Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 142 (2013)

Property Testing Bounds for Linear and Quadratic Functions via Parity Decision Trees

Abhishek Bhrushundi[1], Sourav Chakraborty[1], and Raghav Kulkarni[2]

[1] {abhishek_bhr,sourav}@cmi.ac.in
Chennai Mathematical Institute
India
[2] kulraghav@gmail.com
Center for Quantum Technologies
Singapore

Abstract. In this paper[1] , we study linear and quadratic Boolean functions in the context of property testing. We do this by observing that the query complexity of testing properties of linear and quadratic functions can be characterized in terms of the complexity in another model of computation called *parity decision trees*.
The observation allows us to characterize the testable properties of linear functions in terms of the approximate l_1 norm of the Fourier spectrum of an associated function. It also allows us to reprove the $\Omega(k)$ lower bound for testing k-linearity due to Blais et al [7]. More interestingly, it rekindles the hope of closing the gap of $\Omega(k)$ vs $O(k \log k)$ for testing k-linearity by analyzing the randomized parity decision tree complexity of a fairly simple function called E_k that evaluates to 1 if and only if the number of 1s in the input is exactly k. The approach of Blais et al. using communication complexity fails to give anything better than $\Omega(k)$ as a lower bound.
In the case of quadratic functions, we prove[2] an adaptive, two-sided $\Omega(n^2)$ lower bound for testing affine isomorphism to the inner product function. We remark that this bound is tight and furnishes an example of a function for which the trivial algorithm for testing affine isomorphism is the best possible. As a corollary, we obtain an $\Omega(n^2)$ lower bound for testing the class of *Bent* functions.
We believe that our techniques might be of independent interest and may be useful in proving other testing bounds.

1 Introduction

The field of property testing broadly deals with determining whether a given object satisfies a property $\mathcal{P}$ or is very different from all the objects that satisfy

[1] This paper combines the unpublished manuscripts [5,14].
[2] We remark that this result was proved by us in [5], and Grigorescu et al.[20] concurrently and independently obtained the same lower bound for testing affine isomorphism to the inner product function, and a stronger lower bound for testing Bent functions.

ISSN 1433-8092

$\mathcal{P}$. In this paper, the objects of interest are Boolean functions on n variables, i.e. functions of the form

$$f : \{0,1\}^n \to \{0,1\}.$$

A Boolean function property $\mathcal{P}$ is a collection of Boolean functions. Given a function g and a parameter ϵ, the goal of a tester is to distinguish between the following two cases:

- $g \in \mathcal{P}$
- g differs from every function in $\mathcal{P}$ in at least ϵ fraction of points in $\{0,1\}^n$.

The query complexity for testing $\mathcal{P}$ is the number of queries (of the form "what is the value of g at $x \in \{0,1\}^n$?") made by the best tester that distinguishes between the above two cases. If the queries made by the tester depend on the answers to the previous queries, the tester is called *adaptive*. Also, if the tester accepts whenever $g \in \mathcal{P}$, it is called *one-sided*.

Testing of Boolean function properties has been extensively studied over the last couple of decades (See [16,29]). Examples of problems that have been studied are linearity testing [10], k-junta testing [17,6], monotonicity testing [18,12], k-linearity testing [19,11,7] etc. An important problem in the area is to characterize Boolean function properties whose query complexity is *constant* (i.e., independent of n, though it can depend on ϵ). For example, such a characterization is known in the case of graph properties [1]. Though a general characterization for function properties is not yet known, there has been progress for some special classes of properties. In this paper, we attempt characterizing one such class: properties which only consist of linear functions. More specifically, we try to characterize all properties $\mathcal{P}$ of linear Boolean functions which can be tested using constant number of queries.

