q}$ is defined by its weights $q = (q_f)_{f \in U_D}$, we can view $\mathcal{Q}$ as a function from $\{0,1\}^D$ to $\mathbb{R}$, where we identify a function $f\colon D \to \{0,1\}$ with the corresponding vector in $\{0,1\}^D$ and $q(f)$ with q_f. In particular, we can write $q(\cdot) = \sum_{T \subseteq D} \widehat{q}(T) \chi_T(\cdot)$, where $\chi_T(f) = (-1)^{\sum_{x \in T} f(x)}$, and $\widehat{q}(T) = \langle q, \chi_T \rangle = \frac{1}{2^{|D|}} \sum_{f\colon D \to \{0,1\}} q(f) \chi_T(f)$.

The following lemma is an analogue of Lemma 5.1 for quasi-distributions.

Lemma 7.3. *Let $\mathcal{Q} = (q_f)_f$ be a quasi-distribution, $S = \langle x_1, \ldots, x_s \rangle$ a vector with entries in $\{0,1\}^n$. Then, for every event $E \in \{0,1\}^s$ it holds that*

$$\sum_{f : f(S) \in E} q_f = \sum_{T \subseteq [s]} c_T \cdot \widetilde{\Pr}\left[\sum_{i \in T} \mathcal{Q}(x_i) = 0\right] = \sum_{T \subseteq [s]} c_T \cdot \left(\sum_{f : \sum_{i \in T} f(x_i) = 0} q_f \right) \ ,$$

where $c_\emptyset = 2 \cdot \widehat{\mathbf{1}_E}(\emptyset) - \mathbf{1}_E(\vec{0})$, and $c_T = 2 \cdot \widehat{\mathbf{1}_E}(T)$ for all $T \neq \emptyset$.

The proof of the lemma is immediate from the proof of Lemma 5.1, since the proof only uses the fact that probabilities add up to 1, which also holds for quasi-probabilities.

Definition 7.4 (locality)**.** *Let D be a finite domain of size N. For $1 \leq \ell \leq N$ a quasi-distribution $\mathcal{Q}$ over U_D is* **ℓ-local** *if for every subset $S \subseteq D$ of size $|S| \leq \ell$ and string $\vec{b} \in \{0,1\}^S$,*

$$\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] \in [0,1] \ .$$

For completeness, we also say that all quasi-distributions are 0-local.

If $\mathcal{Q}$ is ℓ-local, then for every subset $S \subseteq D$ of size $|S| \leq \ell$, we may view $\mathcal{Q}(S)$ as a probability distribution over $\{0,1\}^S$. If $\mathcal{Q}$ is ℓ-local then it is s-local for every $s \in \{0, 1, \ldots, \ell\}$.

For $\mathcal{Q}$ to be ℓ-local, it suffices for all relevant $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}]$ to be non-negative (as opposed to be in $[0,1]$). This is because $\sum_f q_f = 1$, so that $\sum_{\vec{b} \in \{0,1\}^S} \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = 1$ and, if all terms in this sum are non-negative, then we can deduce that $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] \leq 1$ for every $\vec{b}$.

Definition 7.5 (statistical distance)**.** *Given a finite domain D and an integer $\ell \in \{1,\ldots,|D|\}$, the* Δ_ℓ**-distance** *between two quasi-distributions $\mathcal{Q}$ and $\mathcal{Q}'$ is*

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

where $\Delta(\mathcal{Q}_S,\mathcal{Q}'_S) := \max_{E\subseteq\{0,1\}^S} \left|\widetilde{\Pr}[\mathcal{Q}(S)\in E] - \widetilde{\Pr}[\mathcal{Q}'(S)\in E]\right|$.

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 7.6 (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 $\Delta_{|D|}$-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 $S \subseteq D$ 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 $\sum_{f\in U} |q_f - q'_f|$ is arbitrarily large. We also remark that the Δ_ℓ-distance is not necessarily upper bounded by 1, and is in general unbounded.

Definition 7.7 (approximate locality)**.** *Given a finite domain D, an integer $\ell \in \{1,\ldots,|D|\}$, and a real number $\varepsilon \geq 0$, a quasi-distribution $\mathcal{Q}$ over U_D is* (ℓ,ε)**-local** *if, for every subset $S \subseteq D$ of size $|S| \leq \ell$ and every event $E \subseteq \{0,1\}^S$,*

$$\widetilde{\Pr}[\mathcal{Q}(S)\in E] \in [-\varepsilon, 1+\varepsilon] \ .$$

Approximate locality generalizes the notion of (exact) locality as in Definition 7.4. Indeed, note that in Definition 7.4 the condition is point-wise, i.e., $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] \in [0,1]$ for each $\vec{b} \in \{0,1\}^S$. However, this is in fact equivalent to the event-wise definition, $\widetilde{\Pr}[\mathcal{Q}(S)\in E] \in [0,1]$ for all $E \subseteq \{0,1\}^S$, and hence every ℓ-local quasi-distribution $\mathcal{Q}$ is $(\ell,0)$-local.

Below we discuss the following questions. Given an approximately local quasi-distribution $\mathcal{Q}$, can we find a local quasi-distribution $\mathcal{Q}'$ close to it? Moreover, can we ensure that $\mathcal{Q}'$ "looks like" $\mathcal{Q}$? We show that if $\mathcal{Q}$ is (ℓ,ε)-local and is supported over a set G of functions that is nice in some precise way, then there is an ℓ-local $\mathcal{Q}'$ over G that is close to $\mathcal{Q}$. The proof idea is similar to that of "smoothening" almost-feasible solutions to Sherali–Adams relaxations into feasible ones [RS09].

Lemma 7.8. *Let D be a finite domain, $\ell \in \{1,\ldots,|D|\}$ be an integer, and $\delta > 0$ and $\varepsilon \geq 0$ be reals. Let $G \subseteq U_D$ be a set of functions $f\colon D \to \{0,1\}$ such that for all subsets $S \subseteq D$ of size $|S| \leq \ell$ and for all strings $\vec{b} \in \{0,1\}^S$ it holds that $\Pr_{f\leftarrow G}[f(S) = \vec{b}] \in \{0\} \cup [\delta,1]$, where f is sampled uniformly at random from G. If $\mathcal{Q}$ is a (ℓ,ε)-local quasi-distribution over G, then there exists an ℓ-local quasi-distribution $\mathcal{Q}'$ over G such that $\Delta_\ell(\mathcal{Q},\mathcal{Q}') \leq (1+\varepsilon-\delta)\cdot\frac{\varepsilon}{\varepsilon+\delta}$.*

We highlight two notable special cases for the domain $D = \{0,1\}^n$. If $G = U_{\{0,1\}^n}$ (the set of *all* functions), then $\Pr_{f\leftarrow G}[f(S) = \vec{b}] = 2^{-\ell}$. Also, if $G = \mathsf{LIN}$ (the set of all *linear* functions), then for every subset $S \subseteq \{0,1\}^n$ of size at most ℓ and every string $\vec{b} \in \{0,1\}^S$ it holds that $\Pr_{f\leftarrow G}[f(S) = \vec{b}] = 0$ or $\Pr_{f\leftarrow G}[f(S) = \vec{b}] = 2^{-\dim(\mathrm{span}(S))} \geq 2^{-|S|} \geq 2^{-\ell}$. These two cases yield the following corollary.

Corollary 7.9. *If $\mathcal{Q}$ is a (ℓ,ε)-local quasi-distribution over $U_{\{0,1\}^n}$ (resp., LIN), then there is an ℓ-local quasi-distribution $\mathcal{Q}'$ over $U_{\{0,1\}^n}$ (resp., LIN) such that $\Delta_\ell(\mathcal{Q},\mathcal{Q}') \leq \frac{1+\varepsilon-2^{-\ell}}{1+2^\ell\varepsilon} \cdot 2^\ell\varepsilon < 2^\ell\varepsilon$.*

Proof. The hypothesis of Lemma 7.8 holds with $\delta = 2^{-\ell}$. So there exists an ℓ-local quasi-distribution $\mathcal{Q}'$ over $U_{\{0,1\}^n}$ (resp., LIN) such that $\Delta_\ell(\mathcal{Q},\mathcal{Q}') \leq \varepsilon \cdot \frac{1+\varepsilon-\delta}{\varepsilon+\delta} = \frac{1+\varepsilon-2^{-\ell}}{\varepsilon+2^{-\ell}} \cdot \varepsilon = \frac{1+\varepsilon-2^{-\ell}}{1+2^\ell\varepsilon} \cdot 2^\ell\varepsilon$. Clearly the fraction is smaller than 1, and so the entire expression is at most $2^\ell\varepsilon$. □

We now prove the lemma.

Proof of Lemma 7.8. Let $\mathcal{U}_G$ be the uniform distribution over all functions in G. For $\varepsilon' := \frac{\varepsilon}{\varepsilon+\delta}$, define the quasi-distribution $\mathcal{Q}' := (1-\varepsilon')\mathcal{Q} + \varepsilon'\mathcal{U}_G$. Namely, if the vector of quasi-probabilities of $\mathcal{Q}$ is $(q_f)_{f\in G}$, then the the vector of quasi-probabilities of $\mathcal{Q}'$ is $(q'_f)_{f\in G}$ where $q'_f := (1-\varepsilon')\cdot q_f + \varepsilon'/|G|$.

First, we show that $\mathcal{Q}'$ is an ℓ-local quasi-distribution. That is, for all subsets $S \subseteq D$ of size at most ℓ and for every $\vec{b} \in \{0,1\}^S$ it holds that $\widetilde{\Pr}[\mathcal{Q}'(S) = \vec{b}] \geq 0$. Fix such an S and $\vec{b}$. If $\Pr_{f\in G}[f(S) = \vec{b}] = 0$, then there is no $f \in G$ such that $f(S) = \vec{b}$, and hence $\widetilde{\Pr}[\mathcal{Q}'(S) = \vec{b}] = 0$. Otherwise, $\Pr_{f\in G}[f(S) = \vec{b}] \geq \delta$, and hence,

$$\begin{aligned}
\widetilde{\Pr}[\mathcal{Q}'(S) = \vec{b}] &= \sum_{f\in G: f(S)=\vec{b}} q'_f \\
&= \left(\sum_{f\in G: f(S)=\vec{b}} (1-\varepsilon')q_f\right) + \varepsilon' \Pr_{f\in G}[f(S) = \vec{b}] \\
&\geq \left(\sum_{f\in G: f(S)=\vec{b}} (1-\varepsilon')q_f\right) + \varepsilon' \cdot \delta \\
&\geq -\varepsilon(1-\varepsilon') + \varepsilon' \cdot \delta \\
&= -\varepsilon\left(\frac{\delta}{\varepsilon+\delta}\right) + \frac{\varepsilon}{\varepsilon+\delta}\delta = 0 \ .
\end{aligned}$$

Second, we show that $\mathcal{Q}$ and $\mathcal{Q}'$ are close in the sense that $\Delta_\ell(\mathcal{Q},\mathcal{Q}') \leq 2\varepsilon' \cdot (1+\varepsilon-\delta)$ (see Definition 7.5). Fix a subset $S \subseteq D$ of size at most ℓ, and let $E \subseteq \{0,1\}^S$. Then

$$\begin{aligned}
\left|\widetilde{\Pr}[\mathcal{Q}(S) \in E] - \widetilde{\Pr}[\mathcal{Q}'(S) \in E]\right| &= \left|\left(\sum_{f\in G: f(S)\in E} \varepsilon' q_f\right) - \varepsilon' \Pr_{f\in G}[f(S) \in E]\right| \\
&= \left|\varepsilon'\widetilde{\Pr}[\mathcal{Q}(S) \in E] - \varepsilon' \Pr_{f\in G}[f(S) \in E]\right| \\
&\leq \varepsilon'(1+\varepsilon-\delta) \ ,
\end{aligned}$$

as required. □

8 Equivalence of non-signaling functions and local quasi-distributions

We establish an equivalence between non-signaling functions and local quasi-distributions. First, we show that every local quasi-distribution induces a non-signaling function. Second, we show that the converse is also true, namely, that every non-signaling function can be described by a local quasi-distribution. In fact, the set of quasi-distributions describing it is a real affine subspace.

Theorem 8 (from local quasi-distributions to non-signaling functions)**.** *Let D be a finite domain. For every ℓ-local quasi-distribution $\mathcal{Q}$ over functions $f\colon D \to \{0,1\}$ there exists an ℓ-non-signaling function $\mathcal{F}$ over D such that for every subset $S \subseteq D$ of size $|S| \leq \ell$ and string $\vec{b} \in \{0,1\}^S$, $\Pr[\mathcal{F}(S) = \vec{b}] = \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}]$.*

Proof. For every subset $S \subseteq D$ of size $|S| \leq \ell$, define $\mathcal{F}_S$ to be the distribution over functions $f\colon S \to \{0,1\}$ where $\Pr[\mathcal{F}_S \text{ outputs } f] := \widetilde{\Pr}[\mathcal{Q}(S) = f(S)]$. Note that $\mathcal{F}_S$ is indeed a distribution because $\mathcal{Q}$ is ℓ-local, so the relevant probabilities are in $[0,1]$ and sum to 1. The definition immediately implies that $\Pr[\mathcal{F}(S) = \vec{b}] = \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}]$ for every string $\vec{b} \in \{0,1\}^S$. We are left to argue that $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq D, |S| \leq \ell}$ is ℓ-non-signaling.

Consider any two distinct subsets $S, T \subseteq D$ of size at most ℓ, and any string $\vec{b} \in \{0,1\}^{S \cap T}$. Let U_S denote the set of functions from $S \to \{0,1\}$. We have that

$$\begin{aligned}\Pr_{f \leftarrow \mathcal{F}_S}[f(S \cap T) = \vec{b}] &= \sum_{\substack{f \in U_S \text{ s.t.} \\ f(S \cap T) = \vec{b}}} \Pr[\mathcal{F}_S \text{ outputs } f] = \sum_{\substack{f \in U_S \text{ s.t.} \\ f(S \cap T) = \vec{b}}} \widetilde{\Pr}[\mathcal{Q}(S) = f(S)] \\ &= \sum_{\substack{f \in U_S \text{ s.t.} \\ f(S \cap T) = \vec{b}}} \sum_{\substack{g \in U \text{ s.t.} \\ g(S) = f(S)}} q_g = \sum_{\substack{g \in U \text{ s.t.} \\ g(S \cap T) = \vec{b}}} q_g = \widetilde{\Pr}[\mathcal{Q}(S \cap T) = \vec{b}]\end{aligned}$$

Similarly, we have that $\Pr_{f \leftarrow \mathcal{F}_T}[f(S \cap T) = \vec{b}] = \widetilde{\Pr}[\mathcal{Q}(S \cap T) = \vec{b}]$, and we conclude that $\Pr_{f \leftarrow \mathcal{F}_S}[f(S \cap T) = \vec{b}] = \Pr_{f \leftarrow \mathcal{F}_T}[f(S \cap T) = \vec{b}]$. Since S, T were arbitrary, $\mathcal{F}$ is ℓ-non-signaling. □

We now show that every k-non-signaling function $\mathcal{F}$ arises from a k-local quasi-distribution $\mathcal{Q}$. Moreover, the set of such quasi-distributions is an affine subspace of co-dimension $\binom{N}{\leq k}$ in $\mathbb{R}^{2^N}$, where $N = |D|$ and $\binom{N}{\leq k} := \sum_{i=0}^{k} \binom{N}{i}$. This converse is the interesting direction of the equivalence.

Theorem 9 (from non-signaling functions to local quasi-distributions)**.** *For every k-non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq D, |S| \leq k}$ over a finite domain D of size N there exists a k-local quasi-distribution $\mathcal{Q}$ over functions $f\colon D \to \{0,1\}$ that describes $\mathcal{F}$ (for every subset $S \subseteq D$ of size $|S| \leq k$ and string $\vec{b} \in \{0,1\}^S$ it holds that $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = \Pr[\mathcal{F}(S) = \vec{b}]$).*

Moreover, the set of such quasi-distributions (viewed as vectors in $\mathbb{R}^{2^N}$) is the affine subspace of co-dimension $\binom{N}{\leq k}$ given by $\mathcal{Q}_0 + \mathrm{span}\{\chi_T : T \subseteq D, |T| > k\}$, where $\mathcal{Q}_0$ is any solution and $\chi_T\colon \{0,1\}^D \to \mathbb{R}$ is defined as $\chi_T(f) := (-1)^{\sum_{x \in T} f(x)}$.

Proof. We break the proof into three parts. First, we find one quasi-distribution that matches $\mathcal{F}$. Then, we find an affine space of such quasi-distributions. Finally, we prove that this affine space contains all possible solutions.

Finding one solution. We construct a k-local quasi-distribution $\mathcal{Q}$ that behaves like $\mathcal{F}$ on all sets of size at most k. Consider $q(\cdot) := \sum_{T:|T|\le k} \widehat{q}(T)\chi_T(\cdot)$, where $\widehat{q}(T)$ is defined as follows.

$$\widehat{q}(T) := \begin{cases} \frac{1}{2^N} & \text{if } T = \emptyset \\ \frac{2}{2^N}\left(\Pr[\sum_{x\in T}\mathcal{F}(x) = 0] - \frac{1}{2}\right) & \text{if } 1 \le |T| \le k \\ 0 & \text{if } |T| > k \end{cases} .$$

Note that $\mathcal{Q}$ is a quasi-distribution because $\sum_f q_f = 2^N\langle q, \chi_\emptyset\rangle = 2^N\widehat{q}(\emptyset) = 1$. Now, for any subset $S = \langle x_1, \ldots, x_s\rangle$ with $|S| \le k$,

$$\begin{aligned} \sum_{f:\sum_{x\in S} f(x)=0} q_f &= \sum_f q_f(-1)^{\sum_{x\in S} f(x)} + \sum_{f:\sum_{x\in S} f(x)=1} q_f \\ &= 2^N\langle q, \chi_S\rangle + \left(1 - \sum_{f:\sum_{x\in S} f(x)=0} q_f\right) \\ &= 2^N \frac{1}{2^{N-1}}\left(\Pr\left[\sum_{x\in S}\mathcal{F}(x) = 0\right] - \frac{1}{2}\right) + \left(1 - \sum_{f:\sum_{x\in S} f(x)=0} q_f\right) \\ &= 2\Pr\left[\sum_{x\in S}\mathcal{F}(x) = 0\right] - \sum_{f:\sum_{x\in S} f(x)=0} q_f \ , \end{aligned}$$

which implies that

$$\widetilde{\Pr}\left[\sum_{x\in S}\mathcal{Q}(x) = 0\right] = \sum_{f:\sum_{x\in S} f(x)=0} q_f = \Pr\left[\sum_{x\in S}\mathcal{F}(x) = 0\right] .$$

Therefore,

$$\widetilde{\Pr}\left[\sum_{x\in S}\mathcal{Q}(x) = 1\right] = 1 - \widetilde{\Pr}\left[\sum_{x\in S}\mathcal{Q}(x) = 0\right] = 1 - \Pr\left[\sum_{x\in S}\mathcal{F}(x) = 0\right] = \Pr\left[\sum_{x\in S}\mathcal{F}(x) = 1\right] .$$

Thus, by Corollary 5.2 for any choice of bits $b_1, \ldots, b_s \in \{0, 1\}$ we have

$$\begin{aligned} \Pr[\mathcal{F}(x_1) = b_1, \ldots, \mathcal{F}(x_s) = b_s] &= -1 + \frac{1}{2^{s-1}}\sum_{T\subseteq[s]} \Pr\left[\sum_{i\in T}\mathcal{F}(x_i) = \sum_{i\in T} b_i\right] \\ &= -1 + \frac{1}{2^{s-1}}\sum_{T\subseteq[s]} \widetilde{\Pr}\left[\sum_{i\in T}\mathcal{Q}(x_i) = \sum_{i\in T} b_i\right] \\ &= \widetilde{\Pr}[\mathcal{Q}(x_1) = b_1, \ldots, \mathcal{Q}(x_s) = b_s] \ . \end{aligned}$$

This shows that $\mathcal{Q}$ behaves like $\mathcal{F}$ on all sets of size at most k.

Finding more solutions. We argue that Fourier coefficients for subsets T of size greater than k do not affect the induced non-signaling function. Indeed, fix a subset $T \subseteq D$ of size greater than

k, and let $\mathcal{Q}' = (q'_f)_f$ be the quasi-distribution obtained from $\mathcal{Q} = (q_f)_f$ by defining its weights as $q'_f := q_f + c\chi_T(f)$. Observe that for every ordered subset $S = \langle x_1, \ldots, x_s \rangle$ with $s \leq k$ and bits $b_1, \ldots, b_s$ it holds that

$$\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = \sum_{f:f(S)=\vec{b}} q_f = \sum_{f:f(S)=\vec{b}} (q_f + c\chi_T(f)) = \widetilde{\Pr}[\mathcal{Q}'(S) = \vec{b}] \ .$$

To see that the middle equality holds, observe that there exists $y \in T \setminus S$, and thus

$$\sum_{f:f(S)=\vec{b}} \chi_T(f) = \sum_{f(S)=\vec{b}} (-1)^{\sum_{x\in T} f(x)} = \sum_{\substack{f:f(S)=\vec{b} \\ f(y)=0}} (-1)^{\sum_{x\in T\setminus\{y\}} f(x)} - \sum_{\substack{f:f(S)=\vec{b} \\ f(y)=1}} (-1)^{\sum_{x\in T\setminus\{y\}} f(x)} = 0 \ .$$

Therefore, $\mathcal{Q}'$ matches $\mathcal{Q}$ (and thus also $\mathcal{F}$) on all sets of size at most k. Since this holds for every T with $|T| > k$, we see that *every* q' in $q + \mathrm{span}\{\chi_T : T \subseteq D, |T| > k\}$ also matches $\mathcal{F}$ on all subsets of size at most k.

We found all solutions. Observe that if $\mathcal{Q}$ is a quasi-distribution, then for every subset $T \subseteq D$ with $1 \leq |T| \leq k$ it holds that

$$\begin{aligned}
\widehat{q}(T) &= \frac{1}{2^N} \sum_f q_f (-1)^{\sum_{x\in T} f(x)} \\
&= \frac{1}{2^N} \left(\sum_{f:\sum_{x\in T} f(x)=0} q_f - \sum_{f:\sum_{x\in T} f(x)=1} q_f \right) \\
&= \frac{1}{2^N} \left(\widetilde{\Pr}\left[\sum_{x\in T} \mathcal{Q}(x) = 0 \right] - \widetilde{\Pr}\left[\sum_{x\in T} \mathcal{Q}(x) = 1 \right] \right) \\
&= \frac{1}{2^{N-1}} \left(\widetilde{\Pr}\left[\sum_{x\in T} \mathcal{Q}(x) = 0 \right] - \frac{1}{2} \right) \ .
\end{aligned}$$

If $\mathcal{Q}$ and $\mathcal{F}$ match on all input sets of size at most k, then they match on all parity events of size at most k, and so $\widehat{q}(T) = \frac{1}{2^{N-1}} \left(\widetilde{\Pr}[\sum_{x\in T} \mathcal{F}(x) = 0] - \frac{1}{2} \right)$. Since $\widehat{q}(\emptyset) = \frac{1}{2^N} \sum_f q_f = \frac{1}{2^N}$, we see that exactly $\binom{N}{\leq k}$ Fourier coefficients are determined. Thus, the set of all solutions is contained in $q + \mathrm{span}\{\chi_T : T \subseteq D, |T| > k\}$.

On the other hand, we have already shown that the affine space $q + \mathrm{span}\{\chi_T : T \subseteq D, |T| > k\}$ contains only quasi-distributions that match $\mathcal{F}$ on all sets of size at most k. Thus, the affine space of *all* quasi-distributions that match $\mathcal{F}$ is precisely $q + \mathrm{span}\{\chi_T : T \subseteq D, |T| > k\}$. □

9 Quasi-distributions over functions with small support

We show that *every* k-non-signaling function can be expressed as a quasi-distribution over functions with small support, namely, functions that evaluate to 1 for at most k inputs. For linearity testing, this implies that restricting a quasi-distribution to functions that are ε-close to linear is an empty condition, because all k-non-signaling functions can be expressed by such quasi-distributions for $\varepsilon = \frac{k}{2^n}$, regardless of whether they pass the linearity test with high or low probability.

For a finite domain D, we denote by U_D the set of all boolean functions $f\colon D \to \{0,1\}$ and, for $k \leq |D|$, denote by $U_{\leq k}$ the subset of U_D of all functions that evaluate to 1 for at most k values in D. We show that every k-non-signaling function $\mathcal{F}$ is described by a quasi-distribution over $U_{\leq k}$.

Theorem 10. *Let D be a finite domain. For every k-non-signaling function $\mathcal{F}$ over D there exists a k-local quasi-distribution $\mathcal{Q}$ over D supported on $U_{\leq k}$ such that for every subset $S \subseteq D$ of size $|S| \leq k$ and string $\vec{b} \in \{0,1\}^S$ it holds that $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = \Pr[\mathcal{F}(S) = \vec{b}]$.*

The proof of Theorem 10 relies on the following claim.

Claim 9.1. *Let $\mathcal{F}$ be a k-non-signaling function over a domain D, and let $\mathcal{Q}$ be a quasi-distribution over functions $f\colon D \to \{0,1\}$. If for every subset $S \subseteq D$ with $1 \leq |S| \leq k$ it holds that $\widetilde{\Pr}[\mathcal{Q}(S) = 1^{|S|}] = \Pr[\mathcal{F}(S) = 1^{|S|}]$ then for every subset $S \subseteq D$ with $|S| \leq k$ and string $\vec{b} \in \{0,1\}^S$ it holds that $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = \Pr[\mathcal{F}(S) = \vec{b}]$.*

We first prove Theorem 10 using the claim, and then prove the claim.

Proof of Theorem 10. By Claim 9.1 it suffices to prove that the following linear system of equations, in the variables $\{q_f\}_{f \in U_{\leq k}}$, has a solution:

$$\left\{ \begin{array}{rcll} \displaystyle\sum_{f \in U_{\leq k}} q_f & = & 1 & \\ \displaystyle\sum_{\substack{f \in U_{\leq k} \text{ s.t.} \\ f(S) = 1^{|S|}}} q_f & = & \Pr[\mathcal{F}(S) = 1^{|S|}] & \forall\, S \subseteq D \text{ with } 1 \leq |S| \leq k \end{array} \right\} .$$

We do so by iteratively assigning values to the variables $\{q_f\}_{f \in U_{\leq k}}$, by considering all functions with support size k, then with support size $k-1$, and so on. At a high level, we shall use the fact that this system of linear equations corresponds to an upper triangular matrix (once variables are ordered according to support sizes), and thus can be solved via back substitution.

First, consider any $f \in U_{\leq k}$ such that $|\mathrm{supp}(f)| = k$, and let $S := \mathrm{supp}(f)$. Since f is the *only* function in $U_{\leq k}$ whose support equals S, we must assign

$$q_f := \Pr[\mathcal{F}(\mathrm{supp}(f)) = 1^k] \ .$$

Next, we use induction on $s = k-1, \ldots, 1$ in decreasing order. Consider any $f \in U_{\leq k}$ such that $|\mathrm{supp}(f)| = s$, and set

$$q_f := \Pr[\mathcal{F}(\mathrm{supp}(f)) = 1^s] - \left(\sum_{\substack{f' \in U_{\leq k} \text{ s.t.} \\ \mathrm{supp}(f') \supsetneq \mathrm{supp}(f)}} q_{f'} \right) .$$

The above is well-defined since we first define q_f for all functions with larger support. Moreover, any choice of $q_{f''}$ for functions f'' whose support does not contain $\mathrm{supp}(f)$ does *not* affect the quasi-probability $\widetilde{\Pr}[\mathcal{Q}(\mathrm{supp}(f)) = 1^s]$, and so we may think of this assignment as q_f satisfying the constraint $\widetilde{\Pr}[\mathcal{Q}(\mathrm{supp}(f)) = 1^s] = \Pr[\mathcal{F}(\mathrm{supp}(f)) = 1^s]$.

Finally, if f is the all-zero function we define

$$q_f := 1 - \sum_{f' \neq f} q_{f'} \ ,$$

so that $\sum_{f \in U_{\leq k}} q_f = 1$. It is clear from the construction that the assignments to the variables $\{q_f\}_{f \in U_{\leq k}}$ above satisfy the necessary linear constraints, as desired. □

Proof of Claim 9.1. Fix any subset $S \subseteq D$ with $|S| \leq k$ and string $\vec{b} \in \{0,1\}^S$. We prove that $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = \Pr[\mathcal{F}(S) = \vec{b}]$, via induction on $|Z|$ where $Z := \{i \in S : b_i = 0\}$.

If $|Z| = 0$, then $\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] = \Pr[\mathcal{F}(S) = \vec{b}]$ holds by the assumption of the claim.

Now suppose that $|Z| > 0$, and let $i^* \in S$ be any coordinate such that $b_{i^*} = 0$. Let $\vec{b}_{\neg i^*} \in \{0,1\}^S$ be the vector obtained from $\vec{b}$ by *flipping* the i^*-th coordinate to 1, and let $\vec{b}_{-i^*} \in \{0,1\}^{S \setminus \{i^*\}}$ be the vector obtained from $\vec{b}$ by *removing* the i^*-th coordinate. We deduce that

$$\begin{aligned}
\Pr[\mathcal{F}(S) = \vec{b}] &= \Pr[\mathcal{F}(S \setminus \{i^*\}) = \vec{b}_{-i^*}] - \Pr[\mathcal{F}(S) = \vec{b}_{\neg i^*}] \ , \text{ and} \\
\widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] &= \widetilde{\Pr}[\mathcal{Q}(S \setminus \{i^*\}) = \vec{b}_{-i^*}] - \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}_{\neg i^*}] \ .
\end{aligned}$$

The inductive hypothesis tells us that $\Pr[\mathcal{F}(S \setminus \{i^*\}) = \vec{b}_{-i^*}] = \widetilde{\Pr}[\mathcal{Q}(S \setminus \{i^*\}) = \vec{b}_{-i^*}]$ and $\Pr[\mathcal{F}(S) = \vec{b}_{\neg i^*}] = \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}_{\neg i^*}]$, from which we obtain that $\Pr[\mathcal{F}(S) = \vec{b}] = \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}]$, as claimed. □

10 Exact local characterization of linear functions

We prove our results about non-signaling functions that always pass the linearity test. The theorem below states that the test passes with probability 1 if and only if the non-signaling function on sets of size at most $k-1$ can be described by a $(k-1)$-local quasi-distribution over linear functions.

Theorem 11 (exact local characterization)**.** *Let $\mathcal{F}$ be a k-non-signaling function with $k \geq 4$. The following statements are equivalent.*

1. *The linearity test always accepts:* $\Pr_{x,y,\mathcal{F}}[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] = 1$.
2. *For all $x, y \in \{0,1\}^n$ it holds that* $\Pr_{\mathcal{F}}[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] = 1$.
3. *There exists a unique $(k-1)$-local quasi-distribution $\mathcal{L}$ over* LIN *such that for every set $S \subseteq \{0,1\}^n$ of size $|S| \leq k-1$ and vector $\vec{b} \in \{0,1\}^S$ it holds that* $\Pr[\mathcal{F}(S) = \vec{b}] = \widetilde{\Pr}[\mathcal{L}(S) = \vec{b}]$.

We comment on several aspects of the theorem.

- **The case of large k.** If $k \geq n+1$, then $\mathcal{L}$ in Item 3 is in fact a (standard) distribution over linear functions.

  Explanation. Let ℓ_α be the weight assigned to the linear function $\langle \alpha, \cdot \rangle$ by $\mathcal{L}$. Since $\mathcal{L}$ matches $\mathcal{F}$ on sets of size n, we see that each ℓ_α is non-negative:

  $$\ell_\alpha = \sum_{\alpha' : \langle \alpha', e_i \rangle = \alpha_i \ \ 1 \leq i \leq n} \ell_{\alpha'} = \Pr[\mathcal{F}(e_1) = \alpha_1, \ldots, \mathcal{F}(e_n) = \alpha_n] \geq 0 \ .$$

- **Agreement on $k-1$ layers.** The fact that $|S| < k$ in Item 3 is necessary, because we can construct a k-non-signaling function $\mathcal{F}$ where $\Pr[\mathcal{F}(S) = \vec{b}] \neq \widetilde{\Pr}[\mathcal{L}(S) = \vec{b}]$ when $|S| = k$.

  Explanation. Let S_1 be the set of S such that $|S| < k$ or S is linearly dependent, and S_2 be the set of S such that $|S| = k$ and S is linearly independent. The non-signaling function $\mathcal{F}$ that answers according to a uniformly random linear function on all sets in S_1 and answers with uniformly random bits that sum to 0 on all sets in S_2 is k-non-signaling. Furthermore, the corresponding unique $\mathcal{L}$ is the uniform distribution over linear functions, and so $\Pr[\mathcal{F}(S) = \vec{b}] \neq \widetilde{\Pr}[\mathcal{L}(S) = \vec{b}]$ when $S \in S_2$.

- **The case of $k = 3$.** In the theorem it is necessary to have $k \geq 4$. This is because for $k = 3$ it is not true that Item 3 always implies Item 2: it is possible for Item 3 to hold while the linearity test passes with probability 0.

  Explanation. Let $\mathcal{L}$ be a uniform distribution over linear functions, and let $\mathcal{F}$ be a 3-non-signaling function that agrees with $\mathcal{L}$ on all query sets of size 2. For every subset $\{x, y, z\} \subseteq \{0,1\}^n \setminus \{0^n\}$ of size 3, the distribution of $\mathcal{F}$ is uniform over $\{(1,0,0), (0,1,0), (0,0,1), (1,1,1)\}$. If the input set S contains 0^n, $\mathcal{F}_S$ assigns 0^n to 0 and answers the rest according to $\mathcal{F}_{S \setminus \{0^n\}}$. One can verify that $\mathcal{F}$ is indeed a 3-non-signaling function. Clearly, $\mathcal{F}$ satisfies Item 3, but passes the linearity test with probability 0, and hence does not satisfy Item 2.

Proof that $1 \iff 2$. The acceptance probability of the test can be re-written as

$$\Pr_{x,y \leftarrow \{0,1\}^n, \mathcal{F}}[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] = \frac{1}{2^{2n}} \sum_{x,y \in \{0,1\}^n} \Pr_{\mathcal{F}}[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] \ ,$$

and note that each of the probabilities in the sum lies in $[0,1]$. Therefore, the acceptance probability is 1 if and only if for *all* $x, y \in \{0,1\}^n$ it holds that $\Pr_{\mathcal{F}}[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] = 1$. □

Proof that 2 $\implies$ 3. We first argue that if $\mathcal{F}$ behaves linearly on sets of the form $\{x, y, x+y\}$, then it behaves linearly on all sets of size less than k. Let $s \in \{2, \ldots, k-1\}$, $x_1, \ldots, x_s \in \{0,1\}^n$, and $b \in \{0,1\}$, and define $S_i := \{\sum_{j=1}^{i} x_j, x_{i+1}, \ldots, x_s\}$ for every $i \in \{1, \ldots, s\}$. Note that $|S_i \cup S_{i+1}| = s - i + 2 \leq s + 1 \leq k$. Letting $\mathsf{add}(\cdot)$ be the addition function, the fact that the linearity test always passes implies that

$$\Pr\left[\mathsf{add}(\mathcal{F}(S_i)) = \mathsf{add}(\mathcal{F}(S_{i+1}))\right] = \Pr\left[\mathcal{F}\left(\sum_{j=1}^{i} x_j\right) + \mathcal{F}(x_{i+1}) = \mathcal{F}\left(\sum_{j=1}^{i+1} x_j\right)\right] = 1 \ .$$

This implies that $\Pr[\mathcal{F}(\sum_{i=1}^{s} x_i) = b] = \Pr[\sum_{i=1}^{s} \mathcal{F}(x_i) = b]$, via the following argument:

$$\begin{aligned}
\left|\Pr\left[\sum_{i=1}^{s} \mathcal{F}(x_i) = b\right] - \Pr\left[\mathcal{F}\left(\sum_{i=1}^{s} x_i\right) = b\right]\right| &= |\Pr[\mathsf{add}(\mathcal{F}(S_1)) = b] - \Pr[\mathsf{add}(\mathcal{F}(S_s)) = b]| \\
&= \left|\sum_{i=1}^{s-1} \Pr[\mathsf{add}(\mathcal{F}(S_i)) = b] - \Pr[\mathsf{add}(\mathcal{F}(S_{i+1})) = b]\right| \\
&\leq \sum_{i=1}^{s-1} |\Pr[\mathsf{add}(\mathcal{F}(S_i)) = b] - \Pr[\mathsf{add}(\mathcal{F}(S_{i+1})) = b]| = 0 \ ,
\end{aligned}$$

where the last equality is by Lemma 6.4, since $|S_i \cup S_{i+1}| \leq k$ for every i. Note that s must be strictly less than k because $|S_1 \cup S_2| = s + 1$.