An example of a property of linear functions is one that contains all parities on k variables[3]. The problem of testing this property is known as k-linearity testing. While this problem had been studied earlier [19], recently Blais et al. [7] used communication complexity to obtain a lower bound of $\Omega(k)$ on the query complexity of adaptive testers for k-linearity. The best known upper bound in the case of adaptive testers is $O(k \log k)$. Whereas a tight bound of $\Theta(k \log k)$ is known for the non-adaptive case [11], a gap still exists for adaptive testing: $\Omega(k)$ vs $O(k \log k)$. In this paper we give another approach to obtain the $\Omega(k)$ lower bound for the adaptive query complexity. While the lower bound technique of Blais et al.[7] cannot be improved beyond $\Omega(k)$, our technique has the potential of proving a better lower bound. We remark that other proof techniques for the lower bound have also been studied [8].

A rich class of properties for which characterizing constant query testability has been studied are properties that are invariant under natural transformations of the domain. For example, [23,4,3] study invariance under affine/linear transformations in this context. Properties that consist of functions isomorphic to a

[3] A function $f : \{0,1\}^n \to \{0,1\}$ is a parity on k variables if it is of the form $\sum_{i \in S} x_i$, where $S \subseteq [n]$ and $|S| = k$

given function also form an important subclass. The testing of such properties is commonly referred to as *isomorphism testing*, and has seen two directions of study: testing if a function is equivalent to a given function up to permutation of coordinates [13,9], and testing affine/linear isomorphism.

Our second result concerns testing affine/linear isomorphism. A function f is affine/linear isomorphic to g if there is an invertible affine/linear transformation T such that $f \circ T = g$. Recently, Wimmer and Yoshida [31] characterized the query complexity of testing affine/linear isomorphism to a function in terms of the *Fourier norm*. We complement their work by providing the first example of a function for which the query complexity of testing affine isomorphism is the largest possible. As a corollary, we also prove an adaptive, two-sided $\Omega(n^2)$ lower bound for testing the class of *Bent* functions which are an important and well-studied class of Boolean functions in cryptography (See [26,27]).

Grigorescu et al. concurrently and independently obtained these results in [20] using a different proof technique. In fact, they prove an $2^{\Omega(n)}$ lower bound for testing Bent functions. We believe that our proof is arguably simpler and more modular, and is also amenable to generalizations (for example, to the quantum setting), even though the bound we obtain for Bent functions is weaker.

The main technique used in proving all our results is a connection between testing properties of linear and quadratic functions, and parity decision trees. Connections between linear functions and parity decision trees have been both implicitly [8] and explicitly [11] observed in earlier papers. Another connection that we exploit for proving some of our results is the one between parity decision tree depth and communication complexity. Similar connections were known earlier, see for example [32]. We remark that, to the best of our knowledge, our result is the first that combines the two connections, giving yet another way of relating property testing lower bounds to communication complexity (Blais et al. [7] observe such a connection in much more generality). Thus, we believe that our techniques might be of independent interest.

1.1 Our results and techniques

Property testing and parity decision trees We give a connection between testing properties of linear functions and parity decision trees. The following is an informal statement of the connection:

Connection 1 *For every property $\mathcal{P}$ of linear functions on n variables, one can associate a Boolean function $E_{\mathcal{P}}$ on n variables such that there is an adaptive q-query tester for distinguishing if a given f is in $\mathcal{P}$ or $1/2$-far from $\mathcal{P}$ if and only if there is a randomized parity decision tree that makes q queries for deciding $E_{\mathcal{P}}$.*

A similar connection holds in the case of quadratic functions.

Connection 2 *For every property $\mathcal{P}$ of quadratic functions on n variables, one can associate a Boolean function $E_{\mathcal{P}}$ on n^2 variables such that there is an adaptive q query tester for distinguishing if a given f is in $\mathcal{P}$ or $1/4$-far from $\mathcal{P}$ only*

if there is a randomized parity decision tree that makes q queries for deciding $E_{\mathcal{P}}$.

Note that, unlike Connection 1, Connection 2 does not give a conversion in both directions i.e. a randomized parity decision tree of depth q for $E_{\mathcal{P}}$ does not necessarily imply a q-query tester for $\mathcal{P}$.

All the results that follow use the above lemmas crucially. Another important ingredient for some of the results is a connection between parity decision trees and the communication complexity of XOR functions. We discuss this in detail in Section 3.