We now construct $\mathcal{L}$, and argue that it has the desired properties. Define $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$ to be the solution to the system of equations in Lemma 5.3 where $c_\beta := \Pr[\mathcal{F}(\beta) = 0]$ for each $\beta \in \{0,1\}^n$, and let $\mathcal{L}$ be the quasi-distribution over LIN that assigns weight ℓ_α to the linear function $\langle \alpha, \cdot \rangle$. That is, $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$ satisfy the linear equations

$$\sum_{\alpha : \langle \alpha, x \rangle = 0} \ell_\alpha = \Pr[\mathcal{F}(x) = 0]$$

for all $x \in \{0,1\}^n$. Note that $\mathcal{L}$ is indeed a quasi-distribution, because $\sum_\alpha \ell_\alpha = \Pr[\mathcal{F}(0^n) = 0] = \Pr_{x \leftarrow \{0,1\}^n}[\mathcal{F}(0^n) + \mathcal{F}(x) = \mathcal{F}(x)] = 1$ (as $\mathcal{F}$ always passes the linearity test). We remark that every quasi-distribution supported on LIN is uniquely determined by its induced distributions on sets of size 1: in Appendix A we prove that a quasi-distribution is supported on LIN if and only if its distributions on sets of size 1 determine all of its Fourier coefficients.

Moreover, by definition of $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$, for every $x \in \{0,1\}^n$ it holds that

$$\Pr[\mathcal{F}(x) = 0] = \sum_{\alpha : \langle \alpha, x \rangle = 0} \ell_\alpha = \widetilde{\Pr}[\mathcal{L}(x) = 0] \ ,$$

which implies that for every $x \in \{0,1\}^n$ and bit $b \in \{0,1\}$ it holds that $\Pr[\mathcal{F}(x) = b] = \widetilde{\Pr}[\mathcal{L}(x) = b]$. In other words, $\mathcal{F}$ and $\mathcal{L}$ match on sets of size 1. This allows us to derive the same conclusion for all sets of size less than k, as follows.

For every $s \in \{1,\ldots,k-1\}$, $x_1,\ldots,x_s \in \{0,1\}^n$, and $b_1,\ldots,b_s \in \{0,1\}$,

$$\begin{aligned}
\Pr[\mathcal{F}(x_1)=b_1,\ldots,\mathcal{F}(x_s)=b_s] &= -1 + \frac{1}{2^{s-1}} \sum_{T\subseteq[s]} \Pr\left[\sum_{i\in T} \mathcal{F}(x_i) = \sum_{i\in T} b_i\right] \text{ (by Corollary 5.2)} \\
&= -1 + \frac{1}{2^{s-1}} \sum_{T\subseteq[s]} \Pr\left[\mathcal{F}\left(\sum_{i\in T} x_i\right) = \sum_{i\in T} b_i\right] \text{ (by linearity)} \\
&= -1 + \frac{1}{2^{s-1}} \sum_{T\subseteq[s]} \widetilde{\Pr}\left[\mathcal{L}\left(\sum_{i\in T} x_i\right) = \sum_{i\in T} b_i\right] \\
&= -1 + \frac{1}{2^{s-1}} \sum_{T\subseteq[s]} \widetilde{\Pr}\left[\sum_{i\in T} \mathcal{L}(x_i) = \sum_{i\in T} b_i\right] \text{ (since } \mathrm{supp}(\mathcal{L}) \subseteq \mathsf{LIN}) \\
&= \widetilde{\Pr}[\mathcal{L}(x_1)=b_1,\ldots,\mathcal{L}(x_s)=b_s] \text{ . (by Lemma 7.3)}
\end{aligned}$$

Finally, since $\mathcal{L}$ agrees with $\mathcal{F}$ on all subsets of size less than k, the quasi-probabilities must be in $[0,1]$, which means that $\mathcal{L}$ is $(k-1)$-local. □

Proof that 3 $\implies$ 2. Suppose that there exists a $(k-1)$-local quasi-distribution $\mathcal{L}$ over LIN such that for every $s \in \{1,\ldots,k-1\}$, $x_1,\ldots,x_s \in \{0,1\}^n$, and $b_1,\ldots,b_s \in \{0,1\}$ it holds that $\Pr[\mathcal{F}(x_1) = b_1,\ldots,\mathcal{F}(x_s)=b_s] = \widetilde{\Pr}[\mathcal{L}(x_1)=b_1,\ldots,\mathcal{L}(x_s)=b_s]$. For every $\alpha \in \{0,1\}^n$ denote by ℓ_α the weight assigned by $\mathcal{L}$ to the linear function $\langle\alpha,\cdot\rangle$. For every $x,y \in \{0,1\}^n$ it holds that

$$\begin{aligned}
\Pr[\mathcal{F}(x)+\mathcal{F}(y)=\mathcal{F}(x+y)] &= \sum_{b_1,b_2} \Pr[\mathcal{F}(x)=b_1, \mathcal{F}(y)=b_2, \mathcal{F}(x+y)=b_1+b_2] \\
&= \sum_{b_1,b_2} \widetilde{\Pr}[\mathcal{L}(x)=b_1, \mathcal{L}(y)=b_2, \mathcal{L}(x+y)=b_1+b_2] \\
&= \sum_{b_1,b_2} \sum_{\substack{\alpha:\langle\alpha,x\rangle=b_1 \\ \langle\alpha,y\rangle=b_2 \\ \langle\alpha,x+y\rangle=b_1+b_2}} \ell_\alpha = \sum_{b_1,b_2} \sum_{\substack{\alpha:\langle\alpha,x\rangle=b_1 \\ \langle\alpha,y\rangle=b_2}} \ell_\alpha = \sum_\alpha \ell_\alpha = 1 \ ,
\end{aligned}$$

as desired. Note that the equality on the second line uses the assumption that $k \geq 4$. This is because we need $\mathcal{L}$ to match $\mathcal{F}$ on sets of size 3, and we only know that $\mathcal{L}$ matches $\mathcal{F}$ on all sets of size at most $k-1$. □

11 Robust local characterization of linear functions

We prove our results about non-signaling functions that pass the linearity test with high probability. Given a k-non-signaling function $\mathcal{F}$, define its self-correction $\hat{\mathcal{F}}$ as follows. On an input $x \in \{0,1\}^n$ we sample from $\hat{\mathcal{F}}_{\{x\}}$ by drawing a uniform $w \in \{0,1\}^n$, sampling a function f from $\mathcal{F}_{\{x+w,w\}}$, and outputting $f(x+w)+f(w)$. We generalize this correction to larger input sets in the natural way.

Definition 11.1. *Given a k-non-signaling function $\mathcal{F}$, define the* **self-correction of $\mathcal{F}$** *as follows. Given a set $S = \{x_1, \ldots, x_s\} \subseteq \{0,1\}^n$, we sample from $\hat{\mathcal{F}}_{\{x_1,\ldots,x_s\}}$ by drawing uniform and independent $w_1, \ldots, w_s \in \{0,1\}^n$, sampling a function f from $\mathcal{F}_{\{x_1+w_1,\ldots,x_s+w_s,w_1,\ldots,w_s\}}$, and outputting the function $\hat{f}$ that maps each x_i to $f(x_i+w_i)+f(w_i)$. That is, for every subset $S = \{x_1, \ldots, x_s\} \subseteq \{0,1\}^n$ of size at most $\hat{k}$ and $\vec{b} \in \{0,1\}^S$,*

$$\Pr[\hat{\mathcal{F}}(S) = \vec{b}] := \Pr_{\substack{w_1,\ldots,w_s \leftarrow \{0,1\}^n \\ \mathcal{F}}} \left[\begin{array}{l} \mathcal{F}(x_1+w_1)+\mathcal{F}(w_1) = b_1 \\ \quad \vdots \\ \mathcal{F}(x_s+w_s)+\mathcal{F}(w_s) = b_s \end{array} \right] .$$

$\hat{\mathcal{F}}$ is a $\hat{k}$-non-signaling function for $\hat{k} \leq \lfloor k/2 \rfloor$. This follows immediately from the fact that the w_i's are random and independent, and the fact that $\mathcal{F}$ is k-non-signaling.

The following theorem says that, if a k-non-signaling function $\mathcal{F}$ passes the linearity test with high probability, then $\hat{\mathcal{F}}$ is close to a quasi-distribution over linear functions.

Theorem 12 (robust local characterization)**.** *Let $\mathcal{F}$ be a k-non-signaling function with $k \geq 7$, and let $\hat{\mathcal{F}}$ be its ($\hat{k}$-non-signaling) self-correction. Each of the following statements implies the next one.*

1. *The linearity test accepts with probability $1-\varepsilon$: $\Pr_{x,y,\mathcal{F}}[\mathcal{F}(x)+\mathcal{F}(y) = \mathcal{F}(x+y)] \geq 1-\varepsilon$.*
2. *For all $x, y \in \{0,1\}^n$ it holds that $\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(x)+\hat{\mathcal{F}}(y) = \hat{\mathcal{F}}(x+y)] \geq 1-\hat{\varepsilon}$ with $\hat{\varepsilon} := 4\varepsilon$; moreover, it also holds that $\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(0^n) = 0] = 1$.*
3. *There exists a quasi-distribution $\mathcal{L}$ over LIN such that for every $\ell \in \{1, \ldots, \hat{k}-1\}$ it holds that $\mathcal{L}$ is $(\ell, 2^{\ell/2}(\ell-1)\hat{\varepsilon})$-local and, for every subset $S \subseteq \{0,1\}^n$ of size at most ℓ and every event $E \subseteq \{0,1\}^S$, $\left|\Pr[\hat{\mathcal{F}}(S) \in E] - \widetilde{\Pr}[\mathcal{L}(S) \in E]\right| \leq (|S|-1) \cdot \|\widehat{\mathbf{1}_E}\|_1 \cdot \hat{\varepsilon} \leq (|S|-1) \cdot \sqrt{|E|} \cdot \hat{\varepsilon}$.*
4. *For every $\ell \in \{1, \ldots, \hat{k}-1\}$, there exists an ℓ-local quasi-distribution $\mathcal{L}'$ over LIN such that $\Delta_\ell(\hat{\mathcal{F}}, \mathcal{L}') \leq (2^\ell+1) \cdot 2^{\ell/2}(\ell-1)\hat{\varepsilon}$.*

We highlight some of the differences of Theorem 12 ($\varepsilon \geq 0$) from Theorem 11 ($\varepsilon = 0$).

- In Item 2, we now need to use the self-correction $\hat{\mathcal{F}}$ to ensure that $\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(x+y) = \hat{\mathcal{F}}(x)+\hat{\mathcal{F}}(y)]$ is large *for every* $x, y \in \{0,1\}^n$, as opposed to random $x, y \in \{0,1\}^n$. This is necessary because otherwise it is possible for $\Pr_{\mathcal{F}}[\mathcal{F}(x)+\mathcal{F}(y) = \mathcal{F}(x+y)]$ to be small for certain choices of x and y, and in this case a quasi-distribution supported only on linear functions has no hope of approximating $\mathcal{F}$ on sets containing $\{x, y, x+y\}$.
- In Item 3, we choose $\mathcal{L}$ to match $\hat{\mathcal{F}}$ exactly on all sets of size 1, as before. However, since the linearity condition only holds approximately, this means that we only get approximate matching on larger input sets, and this approximation deteriorates as the sets get larger.

- Since $\mathcal{L}$ only matches $\hat{\mathcal{F}}$ approximately, it is only an approximately ℓ-local distribution. Thus, we require the additional step of Item 4, where we correct $\mathcal{L}$ to an exactly ℓ-local distribution.

We now proceed to the proof of Theorem 12.

Proof that $1 \implies 2$. Fix $x, y \in \{0,1\}^n$. The definition of $\hat{\mathcal{F}}$ implies that

$$\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(x)+\hat{\mathcal{F}}(y) = \hat{\mathcal{F}}(x+y)] = \Pr_{\substack{w_x,w_y,w_{x+y}\\ \mathcal{F}}}[\mathcal{F}(x+w_x)+\mathcal{F}(w_x)+\mathcal{F}(y+w_y)+\mathcal{F}(w_y) = \mathcal{F}(x+y+w_{x+y})+\mathcal{F}(w_{x+y})] \ .$$

Define

$$\begin{aligned}
S_1 &:= \{x+w_x, y+w_y, x+y+w_{x+y}, w_x, w_y, w_{x+y}\} \ , \\
S_2 &:= \{x+w_x+w_y, y+w_y, x+y+w_{x+y}, w_x, w_{x+y}\} \ , \\
S_3 &:= \{x+w_x+w_y, y+w_y+w_{x+y}, x+y+w_{x+y}, w_x\} \ , \\
S_4 &:= \{x+w_x+w_y, y+w_y+w_{x+y}, x+y+w_{x+y}+w_x\} \ .
\end{aligned}$$

Observe that $|S_i \cup S_{i+1}| \leq 7 \leq k$. Letting $\mathsf{add}(\cdot)$ be the addition function, the linearity test passing with probability at least $1-\varepsilon$ implies that

$$\begin{aligned}
\Pr_{\substack{w_x,w_y,w_{x+y}\\ \mathcal{F}}}[\mathsf{add}(\mathcal{F}(S_1)) = \mathsf{add}(\mathcal{F}(S_2))] &= \Pr_{\substack{w_x,w_y\\ \mathcal{F}}}[\mathcal{F}(x+w_x+w_y) = \mathcal{F}(x+w_x)+\mathcal{F}(w_y)] \geq 1-\varepsilon \ , \\
\Pr_{\substack{w_x,w_y,w_{x+y}\\ \mathcal{F}}}[\mathsf{add}(\mathcal{F}(S_2)) = \mathsf{add}(\mathcal{F}(S_3))] &= \Pr_{\substack{w_y,w_{x+y}\\ \mathcal{F}}}[\mathcal{F}(y+w_y+w_{x+y}) = \mathcal{F}(y+w_y)+\mathcal{F}(w_{x+y})] \geq 1-\varepsilon \ , \\
\Pr_{\substack{w_x,w_y,w_{x+y}\\ \mathcal{F}}}[\mathsf{add}(\mathcal{F}(S_3)) = \mathsf{add}(\mathcal{F}(S_4))] &= \Pr_{\substack{w_x,w_{x+y}\\ \mathcal{F}}}[\mathcal{F}(x+y+w_{x+y}+w_x) = \mathcal{F}(x+y+w_{x+y})+\mathcal{F}(w_x)] \geq 1-\varepsilon \ , \\
\Pr_{\substack{w_x,w_y,w_{x+y}\\ \mathcal{F}}}[\mathsf{add}(\mathcal{F}(S_4)) = 0] &= \Pr_{\substack{w_x,w_y\\ w_{x+y}\\ \mathcal{F}}}[\mathcal{F}(x+w_x+w_y)+\mathcal{F}(y+w_y+w_{x+y}) = \mathcal{F}(x+y+w_{x+y}+w_x)] \geq 1-\varepsilon \ .
\end{aligned}$$

Therefore, by Lemma 6.4,

$$|\Pr[\mathsf{add}(\mathcal{F}(S_1)) = 0] - \Pr[\mathsf{add}(\mathcal{F}(S_4)) = 0]| \leq \sum_{i=1}^{3} |\Pr[\mathsf{add}(\mathcal{F}(S_i)) = 0] - \Pr[\mathsf{add}(\mathcal{F}(S_{i+1})) = 0]| \leq 3\varepsilon \ .$$

Since $\Pr[\mathsf{add}(\mathcal{F}(S_4)) = 0] \geq 1-\varepsilon$, it follows that $\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(x)+\hat{\mathcal{F}}(y) = \hat{\mathcal{F}}(x+y)] = \Pr[\mathsf{add}(\mathcal{F}(S_1)) = 0] \geq 1-4\varepsilon = 1-\hat{\varepsilon}$, as claimed. Finally, $\Pr[\hat{\mathcal{F}}(0^n) = 0] = \Pr_{w\in\{0,1\}^n}[\mathcal{F}(w+0^n)+\mathcal{F}(w) = 0] = 1$. $\square$

Proof that $2 \implies 3$. This proof generalizes the proof that $2 \implies 3$ in Theorem 11. We begin by arguing that $\hat{\mathcal{F}}$ behaves almost linearly on sets of size at most $\hat{k}-1$. Let $s \in \{2, \ldots, \hat{k}-1\}$, $x_1, \ldots, x_s \in \{0,1\}^n$, and $b \in \{0,1\}$, and define $S_i := \{\sum_{j=1}^{i} x_j, x_{i+1}, \ldots, x_s\}$ for every $i \in \{1, \ldots, s\}$. Note that $|S_i \cup S_{i+1}| = s-i+2 \leq s+1 \leq \hat{k}$. Letting $\mathsf{add}(\cdot)$ be the addition function, the fact that the linearity test passes with probability at least $1-\hat{\varepsilon}$ implies that

$$\Pr\left[\mathsf{add}(\hat{\mathcal{F}}(S_i)) = \mathsf{add}(\hat{\mathcal{F}}(S_{i+1}))\right] = \Pr\left[\hat{\mathcal{F}}\left(\sum_{j=1}^{i} x_j\right) + \hat{\mathcal{F}}(x_{i+1}) = \hat{\mathcal{F}}\left(\sum_{j=1}^{i+1} x_j\right)\right] \geq 1-\hat{\varepsilon} \ .$$

This implies that $\left|\Pr[\hat{\mathcal{F}}(\sum_{i=1}^{s} x_i) = b] - \Pr[\sum_{i=1}^{s} \hat{\mathcal{F}}(x_i) = b]\right| \leq (s-1)\hat{\varepsilon}$, via the following argument:

$$\begin{aligned}
\left|\Pr\left[\sum_{i=1}^{s} \hat{\mathcal{F}}(x_i) = b\right] - \Pr\left[\hat{\mathcal{F}}\left(\sum_{i=1}^{s} x_i\right) = b\right]\right| &= \left|\Pr[\mathsf{add}(\hat{\mathcal{F}}(S_1)) = b] - \Pr[\mathsf{add}(\hat{\mathcal{F}}(S_s)) = b]\right| \\
&= \left|\sum_{i=1}^{s-1} \Pr[\mathsf{add}(\hat{\mathcal{F}}(S_i)) = b] - \Pr[\mathsf{add}(\hat{\mathcal{F}}(S_{i+1})) = b]\right| \\
&\leq \sum_{i=1}^{s-1} \left|\Pr[\mathsf{add}(\hat{\mathcal{F}}(S_i)) = b] - \Pr[\mathsf{add}(\hat{\mathcal{F}}(S_{i+1})) = b]\right| \\
&\leq (s-1)\hat{\varepsilon} \ .
\end{aligned}$$

where the last inequality is by Lemma 6.4, since $|S_i \cup S_{i+1}| \leq \hat{k}$ for every i. Note that s must be strictly less than $\hat{k}$ because $|S_1 \cup S_2| = s + 1$.

We construct $\mathcal{L}$ as before. Define $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$ to be the solution to the system of equations in Lemma 5.3 where $c_\beta := \Pr[\hat{\mathcal{F}}(\beta) = 0]$ for each $\beta \in \{0,1\}^n$, and let $\mathcal{L}$ be the quasi-distribution over LIN that assigns weight ℓ_α to the linear function $\langle \alpha, \cdot \rangle$. Note that $\mathcal{L}$ is indeed a quasi-distribution, because $\sum_\alpha \ell_\alpha = \Pr[\hat{\mathcal{F}}(0^n) = 0] = 1$.

Moreover, by definition of $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$, for every $x \in \{0,1\}^n$ and $b \in \{0,1\}$ it holds that $\Pr[\hat{\mathcal{F}}(x) = b] = \widetilde{\Pr}[\mathcal{L}(x) = b]$. In other words, $\mathcal{F}$ and $\mathcal{L}$ match *exactly* on sets of size one. We now prove that $\mathcal{F}$ and $\mathcal{L}$ match *approximately* for sets of larger size (but still less than $\hat{k}$) with a guarantee that degrades with the set size.

Fix $s \in \{1, \ldots, k-1\}$, $S = \{x_1, \ldots, x_s\} \subseteq \{0,1\}^n$, and $E \subseteq \{0,1\}^S$. We use Lemma 5.1 to get real numbers $\{c_T\}_{T \subseteq [s]}$ that depend only on E such that

$$\begin{aligned}
&\left|\Pr[\hat{\mathcal{F}}(S) \in E] - \widetilde{\Pr}[\mathcal{L}(S) \in E]\right| \\
&= \left|\sum_{T \subseteq [s]} c_T \cdot \Pr\left[\sum_{i \in T} \hat{\mathcal{F}}(x_i) = 0\right] - \sum_{T \subseteq [s]} c_T \cdot \widetilde{\Pr}\left[\sum_{i \in T} \mathcal{L}(x_i) = 0\right]\right| \\
&= \left|\sum_{T \subseteq [s]} c_T \left(\Pr\left[\sum_{i \in T} \hat{\mathcal{F}}(x_i) = 0\right] - \widetilde{\Pr}\left[\sum_{i \in T} \mathcal{L}(x_i) = 0\right]\right)\right| \\
&= \left|\sum_{T \subseteq [s]} c_T \left(\Pr\left[\sum_{i \in T} \hat{\mathcal{F}}(x_i) = 0\right] - \widetilde{\Pr}\left[\mathcal{L}\left(\sum_{i \in T} x_i\right) = 0\right]\right)\right| \\
&= \left|\sum_{T \subseteq [s]} c_T \left(\Pr\left[\sum_{i \in T} \hat{\mathcal{F}}(x_i) = 0\right] - \Pr\left[\hat{\mathcal{F}}\left(\sum_{i \in T} x_i\right) = 0\right]\right)\right| \\
&\leq \sum_{T \subseteq [s]} |c_T| \left(|T| - 1\right) \hat{\varepsilon} \leq \hat{\varepsilon} \cdot (s-1) \cdot \sum_{T \subseteq [s]} |c_T| \\
&\leq \hat{\varepsilon} \cdot (s-1) \|\widehat{\mathbf{1}_E}\|_1 \leq \hat{\varepsilon} \cdot (s-1)\sqrt{|E|} \ .
\end{aligned}$$

Since $\hat{\mathcal{F}}$ defines probabilities in $[0,1]$, $\mathcal{L}$ is (ℓ, ε')-local with $\varepsilon' = (\ell - 1)2^{\ell/2}\hat{\varepsilon}$ for any $\ell < \hat{k}$. $\square$

Proof that 3 $\implies$ 4. Fix $\ell \in \{1, \ldots, \hat{k}-1\}$, and let $\mathcal{L}$ be the $(\ell, 2^{\ell/2}(\ell-1)\hat{\varepsilon})$-local quasi-distribution $\mathcal{L}$ over LIN such that for every subset $S \subseteq \{0,1\}^n$ of size at most ℓ and event $E \subseteq \{0,1\}^S$ it holds that

$$\left|\Pr[\hat{\mathcal{F}}(S) \in E] - \widetilde{\Pr}[\mathcal{L}(S) \in E]\right| \leq \sqrt{|E|}(|S|-1)\hat{\varepsilon} \leq 2^{\ell/2}(\ell-1)\hat{\varepsilon} \ .$$

Thus, $\Delta_\ell(\hat{\mathcal{F}}, \mathcal{L}) \leq 2^{\ell/2}(\ell-1)\hat{\varepsilon}$. By Corollary 7.9, there is an ℓ-local quasi-distribution $\mathcal{L}'$ such that $\Delta_\ell(\mathcal{L}, \mathcal{L}') \leq 2^\ell \cdot 2^{\ell/2}(\ell-1)\hat{\varepsilon}$. Therefore,

$$\Delta_\ell(\hat{\mathcal{F}}, \mathcal{L}') \leq \Delta_\ell(\hat{\mathcal{F}}, \mathcal{L}) + \Delta_\ell(\mathcal{L}, \mathcal{L}') \leq 2^{\ell/2}(\ell-1)\hat{\varepsilon} + 2^\ell \cdot 2^{\ell/2}(\ell-1)\hat{\varepsilon} = (2^\ell+1) \cdot 2^{\ell/2}(\ell-1)\hat{\varepsilon} \ . \quad \square$$

A Fourier spectrum of quasi-distributions over linear functions

We characterize the Fourier spectrum of quasi-distributions over linear functions. This characterization forms the intuition underlying our analysis of the linearity test (in Section 10 and Section 11), and implies that the only Fourier coefficients that matter are those corresponding to sets $T \subseteq \{0,1\}^n$ of size 1, since the values of all other coefficients are then determined.

Proposition A.1. *A quasi-distribution $\mathcal{Q}$ over functions $f\colon \{0,1\}^n \to \{0,1\}$ is supported on* LIN *if and only if $\widehat{q}(\{0^n\}) = \frac{1}{2^{2^n}}$ and $\widehat{q}(T) = \widehat{q}(\{\sum_{x\in T} x\})$ for every subset $T \subseteq \{0,1\}^n$. (We take the convention that if T is empty then $\sum_{x\in T} x := 0^n$.)*

Proof. We use a dimension argument. Letting $N := 2^n$, we define two subspaces of $\mathbb{R}^{2^N}$:

- $\mathcal{C}_1$ is the space of all quasi-distributions supported on LIN. Note that $\dim(\mathcal{C}_1) = N - 1$, because $\mathcal{C}_1$ is defined by the linear constraints (i) $\sum_{f\in U_{\{0,1\}^n}} q_f = 1$, and (ii) $q_f = 0$ for every $f \notin \mathsf{LIN}$.
- $\mathcal{C}_2$ is the space of all quasi-distributions $\mathcal{Q}$ such that $\widehat{q}(\emptyset) = \frac{1}{2^N}$ and $\widehat{q}(T) = \widehat{q}(\{\sum_{x\in T} x\})$ for every subset $T \subseteq \{0,1\}^n$. Observe that $\dim(\mathcal{C}_2) = N-1$ because $\mathcal{C}_2$ is defined by free coefficients $\widehat{q}(\{x\})$ for all $x \in \{0,1\}^n \setminus \{0^n\}$. The remaining coefficients are then completely determined: $\widehat{q}(\{0^n\}) = \widehat{q}(\emptyset) = \frac{1}{2^N}$, and $\widehat{q}(T) = \widehat{q}(\{\sum_{x\in T} x\})$ for every subset $T \subseteq \{0,1\}^n$ with $|T| \geq 2$.

Since since the two spaces have the same dimension, to show that they are equal, it suffices to show that one space is contained in the other. We show that $\mathcal{C}_1 \subseteq \mathcal{C}_2$.

Suppose that $\mathcal{Q} \in \mathcal{C}_1$ ($\mathcal{Q}$ is a quasi-distribution over LIN). Then $\widehat{q}(\emptyset) = \frac{1}{2^N}\sum_{f\in U_{\{0,1\}^n}} q(f) = \frac{1}{2^N}$, and for every subset $T \subseteq \{0,1\}^n$ it holds that

$$\begin{aligned}\widehat{q}(T) =& \frac{1}{2^N}\sum_{f\in U_{\{0,1\}^n}} q(f)(-1)^{\sum_{x\in T} f(x)} = \frac{1}{2^N}\sum_{f\in \mathsf{LIN}} q(f)(-1)^{\sum_{x\in T} f(x)} \\ =& \frac{1}{2^N}\sum_{f\in \mathsf{LIN}} q(f)(-1)^{f(\sum_{x\in T} x)} = \widehat{q}\left(\left\{\sum_{x\in T} x\right\}\right) \ ,\end{aligned}$$

which implies that $\mathcal{Q} \in \mathcal{C}_2$. We conclude that $\mathcal{C}_1 \subseteq \mathcal{C}_2$. □

B Necessity of quasi-distributions

In Section 1.3 we showed by way of example that quasi-distributions are necessary to describe non-signaling functions that pass the linearity test with probability 1. We elaborate on this necessity via two families of examples that cannot be described by distributions (over linear functions) alone.

Example 3 (generalization of Example 2 in Section 1.3)**.** For $n > k \geq 3$ and let $\varepsilon > 0$ be such that $\varepsilon < \frac{(1+\varepsilon)(2^{n-k}-1)}{(2^n-1)}$. Let $\mathcal{L} = (\ell_\alpha)_{\alpha \in \{0,1\}^n}$ be the quasi-distribution over linear functions defined as

$$\ell_\alpha := \begin{cases} \frac{1+\varepsilon}{2^n-1} & \text{if } \alpha \neq 0^n \\ -\varepsilon & \text{if } \alpha = 0^n \end{cases} ,$$

and let $\mathcal{F}$ be the non-signaling function induced by $\mathcal{L}$. Note that $\mathcal{F}$ is k-non-signaling: for every subset $S \subseteq \{0,1\}^n$ containing at most k linearly independent vectors and every $\vec{b} \in \{0,1\}^S$,

$$\Pr[\mathcal{F}(S) = \vec{b}] = \sum_{\alpha : \langle \alpha, x \rangle = b_x \ \forall x \in S} \ell_\alpha = \left\{ \begin{array}{ll} (2^{n-k}-1) \cdot \frac{1+\varepsilon}{2^n-1} - \varepsilon & \text{if } \vec{b} = 0^{|S|} \\ 2^{n-k} \cdot \frac{1+\varepsilon}{2^n-1} & \text{otherwise} \end{array} \right\} \geq 0 \ ,$$

where the last inequality (non-negativity) following from the assumption that ε is sufficiently small. Since $\mathcal{L}$ is a quasi-distribution over linear functions, $\mathcal{F}$ passes the linearity test with probability 1. But $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$ is the *unique* solution to the system of equations $\left\{ \sum_{\alpha : \langle \alpha, x \rangle = 0} \ell_\alpha = \Pr[\mathcal{F}(x) = 0] \right\}_{x \in \{0,1\}^n}$, and so we conclude that $\mathcal{F}$ *cannot* be described by any *distribution* over linear functions.

The sum of all negative probabilities in the foregoing example is $-\varepsilon \approx -2^{-k}$. Could it be that if a quasi-distribution $\mathcal{L}$ over linear functions describes a non-signaling function passing the linearity test with probability 1, then the sum of all its negative probabilities is small in absolute value? Below we answer this question negatively by showing an example where the absolute value of the sum is $1/2$ even for large k.

Example 4. Let n be an integer, and set $k := n - 2\log(n)$. Sample a uniformly random subset $R \subseteq \{0,1\}^n$ of size $|R| = 2^{n-1}$, let $\mathcal{L} = (\ell_\alpha)_{\alpha \in \{0,1\}^n}$ be the quasi-distribution over linear functions defined as

$$\ell_\alpha = \begin{cases} -1/2^n & \text{if } \alpha \in \mathbb{R} \\ 3/2^n & \text{if } \alpha \notin \mathbb{R} \end{cases} ,$$

and let $\mathcal{F}$ be the non-signaling function induced by $\mathcal{L}$. As before, since $(\ell_\alpha)_{\alpha \in \{0,1\}^n}$ is the unique solution to the system of equations $\left\{ \sum_{\alpha : \langle \alpha, x \rangle = 0} \ell_\alpha = \Pr[\mathcal{F}(x) = 0] \right\}_{x \in \{0,1\}^n}$, $\mathcal{L}$ is the only quasi-distribution over LIN that can describe $\mathcal{F}$. Note that $|\ell_\alpha| \leq 3/2^n$ for all α, and $\left| \sum_{\alpha : \ell_\alpha < 0} \ell_\alpha \right| = 1/2$.

We are left to argue that $\mathcal{F}$ is k-non-signaling with positive probability over the choice of R (i.e., we use the probabilistic method); in fact this will be true with high probability. It suffices to show that for every subspace $V \subseteq \{0,1\}^n$ of dimension $\dim(V) \geq n - k > 2\log(n)$ it holds that $\sum_{\vec{\alpha} \in V} \ell_\alpha > 0$. Indeed, for every subspace $V \subseteq \{0,1\}^n$ of $\dim(V) = 2\log(n)$, a Chernoff bound implies that $\Pr_R[\sum_{\vec{\alpha} \in V} \ell_\alpha < 0] < \exp(-\Omega(|V|)) = \exp(-\Omega(n^2))$. There are at most $2^{2n\log(n)}$ subspaces of dimension $2\log(n)$. Therefore, by taking a union bound over all of them, we deduce that with high probability $\sum_{\vec{\alpha} \in V} \ell_\alpha > 0$ holds for every subspace $V \subseteq \{0,1\}^n$ of dimension $\dim(V) \geq n - k > 2\log(n)$. We conclude that, for every subset $S \subseteq \{0,1\}^n$ with $|S| \leq k$ and every $\vec{b} \in \{0,1\}^S$ it holds that $\Pr[\mathcal{F}(S) = \vec{b}] = \sum_{\alpha : \langle \alpha, S \rangle = \vec{b}} \ell_\alpha \geq 0$ because the sum is over a subspace of dimension at least $n - |S| \geq n - k > 2\log(n)$.

C Almost non-signaling functions

The two definitions below relax the definition of non-signaling functions (Definition 6.1), by only requiring that the marginals on intersections are *statistically close* or *computationally close*. These relaxations arise, e.g., in cryptographic applications (see Section 4.3). In Lemma C.3 below we prove that every such *almost* non-signaling function can be well-approximated by an exact one.

Definition C.1 (statistical NS)**.** *A* (k,δ)**-non-signaling function** *over a finite domain D is a collection $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq D,|S|\leq k}$ where (i) each $\mathcal{F}_S$ is a distribution over functions $f\colon S \to \{0,1\}$, and (ii) for every two subsets S_1 and S_2 each of size at most k, the restrictions of $\mathcal{F}_{S_1}$ and $\mathcal{F}_{S_2}$ to $S_1 \cap S_2$ are δ-close in statistical distance. (If $S = \emptyset$ then $\mathcal{F}_S$ always outputs the empty string.)*

Definition C.2 (computational NS)**.** *A* (k,δ,T)**-non-signaling function** *over a finite domain D is a collection $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq D,|S|\leq k}$ where (i) each $\mathcal{F}_S$ is a distribution over functions $f\colon S \to \{0,1\}$, and (ii) for every two subsets S_1 and S_2 each of size at most k and for every probabilistic T-time distinguisher $\mathcal{A}$,*

$$\left| \Pr_{f\leftarrow\mathcal{F}_{S_1}|_{S_1\cap S_2}}[\mathcal{A}(f)=1] - \Pr_{f\leftarrow\mathcal{F}_{S_2}|_{S_1\cap S_2}}[\mathcal{A}(f)=1] \right| \leq \delta \ ,$$

i.e., no procedure running in time at most T can distinguish between restrictions of $\mathcal{F}_{S_1}$ and $\mathcal{F}_{S_2}$ to $S_1 \cap S_2$ with probability more than δ. (If $S = \emptyset$ then $\mathcal{F}_S$ always outputs the empty string.)

Note that every (exactly) k-non-signaling function is $(k,0)$-non-signaling, and that every (k,δ)-non-signaling function is (k,δ,∞)-non-signaling.

The lemma below shows that every (k,δ)-non-signaling function, in fact even every (k,δ,T)-non-signaling function, is close to a $(k,0)$-non-signaling function, for δ is sufficiently small. This lemma directly implies straightforward extensions of our results to the almost non-signaling case.

Lemma C.3. *Let $T \geq O(k)$. Then for every (k,δ,T)-non-signaling function $\mathcal{F}$, there exists a $(k,0)$-non-signaling function $\mathcal{F}'$ such that $\Delta_k(\mathcal{F},\mathcal{F}') \leq 2^k\delta + 2^{2k}\delta$.*

The above immediately extends to statistically non-signaling functions by setting $T = \infty$.

Proof. We begin by showing that for any two sets R and S with $R \subseteq S \subseteq D$ and $|R| \leq |S| \leq k$, and any bit $b \in \{0,1\}$ it holds that

$$\left| \Pr_{f\leftarrow\mathcal{F}_R}\left[\sum_{x\in R} f(x) = b\right] - \Pr_{f\leftarrow\mathcal{F}_S}\left[\sum_{x\in R} f(x) = b\right] \right| \leq \delta \ . \tag{2}$$

Indeed, let R and S be such sets, and fix any bit b. Let $\mathcal{A}$ be the distinguisher that given an input $f\colon R \to \{0,1\}$ or $f\colon S \to \{0,1\}$ outputs $\sum_{x\in R} f(x)$. Note that $\mathcal{A}$ runs in time $O(|R|)$, which is upper bounded by $O(k) \leq T$. Observe that

$$\left| \Pr_{f\leftarrow\mathcal{F}_R}\left[\sum_{x\in R} f(x) = 1\right] - \Pr_{f\leftarrow\mathcal{F}_S}\left[\sum_{x\in R} f(x) = 1\right] \right| = \left| \Pr_{f\leftarrow\mathcal{F}_R}[\mathcal{A}(f)=1] - \Pr_{f\leftarrow\mathcal{F}_S|_R}[\mathcal{A}(f)=1] \right| \leq \delta \ ,$$

as claimed. We note that the above inequality also implies that

$$\left| \Pr_{f\leftarrow\mathcal{F}_R}\left[\sum_{x\in R} f(x) = 0\right] - \Pr_{f\leftarrow\mathcal{F}_S}\left[\sum_{x\in R} f(x) = 0\right] \right| \leq \delta \ ,$$

which completes the proof of Eq. (2).