Characterization of testable properties of linear functions A by-product of Connection 1 is that it allows us to characterize the constant query testability of a property $\mathcal{P}$ of linear functions in terms of the approximate L_1 norm of $E_{\mathcal{P}}$.

Theorem 3. *A property $\mathcal{P}$ of linear Boolean functions is constant query testable if and only if $||\widehat{E_{\mathcal{P}}}||_1^{1/4}$ is constant.*

This is the first such characterization of linear function properties, and we hope our result is a small step towards our understanding of function properties testable in constant number of queries.

Testing k-linearity We also obtain an alternate proof of the lower bound for testing k-linearity due to Blais et al. [7].

Theorem 4. *Any adaptive two-sided tester for testing k-linearity requires $\Omega(k)$ queries.*

The idea behind the proof is as follows. Applying Connection 1 in the case of k-linearity, $E_{\mathcal{P}}$ turns out to be equal to the function E_k that outputs 1 if and only if there are exactly k 1s in the input string. Thus, to prove Theorem 4 it is sufficient to lower bound the randomized parity decision tree complexity of E_k by $\Omega(k)$.

As mentioned before, the communication complexity approach of Blais et al. cannot give anything better than $\Omega(k)$ since it crucially relies on the lower bound on the communication complexity of the k-disjointness function, which has an $O(k)$ upper bound [21]. Our technique leaves open the possibility of proving a tight $\Omega(k \log k)$ lower bound by analyzing the parity decision tree complexity of the relatively simple function E_k.

Even if there is an $O(k)$ upper bound on the randomized parity decision tree complexity of E_k, since Connection1 holds in both directions, we will obtain a tight upper bound of $O(k)$ for testing[4] k-linearity.

[4] To be more precise, we will obtain a tester that can distinguish a k-linear function from $k+1$-linear function using $O(k)$ queries. Even for this restricted problem, the best known tester makes $O(k \log k)$ queries.

Lower bound for testing affine isomorphism Let $\mathbf{IP}_n(x)$ denote the inner product function $\sum_{i=1}^{n/2} x_i x_{n/2+i}$. We consider the problem of testing affine isomorphism to $\mathbf{IP}_n(x)$ and prove a tight lower bound.

Theorem 5. *Testing affine isomorphism to* $\mathbf{IP}_n(x)$ *requires* $\Omega(n^2)$ *queries.*

We note that the bound holds even for adaptive 2-sided testers.

The proof of Theorem 5 is similar to that of Theorem 4, though in this case, $E_{\mathcal{P}}$ turns out to be E_n, a function that maps graphs on n vertices to $\{0,1\}$, and outputs 1 if and only if the input graph's adjacency matrix is nonsingular over $\mathbb{F}_2$.

As mentioned before, this is the first example of a function for which testing affine isomorphism requires $\Omega(n^2)$ queries ($O(n^2)$ is a trivial upper bound for any function and follows from a folklore result).

It can be show that testing the set of quadratic Bent functions reduces to testing affine isomorphism to $\mathbf{IP}_n(x)$. Thus, Theorem 5 gives a lower bound for testing the set of quadratic Bent functions. Furthermore, using a result from [15], the following corollary can be obtained.

Corollary 1. *Any adaptive two-sided tester for testing the set of Bent functions requires* $\Omega(n^2)$ *queries.*

1.2 Organization

Section 2 contains a few preliminaries. In Section 3, we prove Lemma 1 and 2, followed by proofs of Theorem 3 and 4 in Sections 4 and 5 respectively. Section 6 gives proofs of Theorem 5 and Corollary 1.

2 Preliminaries

2.1 Boolean functions

Recall that functions mapping $\{0,1\}^n$ to $\{0,1\}$ are called Boolean functions[5]. A Boolean function is linear if it is expressible as $\sum_{i \in S} x_i$ for $S \subseteq [n]$. The set of linear functions will be denoted by $\mathcal{L}$.