We now construct $\mathcal{F}'$ by first defining a quasi-distribution $\mathcal{Q}$ and then using $\mathcal{Q}$ to define $\mathcal{F}'$. We define $\mathcal{Q}$ via its Fourier coefficients, by letting

$$\widehat{q}(S) := \frac{1}{2^{2^n}} \cdot \left(2 \Pr_{f \leftarrow \mathcal{F}_S} \left[\sum_{x \in S} f(x) = 0 \right] - 1 \right)$$

for all $S \subseteq D$ with $|S| \leq k$, and letting $\widehat{q}(S)$ be arbitrary for all $S \subseteq D$ with $|S| > k$. By Lemma 5.1, for every set $S \subseteq D$ with $|S| \leq k$ we have that

$$\begin{aligned}
&\sum_{b \in \{0,1\}^S} \left| \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] - \Pr_{f \leftarrow \mathcal{F}_S}[f(S) = \vec{b}] \right| \\
&\leq \sum_{b \in \{0,1\}^S} \frac{1}{2^{s-1}} \sum_{R \subseteq S} \left| \widetilde{\Pr} \left[\sum_{x \in R} \mathcal{Q}(x) = \sum_{x \in R} b_x \right] - \Pr_{f \leftarrow \mathcal{F}_S} \left[\sum_{x \in R} f(x) = \sum_{x \in R} b_x \right] \right| \\
&= \sum_{b \in \{0,1\}^S} \frac{1}{2^{s-1}} \sum_{R \subseteq S} \left| \Pr_{g \leftarrow \mathcal{F}_R} \left[\sum_{x \in R} g(x) = \sum_{x \in R} b_x \right] - \Pr_{f \leftarrow \mathcal{F}_S} \left[\sum_{x \in R} f(x) = \sum_{x \in R} b_x \right] \right| \\
&= \frac{1}{2^{s-1}} \sum_{R \subseteq S} \sum_{b \in \{0,1\}^S} \left| \Pr_{g \leftarrow \mathcal{F}_R} \left[\sum_{x \in R} g(x) = \sum_{x \in R} b_x \right] - \Pr_{f \leftarrow \mathcal{F}_S} \left[\sum_{x \in R} f(x) = \sum_{x \in R} b_x \right] \right| \\
&\leq \frac{1}{2^{s-1}} \sum_{R \subseteq S} \sum_{b \in \{0,1\}^S} \delta = \frac{1}{2^{s-1}} \cdot 2^s \cdot 2^s \cdot \delta = 2^{s+1} \delta \leq 2^{k+1} \delta \ ,
\end{aligned}$$

where the first inequality in the last line is by Eq. (2). Therefore,

$$\Delta_k(\mathcal{Q}, \mathcal{F}) = \max_{S \subseteq D, |S| \leq k} \frac{1}{2} \sum_{b \in \{0,1\}^S} \left| \widetilde{\Pr}[\mathcal{Q}(S) = \vec{b}] - \Pr_{f \leftarrow \mathcal{F}_S}[f(S) = \vec{b}] \right| \leq 2^k \delta \ ,$$

which, in particular, implies that $\mathcal{Q}$ is $(k, 2^k\delta)$-local (recall Definition 7.7). By Corollary 7.9, there exists a k-non-signaling function $\mathcal{F}'$ such that $\Delta_k(\mathcal{Q}, \mathcal{F}') < 2^k(2^k\delta) = 2^{2k}\delta$, and hence $\Delta_k(\mathcal{F}, \mathcal{F}') \leq 2^k\delta + 2^{2k}\delta$, as required. □

D Non-signaling players

In this paper we take the functional view of non-signaling strategies (Definition 6.1), which generalizes the notion of a function $f\colon D \to \{0,1\}$ to a non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S\subseteq D,|S|\leq k}$ that answers up to k queries in D. This view is natural in the setting of Property Testing.

In this section we discuss the other view of non-signaling strategies, which generalizes the notion of non-communicating players to non-signaling players.

Definition D.1 (non-signaling players)**.** *A* k**-non-signaling (boolean) player** *over finite domains* $(D_1,\ldots,D_k)$ *is a collection* $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_1\in D_1,\ldots,x_k\in D_k}$ *where (i) each* $\mathcal{P}_{(x_1,\ldots,x_k)}$ *is a distribution over functions* $f\colon [k]\to\{0,1\}$*, and (ii) for every two vectors* $(x_1,\ldots,x_k)$ *and* $(y_1,\ldots,y_k)$ *that agree on a subset* $I\subseteq[k]$ *of entries, the restrictions of* $\mathcal{P}_{(x_1,\ldots,x_k)}$ *and* $\mathcal{P}_{(y_1,\ldots,y_k)}$ *to answers in* I *are equal as distributions.*

Remark D.2 (comparison with non-communicating players)**.** The case of k non-communicating players corresponds to strengthening the second item in the definition to the following one: there exist functions $p_1,\ldots,p_k$ and a positive integer t such that $\mathcal{P}_{(x_1,\ldots,x_k)}$ is equal to the distribution $(p_1(x_1,\rho),\ldots,p_k(x_k,\rho))$ for a random $\rho\in\{0,1\}^t$.

Remark D.3 (players vs. functions)**.** Non-signaling functions (Definition 6.1) and non-signaling players (Definition D.1) are incomparable. Informally, the former imposes restrictions to multiple queries to the same 'slot' while the latter imposes restrictions to single queries across multiple 'slots'; in fact, the two notions can be viewed as extremal settings of one definition that considers both restriction types. That said, the two notions of non-signaling can be related in useful ways.[3]

Given a vector of queries $\vec{x} = (x_1,\ldots,x_k)\in D_1\times\cdots\times D_k$ and a vector of answers $\vec{b} = (b_1,\ldots,b_k)\in\{0,1\}^k$, we define

$$\Pr[\mathcal{P}(\vec{x}) = \vec{b}] := \Pr_{f\leftarrow\mathcal{P}_{(x_1,\ldots,x_k)}}[f(1) = b_1,\cdots,f(k) = b_k]\ ,$$

which is the probability that the i-th player answers query x_i with b_i for every $i\in[k]$.

For a subset of players $I\subseteq[k]$, we write $\Pr[\mathcal{P}_i(x_i) = b_i\ \forall i\in I]$ to refer to the probability that the i-th player answers query x_i with b_i for every $i\in I$. (Note that by the non-signaling property, we do not have to specify the queries to the players outside I.)

We prove the following results for non-signaling players.

- **Linearity testing against non-signaling players** (Appendix E).

  We describe how to make a black-box use of our results about linearity testing against non-signaling functions to prove corresponding results non-signaling players.

- **Non-signaling players, quasi-distributions, and Fourier analysis** (Appendix F)

  We describe how to use Fourier analysis to prove a strong equivalence between non-signaling players and quasi-distributions over *tuples* of functions. This strengthens the equivalence proved in [AB11; AS13] by *explicitly describing all quasi-distributions* that describe a given non-signaling player. We also characterize the Fourier spectrum of notable classes of these quasi-distributions, and establish connections to the quasi-distributions arising from non-signaling functions.

[3] E.g., if a language has a PCP with soundness error ε against k-non-signaling functions then it also has an MIP with soundness error ε against k-non-signaling players [KRR14, Sec. 12], and vice versa. These two types of proof systems are known as *non-signaling PCPs* [KRR14, Sec. 4.5] and *non-signaling MIPs* (see, e.g., [KRR14, Sec. 4.3]).

E Linearity testing against non-signaling players

In this section we study linearity testing against non-signaling players. Specifically, we characterize the set of non-signaling players that pass the linearity test with probability 1 (Appendix E.1) and also those that pass the linearity test with high probability (Appendix E.2).

Recall that, given a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$, the linearity test works as follows: (i) sample $x, y \in \{0,1\}^n$ and distinct $i_1, i_2, i_3 \in [k]$ uniformly at random; (ii) send $x, y, x+y$ to players $\mathcal{P}_{i_1}, \mathcal{P}_{i_2}, \mathcal{P}_{i_3}$ to obtain answers b_1, b_2, b_3 respectively; (iii) accept if $b_{i_1} + b_{i_2} = b_{i_3}$.

Below we introduce two notions and a lemma that will be used in both analyses. The first notion considers players whose answers to queries depend only on the set of queries but not the identities of the players answering them. The second notion considers players that always give the same answer to the same query regardless of the identity of the player that answers it. The lemma relates these notions to non-signaling *functions*; this connection will enable us to leverage, in a black-box way, our results on linearity testing against non-signaling functions.

Definition E.1. *A k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ is* **ℓ-symmetric** *if, for every subset $I \subseteq [k]$ with $|I| = \ell$, permutation $\pi \colon I \to I$, inputs $\vec{x} = (x_i)_{i \in I}$ with $x_i \in \{0,1\}^n$, and answers $\vec{b} = (b_i)_{i \in I}$ with $b_i \in \{0,1\}$, it holds that $\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{P}(\pi(\vec{x})) = \pi(\vec{b})]$. If $\ell = k$, then we simply say that $\mathcal{P}$ is* **symmetric**.

Definition E.2. *A k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ is* **consistent** *if, for every $i, j \in [k]$ and $x \in \{0,1\}^n$, it holds that $\Pr[\mathcal{P}_i(x) = \mathcal{P}_j(x)] = 1$.*

Proposition E.3. *If a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ is consistent, then, for every $x \in \{0,1\}^n$, it holds that $\Pr[\mathcal{P}_1(x) = \mathcal{P}_2(x) = \ldots \mathcal{P}_k(x)] = 1$.*

Proof. We prove that $\Pr[\mathcal{P}_1(x) = \mathcal{P}_2(x) = \cdots = \mathcal{P}_i(x)]$ for all $i \in \{2, \ldots, k\}$ by induction on i. For $i = 2$, $\Pr[\mathcal{P}_1(x) = \mathcal{P}_2(x)] = 1$ holds by Definition E.2. For $i > 2$, we have

$$\begin{aligned} &\Pr[\mathcal{P}_1(x) = \mathcal{P}_2(x) = \cdots = \mathcal{P}_i(x)] \\ =\, &\Pr[\mathcal{P}_{i-1}(x) = \mathcal{P}_i(x)] \cdot \Pr[\mathcal{P}_1(x) = \mathcal{P}_2(x) = \cdots = \mathcal{P}_{i-1}(x) \,|\, \mathcal{P}_{i-1}(x) = \mathcal{P}_i(x)] \ . \end{aligned}$$

The left term above equals 1 by Definition E.2, while the second term above equals 1 by the induction hypothesis. Thus the product of the two also equals 1, completing the proof. □

Lemma E.4. *For every k-non-signaling symmetric players $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ there exists a k-non-signaling function $\mathcal{F} = (\mathcal{F}_S)_{S \subseteq \{0,1\}^n, |S| \leq k}$ that matches $\mathcal{P}$ on distinct queries ($\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{F}(\vec{x}) = \vec{b}]$ for all inputs $\vec{x}$ with no repeated entries and answers $\vec{b}$). Moreover, if $\mathcal{P}$ is consistent then $\mathcal{F}$ matches $\mathcal{P}$ on all queries ($\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{F}(\vec{x}) = \vec{b}]$ for all inputs $\vec{x}$ and answers $\vec{b}$).*

Proof. Given k-non-signaling symmetric players $\mathcal{P}$, define a k-non-signaling function $\mathcal{F}$ as follows: for every $S = (x_1, \ldots, x_k) \in (\{0,1\}^n)^k$ and every $\vec{b} \in \{0,1\}^S$

$$\Pr[\mathcal{F}(S) = \vec{b}] := \Pr[\mathcal{P}(x_1) = b_1, \ldots, \mathcal{P}(x_k) = b_k] \ .$$

Note that by symmetry of $\mathcal{P}$ the foregoing definition indeed defines a k-non-signaling function. By definition of $\mathcal{F}$ (and by symmetry of $\mathcal{P}$) it follows that, for all inputs $\vec{x} \in (\{0,1\}^n)^k$ with no repeated entries and all answers $\vec{b} \in \{0,1\}^k$, $\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{F}(\vec{x}) = \vec{b}]$.

Moreover, if $\mathcal{P}$ is consistent then, by Proposition E.3, we know that if $x_i = x_j$ for distinct $i, j \in [k]$ then $\mathcal{F}(\vec{x})$ is supported only vectors $\vec{b}$ with $b_i = b_j$ (i.e., for $b_i \neq b_j$ the probability that $\mathcal{F}(\vec{x}) = \vec{b}$ is equal to zero). Therefore, given a vector $\vec{x} = (x_1, \ldots, x_k) \in (\{0,1\}^n)^k$, we can let $\vec{x}'$ be the restriction of $\vec{x}$ that contains all distinct x_i and let b' be the corresponding restriction of $\vec{b}$; then $\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{P}(\vec{x}') = \vec{b}'] = \Pr[\mathcal{F}(\vec{x}') = \vec{b}']$, as required. □

E.1 Exact characterization

We characterize the set of k-non-signaling players that pass the linearity test with probability 1.

Theorem 13 (exact characterization for non-signaling players)**.** *Let $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ be a k-non-signaling player, with $k \geq 5$. The following statements are equivalent.*

1. *The linearity test always accepts: $\Pr_{\substack{x,y \leftarrow \{0,1\}^n \\ i_1,i_2,i_3 \leftarrow [k] \\ \mathcal{P}}}[\mathcal{P}_{i_1}(x) + \mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)] = 1$.*
2. *There exists a quasi-distribution $\mathcal{L}$ over linear functions that matches $\mathcal{P}$ on every $k-2$ players. That is, $\mathcal{L}$ is such that $\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \widetilde{\Pr}[\mathcal{L}(\vec{x}) = \vec{b}]$ for every subset $I \subseteq [k]$ with $|I| \leq k-2$, inputs $\vec{x} = (x_i)_{i \in I}$, and answers $\vec{b} = (b_i)_{i \in I}$.*

We first prove two lemmas (Lemma E.5 and Lemma E.6 below) and then prove the theorem.

Lemma E.5. *Let $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ be a k-non-signaling player, with $k \geq 4$. If $\mathcal{P}$ passes the linearity test with probability 1, then the following holds.*

1. *For every $i \in [k]$, $\Pr[\mathcal{P}_i(0^n) = 0] = 1$.*
2. *$\mathcal{P}$ is consistent.*
3. *$\mathcal{P}$ is $(k-1)$-symmetric.*

Proof. Fix distinct $i_1, i_2, i_3, i_4 \in [k]$ (this is possible because $k \geq 4$). Let E_j be the event that $\sum_{\ell \in \{1,2,3,4\} \setminus \{j\}} \mathcal{P}_{i_\ell}(0^n) = 0$. Note that $\Pr[E_j] = 1$ for every $j \in [4]$ because $\mathcal{P}$ passes the linearity test with probability 1. Therefore, $\Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] = 1$. This implies that

$$\Pr[\mathcal{P}_{i_1}(0^n) = 0] \geq \Pr[\mathcal{P}_{i_j}(0^n) = 0 \ \forall j \in [4]] = \Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] = 1 \ ,$$

thus proving Item 1.

For Item 2, let $i, i' \in [k]$ and $j \in [k] \setminus \{i, i'\}$ be arbitrary. Then,

$$\Pr[\mathcal{P}_i(x) = \mathcal{P}_{i'}(x)] \geq \Pr[\mathcal{P}_i(x) + \mathcal{P}_{i'}(x) = \mathcal{P}_j(0^n) \ \wedge \ \mathcal{P}_j(0^n) = 0] \ .$$

By Item 1, we conclude that $\Pr[\mathcal{P}_i(x) = \mathcal{P}_{i'}(x)] \geq 1$, as required.

For Item 3, let $I \subseteq [k]$ with $|I| = k-1$ be arbitrary and let $\pi \colon I \to I$ be a permutation. Note that it suffices to prove the statement for π that is a transposition (i.e., π only swaps some $i_1, i_2 \in I$) because any permutation can be obtained by composing transpositions. Let $j \in [k] \setminus I$ be arbitrary, and fix inputs $\vec{x} = (x_i)_{i \in I}$ and answers $\vec{b} = (b_i)_{i \in I}$. Let E be the event that $\mathcal{P}_i(x_i) = b_i$ for all $i \in I \setminus \{i_1\}$. By Item 3, we have

$$\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr[\mathcal{P}_{i_1}(x_{i_1}) = b_{i_1} \wedge E]$$

$$= \Pr[\mathcal{P}_{i_1}(x_{i_1}) = b_{i_1} \wedge \mathcal{P}_j(x_{i_1}) = \mathcal{P}_{i_1}(x_{i_1}) \wedge E]$$
$$= \Pr[\mathcal{P}_j(x_{i_1}) = b_{i_1} \wedge E] \ .$$

Let E' be the event that $\mathcal{P}_i(x_i) = b_i$ for all $i \in I \setminus \{i_1, i_2\}$. Repeating the above argument (first move x_{i_2} from $\mathcal{P}_{i_2}$ to $\mathcal{P}_{i_1}$, and then move x_{i_1} from $\mathcal{P}_j$ to $\mathcal{P}_{i_2}$) we get that

$$\begin{aligned}\Pr[\mathcal{P}_j(x_{i_1}) = b_{i_1} \wedge E] &= \Pr[\mathcal{P}_j(x_{i_1}) = b_{i_1} \wedge \mathcal{P}_{i_2}(x_{i_2}) = b_{i_2} \wedge E'] \\ &= \Pr[\mathcal{P}_j(x_{i_1}) = b_{i_1} \wedge \mathcal{P}_{i_1}(x_{i_2}) = b_{i_2} \wedge E'] \\ &= \Pr[\mathcal{P}_{i_2}(x_{i_1}) = b_{i_1} \wedge \mathcal{P}_{i_1}(x_{i_2}) = b_{i_2} \wedge E'] \\ &= \Pr[\mathcal{P}(\pi(\vec{x})) = \pi(\vec{b})] \ ,\end{aligned}$$

which completes the proof of the lemma. □

Lemma E.6. *Let $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in \{0,1\}^n}$ be a k-non-signaling symmetric player with $k \geq 4$. Suppose that $\mathcal{P}$ passes the linearity test with probability 1. Then there exists a $(k-1)$-local quasi-distribution $\mathcal{L}$ over linear functions that matches $\mathcal{P}$ on every $k-1$ players (i.e., $\Pr[\mathcal{P}(\vec{x}) = \vec{b}] = \widetilde{\Pr}[\mathcal{L}(\vec{x}) = \vec{b}]$ for every subset $I \subseteq [k]$ with $|I| \leq k-1$, inputs $\vec{x} = (x_i)_{i \in I}$, and answers $\vec{b} = (b_i)_{i \in I}$).*

Proof. By Item 2 of Lemma E.5, $\mathcal{P}$ is consistent and thus, by Lemma E.4, there exists a k-non-signaling function $\mathcal{F} = \{\mathcal{F}_S\}_{S \subseteq \{0,1\}^n, |S| \leq k}$ that matches $\mathcal{P}$ on all queries ($\Pr_{\mathcal{P}}[\mathcal{P}(\vec{x}) = \vec{b}] = \Pr_{\mathcal{F}}[\mathcal{F}(\vec{x}) = \vec{b}]$ for all inputs $\vec{x}$ and answers $\vec{b}$ with at most k entries).

In particular, for all $x, y \in \{0,1\}^n$ (even with $x = y$) it holds that

$$\Pr_{\mathcal{F}}[\mathcal{F}(x) + \mathcal{F}(y) = \mathcal{F}(x+y)] = \Pr_{\mathcal{P}}[\mathcal{P}_1(x) + \mathcal{P}_2(y) = \mathcal{P}_3(x+y)] \ .$$

This tells us that, since $\mathcal{P}$ always passes the linearity test (for non-signaling players), $\mathcal{F}$ also always passes the linearity test (for non-signaling functions) and thus, by Theorem 11, there exists a $(k-1)$-local quasi-distribution $\mathcal{L}$ over linear functions that matches $\mathcal{F}$ on all sets of at most $k-1$ queries.

Therefore, for all $\vec{x} = (x_1, \ldots, x_{k-1}) \in (\{0,1\}^n)^{k-1}$ and $\vec{b} = (b_1, \ldots, b_{k-1}) \in \{0,1\}^{k-1}$ we have

$$\Pr_{\mathcal{P}}[\mathcal{P}_i(x_i) = b_i \ \forall i \in [k-1]] = \Pr_{\mathcal{F}}[\mathcal{F}(x_i) = b_i \ \forall i \in [k-1]] = \widetilde{\Pr}[\mathcal{L}(x_i) = b_i \ \forall i \in [k-1]] \ .$$

Therefore, $\mathcal{L}$ matches the first $k-1$ players. In order to show that $\mathcal{L}$ matches any $k-1$ players, note that the symmetry of $\mathcal{P}$ implies that for every subset $I = \{i_1, \ldots, i_{k-1}\}$ of the players, inputs $\vec{x} = (x_{i_1}, \ldots, x_{i_{k-1}})$, and answers $\vec{b} = (b_1, \ldots, b_{k-1})$, it holds that

$$\Pr[\mathcal{P}_{i_1}(x_1) = b_1, \ldots, \mathcal{P}_{i_{k-1}}(x_{k-1}) = b_{k-1}] = \Pr[\mathcal{P}_1(x_1) = b_1, \ldots, \mathcal{P}_{k-1}(x_{k-1}) = b_{k-1}] \ ,$$

which is equal to $\widetilde{\Pr}[\mathcal{L}(x_i) = b_i \ \forall i \in [k-1]]$, as required. □

Proof of Theorem 13. One can easily verify that if $\mathcal{P}$ matches a quasi-distribution $\mathcal{L}$ over linear functions on all $k-2 \geq 3$ players then $\Pr[\mathcal{P}_{i_1}(x) + \mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)] = 1$ for every $x, y \in \{0,1\}^n$ and distinct $i_1, i_2, i_3 \in [k]$ (i.e., $\mathcal{P}$ passes the linearity test with probability 1).

For the converse direction, suppose that $\mathcal{P}$ passes the linearity test with probability 1. By Lemma E.5, $\mathcal{P}$ is $(k-1)$-symmetric (i.e., for every subset $I \subseteq [k]$ with $|I| = k-1$ the players

$(\mathcal{P}_i)_{i\in I}$ are symmetric). By Lemma E.6, there exists a $(k-2)$-local quasi-distribution $\mathcal{L}_I$ over linear functions that matches $(\mathcal{P}_i)_{i\in I}$ on every $k-2$ players.

We are left to show that the $\mathcal{L}_I$'s are all equal. Indeed, fix $I = (i_1, \ldots, i_{k-1})$ and $I' = (i'_1, \ldots, i'_{k-1})$, and let $j \in I \cap I'$. For any query $x \in \{0,1\}^n$ to the player $\mathcal{P}_j$ and any answer $b \in \{0,1\}$ it holds that

$$\widetilde{\Pr}[\mathcal{L}_I(x) = b] = \Pr[\mathcal{P}_j(x) = b] = \widetilde{\Pr}[\mathcal{L}_{I'}(x) = b] \ .$$

By Proposition A.1, any two quasi-distributions over linear functions that agree on every single-query events are equal, and hence $\mathcal{L}_I = \mathcal{L}_{I'}$ for any two subsets $I, I' \subseteq [k]$. Therefore, there is one quasi-distribution $\mathcal{L}$ that matches every subset of $k-2$ players, as required. □

E.2 Robust characterization

We characterize the set of k-non-signaling players that pass the linearity test with high probability. The result involves the notion of self-correction, analogously to the case of non-signaling functions (see Section 11). Given a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i\in\{0,1\}^n}$, the self-correction of $\mathcal{P}$ is the $\hat{k}$-non-signaling player $\hat{\mathcal{P}} = (\hat{\mathcal{P}}_{(x_1,\ldots,x_{\hat{k}})})_{x_i\in\{0,1\}^n}$ (for $\hat{k} := \lfloor k/2 \rfloor$) that, given a query $(x_1, \ldots, x_{\hat{k}}) \in \{0,1\}^{\hat{k}\times n}$, samples $w_1, \ldots, w_{\hat{k}} \in \{0,1\}^n$ and a permutation $\pi\colon [k] \to [k]$ uniformly at random, and answers each x_i with $\mathcal{P}_{\pi(i)}(x_i + w_i) + \mathcal{P}_{\pi(2i)}(w_i)$. Formally, the self-correction is defined as follows.

Definition E.7. *The* **self-correction** *of a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i\in\{0,1\}^n}$ is the $\hat{k}$-non-signaling player $\hat{\mathcal{P}} = (\hat{\mathcal{P}}_{(x_1,\ldots,x_{\hat{k}})})_{x_i\in\{0,1\}^n}$ (with $\hat{k} := \lfloor k/2 \rfloor$) defined as follows: for inputs $\vec{x} = (x_1, \ldots, x_{\hat{k}}) \in (\{0,1\}^n)^{\hat{k}}$ and answers $\vec{b} = (b_1, \ldots, b_{\hat{k}}) \in \{0,1\}^{\hat{k}}$,*

$$\Pr[\hat{\mathcal{P}}(\vec{x}) = \vec{b}] := \Pr_{\substack{w_1,\ldots,w_{\hat{k}}\in\{0,1\}^n \\ \pi\colon [k]\to[k] \\ \mathcal{P}}} \left[\begin{array}{l} \mathcal{P}_{\pi(1)}(x_1 + w_1) + \mathcal{P}_{\pi(2)}(w_1) = b_1 \\ \quad \vdots \\ \mathcal{P}_{\pi(2\hat{k}-1)}(x_{\hat{k}} + w_{\hat{k}}) + \mathcal{P}_{\pi(2\hat{k})}(w_{\hat{k}}) = b_{\hat{k}} \end{array} \right] .$$

Note that the self-correction $\hat{\mathcal{P}}$ is symmetric.

Theorem 14 (robust characterization for non-signaling players)**.** *Let $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i\in\{0,1\}^n}$ be the k-non-signaling player for $k \geq 9$. Suppose that for some $\varepsilon > 0$ it holds that*

$$\Pr_{\substack{x,y\leftarrow\{0,1\}^n \\ i_1,i_2,i_3\leftarrow[k] \\ \mathcal{P}}} [\mathcal{P}_{i_1}(x) + \mathcal{P}_{i_2}(y) = \mathcal{P}_{i_3}(x+y)] > 1 - \varepsilon \ .$$

There exists a $(\hat{k}-1)$-local quasi-distribution $\mathcal{L}$ over linear functions that is $\hat{\varepsilon}$-close $\hat{\mathcal{P}}$ on every $\hat{k}-1$ players, for $\hat{\varepsilon} := 2^{O(\hat{k})} \cdot \varepsilon$. That is, $\left|\Pr[\mathcal{P}(\vec{x}) \in E] - \widetilde{\Pr}[\mathcal{L}(\vec{x}) \in E]\right| < \hat{\varepsilon}$ for all subsets $I \subseteq [\hat{k}]$ with $|I| \leq \hat{k}-1$, inputs $\vec{x} = (x_i)_{i\in I}$, and events $E \subseteq \{0,1\}^I$.

Proof. We first argue that, for every $x, y \in \{0,1\}^n$, $\Pr_{\mathcal{P}}[\hat{\mathcal{P}}_1(x) + \hat{\mathcal{P}}_2(y) = \hat{\mathcal{P}}_3(x+y)] > 1 - 4\varepsilon$. (This average-case-to-worst-case step, which uses the self-correction property of linear functions, is analogous to Item 2 of Theorem 12.) We define several events:

- E_1 is the event that $\mathcal{P}_{\pi(1)}(x+w_x)+\mathcal{P}_{\pi(4)}(w_y)=\mathcal{P}_{\pi(7)}(x+w_x+w_y)$;
- E_2 is the event that $\mathcal{P}_{\pi(2)}(w_x)+\mathcal{P}_{\pi(4)}(x+y+w_{x+y})=\mathcal{P}_{\pi(8)}(x+y+w_x+w_{x+y})$;
- E_3 is the event that $\mathcal{P}_{\pi(2)}(w_{x+y})+\mathcal{P}_{\pi(4)}(y+w_y)=\mathcal{P}_{\pi(9)}(y+w_y+w_{x+y})$;
- E_4 is the event that $\mathcal{P}_{\pi(7)}(x+w_x+w_y)+\mathcal{P}_{\pi(8)}(x+y+w_x+w_{x+y})=\mathcal{P}_{\pi(9)}(y+w_y+w_{x+y})$.

Since w_x, w_y, w_{x+y} are uniform in $\{0,1\}^n$, $\Pr[E_i]\geq 1-\varepsilon$ for $i=1,2,3,4$. By definition of $\hat{\mathcal{P}}$,

$$\begin{aligned}
&\Pr_{\hat{\mathcal{P}}}[\hat{\mathcal{P}}_1(x)+\hat{\mathcal{P}}_2(y)=\hat{\mathcal{P}}_3(x+y)]\\
=&\Pr_{\substack{w_x,w_y,w_{x+y}\\ \pi\colon [k]\to[k]\\ \mathcal{P}}}[\mathcal{P}_{\pi(1)}(x+w_x)+\mathcal{P}_{\pi(2)}(w_x)+\mathcal{P}_{\pi(3)}(y+w_y)+\mathcal{P}_{\pi(4)}(w_y)=\mathcal{P}_{\pi(5)}(x+y+w_{x+y})+\mathcal{P}_{\pi(6)}(w_{x+y})]\\
\geq&\Pr_{\substack{w_x,w_y,w_{x+y}\\ \pi\colon [k]\to[k]\\ \mathcal{P}}}[E_1\wedge E_2\wedge E_3\wedge E_4]\\
\geq&1-4\varepsilon\ ,
\end{aligned}$$

as claimed.

Next, by applying Lemma E.4 to the $\hat{k}$-non-signaling symmetric player $\hat{\mathcal{P}}$, we get a $\hat{k}$-non-signaling function $\hat{\mathcal{F}}=\{\hat{\mathcal{F}}_S\}_{S\subseteq\{0,1\}^n,|S|\leq\hat{k}}$ that matches $\hat{\mathcal{P}}$ on inputs with no repeated entries. That is, for every $S=(x_1,\ldots,x_s)\subseteq\{0,1\}^n$ and $\vec{b}=(b_1,\ldots,b_s)\in\{0,1\}^s$ with $s\leq\hat{k}$ it holds that

$$\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(S)=\vec{b}]=\Pr_{\hat{\mathcal{P}}}[\hat{\mathcal{P}}(\vec{x})=\vec{b}]\ .$$

In particular, for every distinct $x,y\in\{0,1\}^n\setminus\{0\}$ it holds that

$$\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(x)+\hat{\mathcal{F}}(y)=\hat{\mathcal{F}}(x+y)]=\Pr_{\hat{\mathcal{P}}}[\hat{\mathcal{P}}_1(x)+\hat{\mathcal{P}}_2(y)=\hat{\mathcal{P}}_3(x+y)]\geq 1-4\varepsilon\ ,$$

and for every $x\in\{0,1\}^n$ it holds that

$$\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(x)+\hat{\mathcal{F}}(x)=\hat{\mathcal{F}}(0^n)]=\Pr_{\hat{\mathcal{F}}}[\hat{\mathcal{F}}(0^n)=0]=\Pr_{\hat{\mathcal{P}}}[\hat{\mathcal{P}}_1(x)+\hat{\mathcal{P}}_1(x)=\hat{\mathcal{P}}_2(0^n)]=\Pr_{\hat{\mathcal{P}}}[\hat{\mathcal{P}}_2(0^n)=0]\geq 1-4\varepsilon\ ,$$

where the bound $\Pr_{\hat{\mathcal{P}}}[\hat{\mathcal{P}}_2(0^n)=0]\geq 1-4\varepsilon$ is argued similarly to that in Lemma E.5's proof.

Next, we would like to apply the result of Theorem 12, where we proved the implications $2\implies 3\implies 4$. However, we need $\hat{\mathcal{F}}$ to satisfy $\Pr[\hat{\mathcal{F}}(0^n)=0]=1$, but here we can only guarantee that $\Pr[\hat{\mathcal{F}}(0^n)=0]\geq 1-4\varepsilon$.

In order to fix this, we define another non-signaling function $\mathcal{F}^*$ that on the query 0^n responds with 0 with probability 1, and otherwise behaves like $\hat{\mathcal{F}}$. Formally, for every $S=\{x_1,\ldots,x_s\}$ with $s\leq\hat{k}$,

$$\Pr[\mathcal{F}^*(S)=\vec{b}]:=\begin{cases}\Pr[\hat{\mathcal{F}}(S)=\vec{b}] & \text{if } 0^n\notin S\\ \Pr[\hat{\mathcal{F}}(S\setminus\{x_i\})=(b_i)_{i\in[s]\setminus j}] & \text{if } x_j=0^n \text{ and } b_j=0\\ 0 & \text{if } x_j=0^n \text{ and } b_j=1\ .\end{cases}$$

Observe that $\mathcal{F}^*$ satisfies the the following properties.

1. $\Pr_{\mathcal{F}^*}[\mathcal{F}^*(0^n)=0]=1$.
2. For every $x,y\in\{0,1\}^n$, $\Pr_{\mathcal{F}^*}[\mathcal{F}^*(x)+\mathcal{F}^*(y)=\mathcal{F}^*(x+y)]>1-4\varepsilon$.
3. $\Delta_{\hat{k}}(\hat{\mathcal{F}},\mathcal{F}^*)\leq 4\varepsilon$.

The first two items are immediate from $\mathcal{F}^*$'s definition. The third item holds because, on all sets S that do not contain 0^n, $\mathcal{F}^*$ equals $\hat{\mathcal{F}}$, and, on all sets S that contain 0^n, the statistical distance between $\mathcal{F}^*_S$ and $\hat{\mathcal{F}}_S$ is at most the probability that $\hat{\mathcal{F}}(0^n) = 1$, which is at most 4ε.

By applying the implications $2 \Longrightarrow 3 \Longrightarrow 4$ of Theorem 12, we conclude that for every $\ell \in [\hat{k}-1]$ there exists an ℓ-local quasi-distribution $\mathcal{L}$ over linear functions such that $\Delta_\ell(\mathcal{F}^*, \mathcal{L}) \leq (2^\ell + 1) \cdot 2^{\ell/2}(\ell - 1) \cdot 4\varepsilon$, and hence $\Delta_\ell(\hat{\mathcal{F}}, \mathcal{L}) \leq \Delta_\ell(\mathcal{F}^*, \mathcal{L}) + 4\varepsilon$.

Therefore, by the symmetry of $\hat{\mathcal{P}}$ we conclude that for any vector of distinct queries $\vec{x} = (x_{i_1}, \ldots, x_{i_s})$ to $s \leq \hat{k} - 1$ players and for all events $E \subseteq \{0,1\}^s$ it holds that

$$|\Pr[\hat{\mathcal{P}}(\vec{x}) \in E] - \widetilde{\Pr}[\mathcal{L}(\vec{x}) \in E]| \leq (2^s + 1) \cdot 2^{s/2}(s-1) \cdot 4\varepsilon + 4\varepsilon \ ,$$

which is upper bounded by $2^{O(\hat{k})}\varepsilon$ for $\hat{k} \geq 2$ and $\ell \leq \hat{k} - 1$. □

F Quasi-distributions over tuples of functions

In Section 8 we used Fourier analysis to prove an equivalence between non-signaling functions and quasi-distributions over functions. In this section we use Fourier analysis to prove an analogous equivalence between non-signaling *players* and quasi-distributions over *tuples of functions*, and other results about these. The mathematical structure that we uncover seems of independent interest.

Definition F.1. *Let D be a finite domain, and denote by U_D^k the set of all k-tuples $\vec{f} = (f_1, \ldots, f_k)$ where each entry is a function $f_i \colon D \to \{0,1\}$. A* **quasi-distribution** *$\vec{\mathcal{Q}}$ over a subset $G \subseteq U_D^k$ is a set of real numbers $(q_{\vec{f}})_{\vec{f} \in G}$ such that $\sum_{\vec{f}} q_{\vec{f}} = 1$ and $q_{\vec{f}} = 0$ for all $\vec{f} \notin G$.*

Remark F.2. Non-communicating players are equivalent to *distributions* over tuples of functions. We shall prove that non-signaling players correspond to, instead, quasi-distributions. The tuples of functions $\vec{f} = (f_1, \ldots, f_k)$ can be interpreted as deterministic players that independently answer each query, the i-th player answering via the i-th "local" function f_i.

Definition F.3. *Let $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ be a quasi-distribution over U_D^k. Given a subset $I \subseteq [k]$, a vector of sets $\vec{S} = (S_i)_{i \in I}$ with $S_i \subseteq D$, and a vector of bits $\vec{b} = (b_i)_{i \in I}$ with $b_i \in \{0,1\}^{S_i}$, we define the* **quasi-probability** *of the event "$\vec{\mathcal{Q}}(\vec{S}) = \vec{b}$" to be the following (possibly negative) real number:*

$$\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{S}) = \vec{b}] = \sum_{\vec{f} \in U_D^k \text{ s.t. } \forall\, i \in I\ f_i(S_i) = b_i} q_{\vec{f}} \ .$$

We also introduce several notational shorthands. Given $\vec{S} = (S_i)_{i \in I}$ and $\vec{b} = (b_i)_{i \in I}$, we define the quasi-probability

$$\widetilde{\Pr}[\mathcal{Q}_i(S_i) = b_i \ \forall\, i \in I] := \widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{S}) = \vec{b}] \ .$$

If each S_i is a singleton $\{x_i\}$, we also write $\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}]$ and $\widetilde{\Pr}[\mathcal{Q}_i(x_i) = b_i \,\forall i \in I]$ for $\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{S}) = \vec{b}]$.

Recall a quasi-distribution that induces a non-signaling function must be local (Definition 7.4), namely, the quasi-probabilities on all "observable" events (the query sets $S \subseteq D$ with $|S| \leq k$) must be probabilities (values in $[0,1]$). In the case of non-signaling players, the observable events are query vectors $\vec{S} = (S_1, \ldots, S_k)$ with $|S_i| \leq 1$ for every i. This gives us the corresponding (unparametrized) notion of locality for quasi-distributions over tuples of functions.

Definition F.4. *A quasi-distribution $\vec{\mathcal{Q}}$ over U_D^k is* **local** *if for every $x_1, \ldots, x_k \in D$ and $b_1, \ldots, b_k \in \{0,1\}$ it holds that*

$$\widetilde{\Pr}[\mathcal{Q}_i(x_i) = b_i \,\forall i \in [k]] \in [0,1] \ .$$

The rest of this section is structured as follows.

- In Appendix F.1, we introduce the Fourier basis and coefficients that we use.
- In Appendix F.2, we prove that non-signaling players are equivalent to local quasi-distributions over tuples of functions.
- In Appendix F.3, we characterize the Fourier spectrum of notable classes of quasi-distributions (symmetric, consistent, and linear).
- In Appendix F.4, we establish relations between various notions of quasi-distributions over functions and tuples of functions. These are the intuition behind the results in Appendix E.