A Boolean function is quadratic if it can be expressed as a polynomial of degree at most two over $\mathbb{F}_2$. We shall denote the set of quadratic functions by $\mathcal{Q}$, and the set of homogenous quadratic functions by $\mathcal{Q}_0$. By a property of linear or quadratic functions, we shall always mean a subset of $\mathcal{L}$ or $\mathcal{Q}$.

For Boolean functions f and g, $dist(f,g) = \Pr_x[f(x) \neq g(x)]$. The notion can be extended to sets of Boolean functions S and T in a natural way: $dist(S,T) = \min_{f \in S, g \in T} dist(f,g)$. We state a simple but useful observation:

Observation 6 *If* f *and* g *are linear (quadratic) functions then either* $f = g$ *or* $dist(f,g) \geq 1/2$ *(*$dist(f,g) \geq 1/4$*).*

[5] In certain contexts it will be useful to identify $\{0,1\}$ with $\mathbb{F}_2$

We now introduce the basics of Fourier analysis for Boolean functions [6]

For a subset $S \subseteq [n]$, $\chi_S(x) := (-1)^{\sum_{i \in S} x_i}$. These are called the character functions. Consider the space of all functions from $\{0,1\}^n$ to $\mathbb{R}$, equipped with the inner product $\langle f, g \rangle = \mathbb{E}_x f(x)g(x)$. The character functions form an orthonormal basis with respect to the this inner product, and for any function $f : \{0,1\}^n \to \mathbb{R}$,

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S(x)$$

$(\hat{f}(S))_{S \subseteq [n]}$ is called the Fourier transform of f, where the Fourier coefficient $\hat{f}(S)$ can be computed as follows:

$$\hat{f}(S) = \langle f, \chi_S \rangle$$

The norm of a function f is defined to be $||f|| = \sqrt{\langle f, f \rangle}$. Orthonormality of $\{\chi_S\}$ implies the *Parseval's identity:* $||f|| = \sum_{S \subseteq n} \hat{f}^2(S)$. For Boolean functions $||f|| = 1$, and hence Parseval's identity shows that $\sum_{S \subseteq n} \hat{f}^2(S) = 1$

The Fourier norm of a function f is defined as the l_1 norm of its Fourier transform i.e $\sum_{S \subseteq n} |\hat{f}(S)|$. We shall denote it by $\|\hat{f}\|_1$. The ϵ-approximate l_1 norm of the Fourier spectrum of f, denoted by $||\widehat{f}||_1^{\epsilon}$, is the minimum possible $||\widehat{g}||_1$ over all g such that, for all x $|g(x) - f(x)| \leq \epsilon$.

In the paper we also encounter Bent Boolean functions. A function f is said to be Bent if $\forall S \subseteq [n]$, $\hat{f}^2(S) = \frac{1}{2^n}$.

2.2 Property testing

Let $\mathcal{P}$ be a property of Boolean functions on n variables. We say a randomized algorithm $\mathcal{A}$ ϵ-tests $\mathcal{P}$, if given oracle access to the truth table of an input function f, $\mathcal{A}$ determines with probability at least $2/3$ whether $f \in \mathcal{P}$, or $dist(f, \mathcal{P}) \geq \epsilon$. The number of queries made by the best tester for ϵ-testing $\mathcal{P}$ is known as the query complexity of $\mathcal{P}$. It is denoted by $Q^{\epsilon}(\mathcal{P})$ and may be a function of n.

Remark When testing properties of linear functions, it is common to assume that the input function is promised to be a linear function. For a property $\mathcal{P}$ of linear functions, we denote the query complexity of testing $\mathcal{P}$ under such a promise by $Q_1(\mathcal{P})$.

For technical reasons, it will be useful to consider such a notion for quadratic function. For a property $\mathcal{P} \subseteq \mathcal{Q}$ of quadratic functions, we shall denote by $Q_2(\mathcal{P})$ the query complexity of testing $\mathcal{P}$ under the promise that the input is always a function in $\mathcal{Q}_0$. Observation 6 implies the following statement.