F.1 Fourier basis

Let D be a finite domain, and let $N := |D|$. Recall (from Section 7) that a quasi-distribution over functions $f\colon D \to \{0,1\}$ is a vector in $\mathbb{R}^{2^N}$ that assigns a real number q_f to each function $f \in U_D$ such that $\sum_{f \in U_D} q_f = 1$. Analogously, a quasi-distribution over tuples of functions $(f_1, \ldots, f_k)$ is a vector in $\mathbb{R}^{2^{Nk}}$ that assigns a real number $q_{\vec{f}}$ to each $\vec{f} \in U_D^k$ such that $\sum_{\vec{f} \in U_D^k} q_{\vec{f}} = 1$.

Given a tuple $\vec{S} = (S_1, \ldots, S_k)$ of sets $S_i \subseteq D$, define the Fourier basis vector

$$\chi_{\vec{S}}(\vec{f}) = \prod_{i=1}^{k} \chi_{S_i}(f_i) = \prod_{i=1}^{k} (-1)^{\sum_{x_i \in S_i} f_i(x_i)} = (-1)^{\sum_{i=1}^{k} \sum_{x_i \in S_i} f_i(x_i)} \ .$$

Note that $\chi_{\vec{S}} = \chi_{S_1} \otimes \chi_{S_2} \otimes \cdots \otimes \chi_{S_k}$, where the $\{\chi_{S_i}\}_i$ are Fourier basis vectors for the space of functions from $\{0,1\}^N$ to $\mathbb{R}$. In other words, the Fourier basis for quasi-distributions over U_D^k is given by the k-wise tensor product of the Fourier basis elements for quasi-distributions over U_D.

It is straightforward to verify that the set of vectors $\{\chi_{\vec{S}} : S_1, \ldots, S_k \subseteq \{0,1\}^D\}$ is orthonormal with respect to the inner product $\langle A, B \rangle := \frac{1}{2^{Nk}} \sum_{\vec{f} \in U_D^k} A(\vec{f}) \cdot B(\vec{f})$, and hence they form a basis of $\mathbb{R}^{2^{Nk}}$. Therefore, every quasi-distribution $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ can be expressed in the Fourier basis as

$$\vec{\mathcal{Q}}(\cdot) = \sum_{\vec{S} = (S_1, \ldots, S_k) : S_i \subseteq \{0,1\}^D} \widehat{q}(\vec{S}) \cdot \chi_{\vec{S}}(\cdot) \ ,$$

where $\widehat{q}(\vec{S}) = \langle \chi_{\vec{S}}, \vec{\mathcal{Q}} \rangle = \mathbb{E}_{\vec{f}}[q_{\vec{f}} \cdot \chi_{\vec{S}}(\vec{f})] = \frac{1}{2^{Nk}} \sum_{\vec{f} \in U_D^k} q_{\vec{f}} \cdot \chi_{\vec{S}}(\vec{f})$.

F.2 Equivalence

We prove that non-signaling players and local quasi-distribution over tuples of functions are equivalent. The fact that every local quasi-distribution over U_D^k induces a k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_1 \in D_1, \ldots, x_k \in D_k}$ is not hard to see. The reverse direction, namely, that every set of k-non-signaling players can be explained by a quasi-distribution over U_D^k was proved in [AB11; AS13]. Below we use Fourier analysis to prove a strengthening of this implication, by *explicitly characterizing all quasi-distributions* that explain a given k-non-signaling player.

Theorem 15. *For every k-non-signaling player $\mathcal{P} = (\mathcal{P}_{(x_1,\ldots,x_k)})_{x_i \in D}$ over a domain D of size N there exists a local quasi-distribution $\vec{\mathcal{Q}}$ over U_D^k that describes $\mathcal{P}$ (for every tuple $\vec{x} = (x_1, \ldots, x_k)$ with $x_i \in D$ and every string $\vec{b} \in \{0,1\}^k$ it holds that $\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}] = \Pr[\mathcal{P}(\vec{x}) = \vec{b}]$).*

Moreover, the set of such quasi-distributions (viewed as vectors in $\mathbb{R}^{2^{Nk}}$) is the affine subspace of co-dimension $(N+1)^k$ given by $\vec{\mathcal{Q}}_0 + span\{\chi_{(S_1,\ldots,S_k)} : |S_i| \geq 2 \text{ for some } i \in [k]\}$, where $\vec{\mathcal{Q}}_0$ is any solution and $\chi_{(S_1,\ldots,S_k)}$ is as defined above.

Proof. Similarly to the proof of Theorem 9 we divide the proof into three parts.

Finding one solution. Given a k-non-signaling player $\mathcal{P}$, let $\vec{\mathcal{Q}}$ be the quasi-distribution defined as $\vec{\mathcal{Q}}(\vec{f}) = \sum_{\vec{S} = (S_1,\ldots,S_k) : S_i \subseteq \{0,1\}^D} \widehat{q}(\vec{S}) \chi_{\vec{S}}(\vec{f})$, where $\widehat{q}(\vec{S})$ is defined as follows:

$$\widehat{q}(S_1, \ldots, S_k) := \begin{cases} \frac{1}{2^{Nk}} \left(2 \Pr[\sum_{i \in [k]} \sum_{x_i \in S_i} \mathcal{P}_i(x_i) = 0] - 1 \right) & \text{if } 0 \leq |S_i| \leq 1 \text{ for all } i \in [k] \\ 0 & \text{if } \exists\, i \in [k] \text{ such that } |S_i| \geq 2 \end{cases} .$$

In particular, $\widehat{q}(\emptyset,\ldots,\emptyset) = \frac{1}{2^{Nk}}$. Note that $\vec{\mathcal{Q}}$ is indeed a quasi-distribution because $\sum_{\vec{f}\in U_D^k} q_{\vec{f}} = 2^{Nk}\langle q, \chi_{(\emptyset,\ldots,\emptyset)}\rangle = 2^{Nk}\widehat{q}(\emptyset,\ldots,\emptyset) = 1$. We claim that for any $\vec{S} = (S_1,\ldots,S_k)$ it holds that

$$\widetilde{\Pr}\left[\sum_{i\in[k]}\sum_{x_i\in S_i}\mathcal{Q}_i(x_i) = 0\right] = \Pr\left[\sum_{i\in[k]}\sum_{x_i\in S_i}\mathcal{P}_i(x_i) = 0\right] \ .$$

Indeed,

$$\begin{aligned}
\Pr\left[\sum_{i\in[k]}\sum_{x_i\in S_i}\mathcal{P}_i(x_i) = 0\right] &= \frac{2^{Nk}\widehat{q}(S_1,\ldots,S_k)+1}{2} \\
&= \frac{\sum_{\vec{f}\in U_D^k} q_{\vec{f}}\cdot\chi_{\vec{S}}(\vec{f})+1}{2} \\
&= \frac{\sum_{\vec{f}\in U_D^k}\left(q_{\vec{f}}\cdot(-1)^{\sum_{i=1}^k\sum_{x_i\in S_i}f_i(x_i)}\right)+1}{2} \\
&= \frac{\sum_{\vec{f}\in U_D^k} q_{\vec{f}}\cdot\left((-1)^{\sum_{i=1}^k\sum_{x_i\in S_i}f_i(x_i)}+1\right)}{2} \\
&= \sum_{\substack{\vec{f}\in U_D^k \\ \sum_{i\in[k]}\sum_{x_i\in S_i}f_i(x_i)=0}} q_{\vec{f}} \\
&= \widetilde{\Pr}\left[\sum_{i\in[k]}\sum_{x_i\in S_i}\mathcal{Q}_i(x_i) = 0\right] \ .
\end{aligned}$$

Therefore, by applying Lemma 5.1 it follows that $\mathcal{P}$ matches $\vec{\mathcal{Q}}$.

Finding more solutions. Next, we claim that the Fourier coefficients of $\chi_{(S_1,\ldots,S_k)}$ such that $|S_i| \geq 2$ for some $i \in [k]$ do not affect the induced non-signaling players.

Indeed, consider any quasi-distribution $\vec{\mathcal{Q}}$, and let $\vec{S} = (S_1,\ldots,S_k)$ be such that $|S_i| \geq 2$ for some $i \in [k]$. Let $\vec{\mathcal{Q}}' = (q'_{\vec{f}})_{\vec{f}}$ be the quasi-distribution obtained from $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f}}$ by setting $q'_{\vec{f}} := q_{\vec{f}} + c\chi_{\vec{S}}(\vec{f})$. By definition, for every tuple of queries $\vec{x} = (x_1,\ldots,x_k)$ to the players and their responses $\vec{b} = (b_1,\ldots,b_k)$, it holds that

$$\widetilde{\Pr}[\vec{\mathcal{Q}}'(\vec{x}) = \vec{b}] = \sum_{\vec{f}:\vec{f}(\vec{x})=\vec{b}}\left(q_{\vec{f}} + c\chi_{\vec{S}}(\vec{f})\right) = \widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}] + c\sum_{\vec{f}:\vec{f}(\vec{x})=\vec{b}}\chi_{\vec{S}}(\vec{f}) \ .$$

We claim that $\sum_{\vec{f}:\vec{f}(\vec{x})=\vec{b}}\chi_{\vec{S}}(\vec{f}) = 0$, which implies that $\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}] = \widetilde{\Pr}[\vec{\mathcal{Q}}'(\vec{x}) = \vec{b}]$. Indeed, let $y \in S_i \setminus \{x_i\}$ (such y exists since $|S_i| \geq 2$). Then

$$\begin{aligned}
\sum_{\vec{f}:\vec{f}(\vec{x})=\vec{b}}\chi_{\vec{S}}(\vec{f}) &= \sum_{\vec{f}:\vec{f}(\vec{x})=\vec{b}}(-1)^{\sum_{i=1}^k\sum_{z_i\in S_i}f_i(z_i)} \\
&= \sum_{\substack{\vec{f}:\vec{f}(\vec{x})=\vec{b} \\ f_i(y)=0}}(-1)^{\sum_{i=1}^k\sum_{z_i\in S_i\setminus\{x_i\}}f_i(z_i)} - \sum_{\substack{\vec{f}:\vec{f}(\vec{x})=\vec{b} \\ f_i(y)=1}}(-1)^{\sum_{i=1}^k\sum_{z_i\in S_i\setminus\{x_i\}}f_i(z_i)} = 0 \ .
\end{aligned}$$

Therefore, $\vec{\mathcal{Q}}'$ matches $\vec{\mathcal{Q}}$ on all tuples of queries. Since this holds for every $\vec{S} = (S_1, \ldots, S_k)$ such that $|S_i| \geq 2$ for some $i \in [k]$, it follows that *every* $\vec{\mathcal{Q}}' \in \vec{\mathcal{Q}} + \mathrm{span}\{\chi_{\vec{S}} : \exists i \in [k] \text{ s.t. } |S_i| \geq 2\}$ also matches $\mathcal{P}$ on all queries. The co-dimension of this affine subspace is $(N+1)^k$, since the number of sets $T \subseteq D$ with $|T| \leq 1$ is $N+1$, and so the number of $\vec{S}$'s such that $|S_i| \leq 1$ for all $i \in [k]$ is $(N+1)^k$.

We found all solutions. Observe that if $\vec{\mathcal{Q}}$ is a quasi-distribution, then for every vector of sets $\vec{S} = (S_1, \ldots, S_k)$ with $\max_i\{|S_i|\} \leq 1$ it holds that

$$\widehat{q}(S_1, \ldots, S_k) = \frac{1}{2^{Nk}} \left(2\widetilde{\Pr}\left[\sum_{i \in [k]} \sum_{x_i \in S_i} \mathcal{Q}_i(x_i) = 0 \right] - 1 \right) \quad .$$

If $\vec{\mathcal{Q}}$ and $\mathcal{P}$ match, then $\widehat{q}(S_1, \ldots, S_k) = \frac{1}{2^{Nk}} \left(2\widetilde{\Pr}\left[\sum_{i \in [k]} \sum_{x_i \in S_i} \mathcal{P}_i(x_i) = 0 \right] - 1 \right)$ for all such $\vec{S}$. Thus, the set of all solutions is contained in $\vec{\mathcal{Q}} + \mathrm{span}\{\chi_{\vec{S}} : \exists i \in [k] \ |S_i| \geq 2\}$. □

F.3 Notable classes of quasi-distributions

We characterize the Fourier spectrum of quasi-distributions over U_D^k that satisfy certain natural restrictions on the support. Concretely, we consider *consistent* quasi-distributions (Appendix F.3.1), *symmetric* quasi-distributions (Appendix F.3.2), and *linear* quasi-distributions (Appendix F.3.3).

F.3.1 Consistent quasi-distributions

A quasi-distribution $\vec{\mathcal{Q}}$ is *consistent* if it is supported on tuples of functions where all functions in the tuple are the same. That is, the same input given to different slots returns the same answer.

Definition F.5. *A quasi-distribution $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_{D^k}}$ is* **consistent** *if it is supported only on tuples of functions $\vec{f} = (f_1, \ldots, f_k)$ such that $f_1 = \cdots = f_k$.*

We provide a characterization of the Fourier spectrum of consistent quasi-distributions. In the statement below, given a tuple $\vec{S} = (S_1, \ldots, S_k)$, we use $\oplus_{i=1}^k S_i$ to denote the (generalized) symmetric difference of sets (all $x \in D$ such that x appears in an odd number of S_i's).

Proposition F.6. *A quasi-distribution $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ is consistent if and only if $\widehat{q}(S_1, \ldots, S_k) = \widehat{q}(\oplus_{i=1}^k S_i, \emptyset, \ldots, \emptyset)$ for every tuple $\vec{S} = (S_1, \ldots, S_k)$.*

Proof. We use a dimension argument similar to the one used in the proof of Proposition A.1.

- Let $\mathcal{C}_1$ be the subspace of $\mathbb{R}^{2^{Nk}}$ that contains all consistent quasi-distributions. Note that $\dim(\mathcal{C}_1) = 2^{|D|} - 1 = 2^N - 1$, because $\mathcal{C}_1$ is defined by the linear constraints (i) $\sum_{\vec{f} \in U_D^k} q_{\vec{f}} = 1$, and (ii) $q_{\vec{f}} = 0$ for all $\vec{f}$ that are not of the form $(f, \ldots, f)$.

- Let $\mathcal{C}_2$ be the subspace of $\mathbb{R}^{2^{Nk}}$ that contains all quasi-distributions $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ such that (i) $\widehat{q}(\emptyset, \ldots, \emptyset) = \frac{1}{2^{Nk}}$, and (ii) $\widehat{q}(S_1, \ldots, S_k) = \widehat{q}(\oplus_{i=1}^k S_i, \emptyset, \ldots, \emptyset)$ for every tuple $\vec{S} = (S_1, \ldots, S_k)$. Observe that $\dim(\mathcal{C}_2) = 2^N - 1$ as well.

Since the two spaces have the same dimension, in order to show that they are equal it suffices to show that one space is contained in the other. We show that $\mathcal{C}_1 \subseteq \mathcal{C}_2$.

Suppose that $\vec{\mathcal{Q}}$ is consistent (if $q_{\vec{f}} \neq 0$ then $\vec{f} = (f, \ldots, f)$ for some $f \colon D \to \{0,1\}$). Note first that since $\vec{\mathcal{Q}}$ is a quasi-distribution, we have $\widehat{q}(\emptyset, \ldots, \emptyset) = \frac{\sum_f q_{\vec{f}}}{2^{Nk}} = \frac{1}{2^{Nk}}$, and thus the first condition (Item i) is satisfied. For the second condition, observe that for $\vec{f} = (f, \ldots, f)$ it holds that

$$\chi_{\vec{S}}(\vec{f}) = \prod_{i=1}^{k} (-1)^{\sum_{x_i \in S_i} f(x_i)} = (-1)^{\sum_{x \in \oplus_{i=1}^k S_i} f(x)} = \chi_{(\oplus_{i=1}^k S_i, \emptyset, \ldots, \emptyset)}(\vec{f}) \ ,$$

and hence

$$\widehat{q}(S_1, \ldots, S_k) = \frac{1}{2^{Nk}} \sum_{\vec{f}=(f,\ldots,f)} q_{\vec{f}} \cdot \chi_{\vec{S}}(\vec{f}) = \frac{1}{2^{Nk}} \sum_{\vec{f}=(f,\ldots,f)} q_{\vec{f}} \cdot \chi_{(\oplus_{i=1}^k S_i, \emptyset, \ldots, \emptyset)}(\vec{f}) = \widehat{q}(\oplus_{i=1}^k S_i, \emptyset, \ldots, \emptyset) \ ,$$

as required. □

F.3.2 Symmetric quasi-distributions

A quasi-distribution $\vec{\mathcal{Q}}$ is *symmetric* if the weights assigned to a tuple of functions and all of its permutations are the same. Below, given a permutation $\pi \colon [k] \to [k]$ and a tuple $\vec{a} = (a_1, \ldots, a_k)$, we denote by $\pi(\vec{a})$ the permuted tuple $(a_{\pi(1)}, \ldots, a_{\pi(k)})$.

Definition F.7. *A quasi-distribution $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ is* **symmetric** *if $q_{\vec{f}} = q_{\pi(\vec{f})}$ for every permutation $\pi \colon [k] \to [k]$ and tuple of functions $\vec{f} = (f_1, \ldots, f_k)$.*

A consistent quasi-distribution (Definition F.5) is, in particular, symmetric.

We provide a characterization of the Fourier spectrum of symmetric quasi-distributions.

Proposition F.8. *A quasi-distribution $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ is symmetric if and only if $\widehat{q}(\vec{S}) = \widehat{q}(\pi(\vec{S}))$ for every tuple $\vec{S} = (S_1, \ldots, S_k)$ and permutation $\pi \colon [k] \to [k]$.*

Note that the above proposition implies that Definition F.7 is equivalent to a natural alternative definition of symmetry, namely that all quasi-probabilities $\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{S}) = \vec{b}]$ depend only on the pairs $(S_1, b_1), \ldots, (S_k, b_k)$ but not their ordering in $\vec{S}$ and $\vec{b}$.