Observation 7 *Let $\mathcal{P}$ be a property of linear functions. Then, $Q^{1/2}(\mathcal{P}) \geq Q_1(\mathcal{P})$. Similarly, in the case of quadratic functions, $Q^{1/4}(\mathcal{P}) \geq Q_2(\mathcal{P})$*

It can also be shown that:

[6] Sometimes it will be convenient to consider a Boolean function f as a function mapping $\{0,1\}^n$ to $\{-1,+1\}$ by looking at $(-1)^{f(x)}$.

Observation 8 *If $Q_1(\mathcal{P}) = Q$ then $\forall \epsilon \in (0, 1/4)$, $Q^\epsilon(\mathcal{P}) \leq O_\epsilon(Q \log Q)$*

We include a proof in Appendix A.

Let G be a group that acts on $\{0,1\}^n$. A function f is G-isomorphic to another function g if there is a $\phi \in G$ such that $f \circ \phi = g$. For a fixed function g, the problem of testing G-isomorphism to g is to test if an input function f is G-isomorphic to g, or ϵ-far from all functions that are G-isomorphic to g. A folklore result gives a trivial upper bound for the problem:

Lemma 1. *Testing G-isomorphism to a function g can be done in $O(\log |G|)$ queries.*

Here $|G|$ denotes the size of the group.

When G is the group of invertible affine transformations, the problem is known as affine isomorphism testing. The above lemma gives us the following corollary:

Corollary 2. *$O(n^2)$ queries suffice to test affine isomorphism.*

2.3 Parity decision trees

Parity decision trees extends the model of ordinary decision trees such that one may query the parity of a subset of input bits, i.e. the queries are of form "is $\sum_{i \in S} x_i \equiv 1 \pmod 2$? " for an arbitrary subset $S \subseteq [n]$. We call such queries parity queries.

For a parity decision tree P_f for f, let $C(P_f, x)$ denote the number of parity queries made by P_f on input x. The parity decision tree complexity of f is $D_\oplus(f) = \min_{P_f} \max_x C(P_f, x)$.

Note that $D_\oplus(f) \leq D(f)$ as the queries made by a usual decision tree, "is $x_i = 1$?, " are also valid parity queries. Here $D(f)$ denotes the deterministic decision tree complexity of f

A bounded error randomized parity decision tree $R^f_\oplus$ is a probability distribution over all deterministic decision trees such that for every input, the expected error of the algorithm is bounded by $1/3$. The cost $C(R^f_\oplus, x)$ is the highest possible number of queries made by $R^f_\oplus$ on x, and the bounded error randomized decision tree complexity of f is $R_\oplus(f) = \min_{R^f_\oplus} \max_x C(R^f_\oplus, x)$

For a Boolean function f, it turns out that $R_\oplus(f)$ can be lower bounded by the randomized communication complexity of the so-called XOR function $f(x \oplus y)$ (See [24] for the defintion of randomized communication complexity and XOR functions). So we have the following lemma.

Lemma 2.

$$R_\oplus(f) \geq \frac{1}{2} RCC(f(x \oplus y)).$$

Proof. Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$ on n consider the communication game where x is with Alice and y is with Bob and they want to compute

$f(x \oplus y)$ with error bounded by 1/3. Let $RCC(f(x \oplus y))$ denote the randomized communication complexity of this communication game.
Given a randomized parity decision tree $R^f_\oplus$, Alice and Bob can convert it into a protocol by simulating the parity queries made by $R^f_\oplus$ by two bits of communication, and thus the inequality follows.

3 Property testing and parity trees

In this section we describe a relation between the testing complexity of a property of linear/quadratic functions, and the parity decision tree complexity of an associated function. We remark that such connections have been observed before in the case of linear functions, though, to the best of our knowledge, such an observation had not been made for quadratic functions before our work.