Proof. Suppose that $\vec{\mathcal{Q}}$ is symmetric. Then, for every tuple $\vec{S}$ and every permutation π,

$$\widehat{q}(\vec{S}) = \mathbb{E}_{\vec{f}}[q_{\vec{f}} \cdot \chi_{\vec{S}}(\vec{f})] = \mathbb{E}_{\vec{f}}[q_{\pi^{-1}(\vec{f})} \cdot \chi_{\vec{S}}(\vec{f})] = \mathbb{E}_{\vec{f}}[q_{\vec{f}} \cdot \chi_{\pi(\vec{S})}(\vec{f})] = \widehat{q}(\pi(\vec{S})) \ .$$

In the opposite direction, suppose that $\vec{\mathcal{Q}}$ is such that $\widehat{q}(\vec{S}) = \widehat{q}(\pi(\vec{S}))$ for every tuple $\vec{S}$ and every permutation π. Then, for every $\vec{f} \in U_D^k$ and every permutation π,

$$q_{\vec{f}} = \sum_{\vec{S}} \widehat{q}(\vec{S}) \chi_{\vec{S}}(\vec{f}) = \sum_{\vec{S}} \widehat{q}(\pi^{-1}(\vec{S})) \chi_{\vec{S}}(\vec{f}) = \sum_{\vec{S}} \widehat{q}(\vec{S}) \chi_{\vec{S}}(\pi(\vec{f})) = q_{\pi(\vec{f})} \ . \qquad \square$$

F.3.3 Linear quasi-distributions

A quasi-distribution $\vec{\mathcal{Q}}$ is *linear* if it is supported on tuples of linear functions.

Definition F.9. *A quasi-distribution $\vec{\mathcal{Q}}$ over $U^k_{\{0,1\}^n}$ is* **linear** *if it is supported on tuples $\vec{f} = (f_1, \ldots, f_k)$ such that each $f_i \colon \{0,1\}^n \to \{0,1\}$ is a linear function.*

We provide a characterization of the Fourier spectrum of linear quasi-distributions. This characterization extends Proposition A.1 from the case of single functions to tuples of functions.

Proposition F.10. *A quasi-distribution $\vec{\mathcal{Q}}$ over $U^k_{\{0,1\}^n}$ is linear if and only if $\widehat{q}(S_1, \ldots, S_k) = \widehat{q}(\{\sum_{x \in S_1} x\}, \ldots, \{\sum_{x \in S_k} x\})$ for every tuple $\vec{S} = (S_1, \ldots, S_k)$. (If S_i is empty then $\sum_{x \in S_i} x := 0^n$.)*

Proof. We adapt the dimension argument used in the proof of Proposition A.1.

- Let $\mathcal{C}_1$ be the space of all linear quasi-distributions (as a subspace of $\mathbb{R}^{2^{Nk}}$). Note that $\dim(\mathcal{C}_1) = N^k - 1$, because $\mathcal{C}_1$ is defined by the linear constraints (i) $\sum_{\vec{f} \in U^k_{\{0,1\}^n}} q_{\vec{f}} = 1$, and (ii) $q_{\vec{f}} = 0$ for every $\vec{f}$ that is not a tuple of linear functions.
- Let $\mathcal{C}_2$ be the space of all quasi-distributions $\vec{\mathcal{Q}}$ such that $q(\emptyset, \ldots, \emptyset) = \frac{1}{2^{Nk}}$ and $\widehat{q}(S_1, \ldots, S_k) = \widehat{q}(\{\sum_{x \in S_1} x\}, \ldots, \{\sum_{x \in S_k} x\})$ for every tuple $\vec{S} = (S_1, \ldots, S_k)$. Observe that $\dim(\mathcal{C}_2) = N^k - 1$ since it is defined by the equality constraints above and the constraint $\widehat{q}(\emptyset, \ldots, \emptyset) = \frac{1}{2^{Nk}}$.

Since since the two spaces have the same dimension, to show that they are equal, it suffices to show that one space is contained in the other. Note $\mathcal{C}_1 \subseteq \mathcal{C}_2$ is clear since every linear $\vec{\mathcal{Q}}$ satisfies $\widehat{q}(S_1, \ldots, S_k) = \widehat{q}(\{\sum_{x \in S_1} x\}, \ldots, \{\sum_{x \in S_k} x\})$ by definition of the Fourier coefficients and linearity, which concludes the proof. □

F.4 Two lemmas on symmetric quasi-distributions

We prove that: (i) consistent quasi-distributions over U_D^k correspond to quasi-distributions over U_D (Lemma F.11); (ii) symmetric quasi-distributions over U_D^k can be simulated by consistent quasi-distributions over U_D^k via queries with non-repeated entries (Lemma F.12).

Lemma F.11. *There is a natural equivalence between quasi-distributions over functions and consistent quasi-distributions over tuples of functions. Specifically:*

1. *For every quasi-distribution $\mathcal{Q}$ over U_D and for every k, there exists a consistent quasi-distribution $\vec{\mathcal{Q}}$ over U_D^k such that for every $\vec{x} = (x_1, \ldots, x_k)$ with $x_i \in D$ and $\vec{b} = (b_1, \ldots, b_k)$ with $b_i \in \{0,1\}$ it holds that $\widetilde{\Pr}[\mathcal{Q}(\vec{x}) = \vec{b}] = \widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}]$. Moreover, if $\mathcal{Q}$ is k-local then $\vec{\mathcal{Q}}$ is local.*
2. *For every consistent quasi-distribution $\vec{\mathcal{Q}}$ over U_D^k there exists a quasi-distribution $\mathcal{Q}$ over U_D such that for every set $\vec{x} = (x_1, \ldots, x_k) \subseteq D$ and $\vec{b} = (b_1, \ldots, b_k) \in \{0,1\}^k$ it holds that $\widetilde{\Pr}[\mathcal{Q}(\vec{x}) = \vec{b}] = \widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}]$. Moreover, if $\vec{\mathcal{Q}}$ is local then $\mathcal{Q}$ is k-local.*

Proof. Let $\mathcal{Q} = (p_f)_{f \in U_D}$ be a quasi-distribution over U_D and let k be a positive integer. Define $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ to be the consistent quasi-distribution over U_D^k where $q_{(f,\ldots,f)} := p_f$ for every $f \in U_D$ and all other weights are zero. Note that $\vec{\mathcal{Q}}$ has the desired property by construction. Furthermore, it is clear that if $\mathcal{Q}$ is k-local then $\vec{\mathcal{Q}}$ is local.

Conversely, let $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ be a consistent quasi-distribution over U_D^k. By definition, $\vec{\mathcal{Q}}$ is supported only on tuples of functions of the form $(f, \ldots, f)$. Let $\mathcal{Q} = (p_f)_{f \in U_D}$ be the quasi-distribution over U_D where $p_f := q_{(f,\ldots,f)}$ for every $f \in U_D$. Note that $\mathcal{Q}$ has the desired property by construction. Moreover, it is clear that if $\vec{\mathcal{Q}}$ is local then $\mathcal{Q}$ is k-local. □

Lemma F.12. *For every* symmetric *quasi-distribution $\vec{\mathcal{Q}}$ over U_D^k there exists a* consistent *quasi-distribution $\vec{\mathcal{Q}}'$ over U_D^k such that for every $\vec{x} = (x_1, \ldots, x_k) \in D^k$ and $\vec{b} = (b_1, \ldots, b_k) \in \{0,1\}^k$ such that $x_i \neq x_j$ for all $i \neq j$ it holds that $\widetilde{\Pr}[\vec{\mathcal{Q}}(\vec{x}) = \vec{b}] = \widetilde{\Pr}[\vec{\mathcal{Q}}'(\vec{x}) = \vec{b}]$.*

Proof. Let $\vec{\mathcal{Q}} = (q_{\vec{f}})_{\vec{f} \in U_D^k}$ be a symmetric quasi-distribution over U_D^k. We first define a quasi-distribution $\mathcal{P} = (p_f)_{f \in U_D}$ over U_D (i.e., over functions) that matches $\vec{\mathcal{Q}}$ in a specific way. Formally, we specify $\mathcal{P}$ via its Fourier coefficients:

$$\widehat{p}(S) := \begin{cases} \frac{1}{2^N} \left(2 \sum_{\vec{f}: \sum_{i=1}^s f_i(x_i) = 0} q_{\vec{f}} - 1 \right) & S = \{x_1, \ldots, x_s\} \subseteq D \text{ with } s \leq k \\ 0 & \text{if } |S| > k \end{cases} .$$

Note that since $\vec{\mathcal{Q}}$ is symmetric, the summation is *independent* of the ordering assigned to the elements of S. It follows that for any set of s queries $S = \{x_1, \ldots, x_s\} \subseteq \{0,1\}^n$, it holds that

$$\widetilde{\Pr}\left[\sum_{i=1}^s \mathcal{P}(x_i) = 0\right] = \sum_{f: \sum_{i=1}^s f(x_i) = 0} p_f = \frac{2^N \widehat{p}(S) + 1}{2} = \sum_{\vec{f}: \sum_{i=1}^s f_i(x_i) = 0} q_{\vec{f}} = \widetilde{\Pr}\left[\sum_{i=1}^s \vec{\mathcal{Q}}_i(x_i) = 0\right] .$$

Note that on the lefthand side we sample one function from a quasi-distribution over U_D, while on the righthand side we sample a tuple of functions from a quasi-distribution over U_D^k. By Lemma 7.3 this implies that for every $S = \{x_1, \ldots, x_s\}$ with ordering $\vec{x} = (x_1, \ldots, x_s) \in D^s$ and $\vec{b} = (b_1, \ldots, b_s) \in \{0,1\}^s$ it holds that $\widetilde{\Pr}[\mathcal{P}(S) = \vec{b}] = \widetilde{\Pr}[\mathcal{Q}(\vec{x}) = \vec{b}]$. By Proposition F.6 there is a consistent quasi-distribution $\vec{\mathcal{Q}}'$ matching $\mathcal{P}$, and so $\vec{\mathcal{Q}}'$ has the desired properties. □

Acknowledgements

We are grateful to Aneesh Manohar for helpful discussions on the prior uses of quasi-distributions in quantum mechanics. We thank Tom Gur and Thomas Vidick for useful discussions and suggestions that have improved the presentation in this paper. We thank anonymous reviewers who brought [SA90; RS09; AS13] to our attention, encouraged us to also explore statements for non-signaling players, and provided other valuable feedback. We thank Matthew Pusey for referring us to [AB11].

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.

[ABOR00] William Aiello, Sandeep N. Bhatt, Rafail Ostrovsky, and Sivaramakrishnan Rajagopalan. "Fast Verification of Any Remote Procedure Call: Short Witness-Indistinguishable One-Round Proofs for NP". In: *Proceedings of the 27th International Colloquium on Automata, Languages and Programming*. ICALP '00. 2000, pp. 463–474.

[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.

[AS03] Sanjeev Arora and Madhu Sudan. "Improved Low-Degree Testing and its Applications". In: *Combinatorica* 23.3 (2003). Preliminary version appeared in STOC '97., pp. 365–426.

[AS13] Sabri W. Al-Safi and Anthony J. Short. "Simulating all Nonsignaling Correlations via Classical or Quantum Theory with Negative Probabilities". In: *Physical Review Letters* 111 (17 2013), p. 170403.

[AS98] Sanjeev Arora and Shmuel Safra. "Probabilistic checking of proofs: a new characterization of NP". In: *Journal of the ACM* 45.1 (1998). Preliminary version in FOCS '92., pp. 70–122.

[BBLMTU06] Gilles Brassard, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger. "Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial". In: *Physical Review Letters* 96 (25 2006), p. 250401.

[BCHKS96] Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos A. Kiwi, and Madhu Sudan. "Linearity testing in characteristic two". In: *IEEE Transactions on Information Theory* 42.6 (1996), pp. 1781–1795.

[BCLR08] Michael Ben-Or, Don Coppersmith, Mike Luby, and Ronitt Rubinfeld. "Non-abelian homomorphism testing, and distributions close to their self-convolutions". In: *Random Structures and Algorithms* 32.1 (2008), pp. 49–70.

[BCUWW06] Harry Buhrman, Matthias Christandl, Falk Unger, Stephanie Wehner, and Andreas Winter. "Implications of superstrong non-locality for cryptography". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 462.2071 (2006), pp. 1919–1932.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. "Non-Deterministic Exponential Time has Two-Prover Interactive Protocols". In: *Computational Complexity* 1 (1991). Preliminary version appeared in FOCS '90., pp. 3–40.

[BFLS91] László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. "Checking computations in polylogarithmic time". In: *Proceedings of the 23rd ACM Symposium on Theory of Computing*. STOC '91. 1991, pp. 21–32.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. "No Signaling and Quantum Key Distribution". In: *Physical Review Letters* 95 (1 2005), p. 010503.

[BKSSZ10] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. "Optimal testing of Reed-Muller codes". In: *Proceedings of the 51st IEEE Symposium on Foundations of Computer Science*. FOCS '10. 2010, pp. 488–497.

[BLMPPR05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. "Nonlocal correlations as an information-theoretic resource". In: *Physical Review Letters* 71 (2 2005), p. 022101.

[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.

[BM06] Anne Broadbent and André Allan Méthot. "On the Power of Non-local Boxes". In: *Theoretical Computer Science* 358.1 (2006), pp. 3–14.

[BP05] Jonathan Barrett and Stefano Pironio. "Popescu–Rohrlich Correlations as a Unit of Nonlocality". In: *Physical Review Letters* 95 (14 2005), p. 140401.

[Bar07] Jonathan Barrett. "Information processing in generalized probabilistic theories". In: *Physical Review A* 75 (3 2007), p. 032304.

[CGMP05] Nicolas J. Cerf, Nicolas Gisin, Serge Massar, and Sandu Popescu. "Simulating Maximal Quantum Entanglement without Communication". In: *Physical Review Letters* 94 (22 2005), p. 220403.

[CR17] Rui Chao and Ben W. Reichardt. *Test to separate quantum theory from non-signaling theories*. arXiv quant-ph/1706.02008. 2017.

[DDGKS17] Roee David, Irit Dinur, Elazar Goldenberg, Guy Kindler, and Igor Shinkar. "Direct Sum Testing". In: *SIAM Journal on Computing* 46 (4 2017), pp. 1336–1369.

[DLNNR04] Cynthia Dwork, Michael Langberg, Moni Naor, Kobbi Nissim, and Omer Reingold. *Succinct NP Proofs and Spooky Interactions*. Available at `www.openu.ac.il/home/mikel/papers/spooky.ps`. 2004.

[Dir42] Paul A. M. Dirac. "The physical interpretation of quantum mechanics". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 180.980 (1942), pp. 1–40.

[FGLSS96] Uriel Feige, Shafi Goldwasser, Laszlo Lovász, Shmuel Safra, and Mario Szegedy. "Interactive proofs and the hardness of approximating cliques". In: *Journal of the ACM* 43.2 (1996). Preliminary version in FOCS '91., pp. 268–292.

[Fey87] Richard P. Feynman. "Negative Probability". In: *Quantum Implications: Essays in Honour of David Bohm*. Ed. by Basil J. Hiley and D. Peat. 1987, pp. 235–248.

[GGR98] Oded Goldreich, Shafi Goldwasser, and Dana Ron. "Property Testing and its Connection to Learning and Approximation". In: *Journal of the ACM* 45.4 (1998), pp. 653–750.

[Hol09] Thomas Holenstein. "Parallel Repetition: Simplification and the No-Signaling Case". In: *Theory of Computing* 5.1 (2009). Preliminary version appeared in STOC '07., pp. 141–172.

[IKM09] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. "Oracularization and Two-Prover One-Round Interactive Proofs against Nonlocal Strategies". In: *Proceedings of the 24th IEEE Annual Conference on Computational Complexity*. CCC '09. 2009, pp. 217–228.

[IV12] Tsuyoshi Ito and Thomas Vidick. "A Multi-prover Interactive Proof for NEXP Sound against Entangled Provers". In: *Proceedings of the 53rd IEEE Symposium on Foundations of Computer Science*. FOCS '12. 2012, pp. 243–252.

[Ito10] Tsuyoshi Ito. "Polynomial-Space Approximation of No-Signaling Provers". In: *Proceedings of the 37th International Colloquium on Automata, Languages and Programming*. ICALP '10. 2010, pp. 140–151.

[JM05] Nick S. Jones and Lluís Masanes. "Interconversion of nonlocal correlations". In: *Physical Review A* 72 (5 2005), p. 052312.

[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.

[KT85] Leonid A. Khalfin and Boris S. Tsirelson. "Quantum and quasi-classical analogs of Bell inequalities". In: *Symposium on the Foundations of Modern Physics* (1985), pp. 441–460.

[LFKN92] Carsten Lund, Lance Fortnow, Howard J. Karloff, and Noam Nisan. "Algebraic Methods for Interactive Proof Systems". In: *Journal of the ACM* 39.4 (1992), pp. 859–868.

[LPSW07] Noah Linden, Sandu Popescu, Anthony J. Short, and Andreas Winter. "Quantum Nonlocality and Beyond: Limits from Nonlocal Computation". In: *Physical Review Letters* 99 (18 2007), p. 180502.

[MAG06] Lluís Masanes, Antonio Acín, and Nicolas Gisin. "General properties of nonsignaling theories". In: *Physical Review A* 73 (1 2006), p. 012112.

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

[PR98] Sandu Popescu and Daniel Rohrlich. "Causality and Nonlocality as Axioms for Quantum Mechanics". In: *Causality and Locality in Modern Physics: Proceedings of a Symposium in honour of Jean-Pierre Vigier*. Ed. by Geoffrey Hunter, Stanley Jeffers, and Jean-Pierre Vigier. Springer Netherlands, 1998, pp. 383–389.

[RS09] Prasad Raghavendra and David Steurer. "Integrality Gaps for Strong SDP Relaxations of UNIQUE GAMES". In: *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science*. FOCS '09. Full version at `http://people.eecs.berkeley.edu/~prasad/Files/cspgaps.pdf`. 2009, pp. 575–585.

[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.

[RS97] Ran Raz and Shmuel Safra. "A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP". In: *Proceedings of the 29th ACM Symposium on Theory of Computing*. STOC '97. 1997, pp. 475–484.

[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.

[SGP06] Anthony J. Short, Nicolas Gisin, and Sandu Popescu. "The Physics of No-Bit-Commitment: Generalized Quantum Non-Locality Versus Oblivious Transfer". In: *Quantum Information Processing* 5.2 (2006), pp. 131–138.

[SPG06] Anthony J. Short, Sandu Popescu, and Nicolas Gisin. "Entanglement swapping for generalized nonlocal correlations". In: *Physical Review A* 73 (1 2006), p. 012101.

[SW04] Amir Shpilka and Avi Wigderson. "Derandomizing Homomorphism Testing in General Groups". In: *Proceedings of the 36th ACM Symposium on the Theory of Computing*. STOC '04. 2004, pp. 427–435.

[Sha92] Adi Shamir. "IP = PSPACE". In: *Journal of the ACM* 39.4 (1992), pp. 869–877.

[Vid14] Thomas Vidick. *Linearity testing with entangled provers*. `http://users.cms.caltech.edu/~vidick/linearity_test.pdf`. 2014.

[WW05] Stefan Wolf and Jürg Wullschleger. "Oblivious transfer and quantum non-locality". In: *Proceedings of the 2005 International Symposium on Information Theory*. ISIT '05. 2005, pp. 1745–1748.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. 2014.

[van13] Wim van Dam. "Implausible consequences of superstrong nonlocality". In: *Natural Computing* 12 (1 2013), pp. 9–12.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il