3.1 Parity trees and linear functions

Let $\mathcal{L}$ be the set of all linear functions from $\{0,1\}^n$ to $\{0,1\}$. Let $e_i \in \{0,1\}^n$ denote the Boolean string whose i^{th} bit is 1 and all other bits are 0. For any linear function f let us define a string $B(f) \in \{0,1\}^n$ such that the i^{th} bit of $B(f)$ is 1 iff $f(e_i) = 1$. The following lemma is easy to prove:

Lemma 3. *The map $B : \mathcal{L} \to \{0,1\}^n$ gives a bijection between the set $\mathcal{L}$ and strings of length n.*

Now let $\mathcal{P} \subseteq \mathcal{L}$ be a set of linear functions. Given a linear function f we want a tester $\mathcal{T}$ that makes queries to the truth table of f and distinguishes whether f is in $\mathcal{P}$ or is ϵ-far from $\mathcal{P}$. Let us define a set $S_\mathcal{P} \subseteq \{0,1\}^n$ as follows:

$$S_\mathcal{P} = \{B(f) \mid f \in \mathcal{P}\}$$

Lemma 4. *For any $\mathcal{P} \subseteq \mathcal{L}$ and any $f \in \mathcal{L}$ we have:*

- *$f \in \mathcal{P}$ if and only if $B(f) \in S_\mathcal{P}$ and*
- *f is 1/2-far from $\mathcal{P}$ if and only if $B(f) \notin S_\mathcal{P}$*

We omit the proof of Lemma 4 as it follows directly from Lemma 3 and Observation 6.

Thus by Lemma 4, testing where f is in $\mathcal{P}$ or is 1/2-far from $\mathcal{P}$ is exactly same as deciding if $B(f) \in S_\mathcal{P}$.

Furthermore, we can translate the queries made by the tester $\mathcal{T}$ to the truth table of f into parity queries to the string $B(f)$, and vice-versa. Since f is linear, we have $f(x) = \bigoplus_i x_i \cdot f(e_i)$ Let $S_x := \{i \mid x_i = 1\}$. Thus, whenever $\mathcal{T}$ queries f at x, it can be equivalently viewed as the query $\bigoplus_{i \in S_x} (B(f))_i$ made to $B(f)$.

Consider the Boolean function $E_\mathcal{P} : \{0,1\}^n \to \{0,1\}$, where $E_\mathcal{P}(x) = 1$ iff $B^{-1}(x) \in \mathcal{P}$. Observe that deciding "is $x \in S_\mathcal{P}$?" is same as deciding "is $E_\mathcal{P}(x) = 1$?" Thus we have:

Theorem 9. *There is a tester that makes q queries for distinguishing if a linear function f satisfies the property $\mathcal{P}$ or is $1/2$-far from satisfying $\mathcal{P}$ if and only if there is a randomized parity decision that makes q queries for deciding $E_{\mathcal{P}}$. Equivalently, $Q_1(\mathcal{P}) = R_{\oplus}(E_{\mathcal{P}})$.*

3.2 Parity trees and quadratic functions

To prove a result like Theorem 9 for quadratic functions, we follow almost the same strategy as before.
Let $\mathcal{G}_n \subseteq \{0,1\}^{n^2}$ denote the set of graphs on n vertices[7]. For any homogenous quadratic function $f \in \mathcal{Q}_0$ let us define a graph $G(f)$ with vertex set $[n]$ such that the edge $\{i,j\}$ is present in $G(f)$ iff $x_i x_j$ occurs as a monomial when f is expressed as a polynomial over $\mathbb{F}_2$.

The following observation follows from the way we defined $G(f)$.

Observation 10 *The map $G : \mathcal{Q}_0 \to \mathcal{G}_n$ is a bijection.*

Let $\mathcal{P} \subseteq \mathcal{Q}$ be a property of quadratic functions. We define $S_{\mathcal{P}} \subseteq \mathcal{G}$ as follows:

$$S_{\mathcal{P}} = \{G(f) \mid f \in \mathcal{P} \cap \mathcal{Q}_0\}.$$

Also, the following lemma can be proved by using Observation 10 and 6.

Lemma 5. *For any $\mathcal{P} \subseteq \mathcal{Q}$ and any $f \in \mathcal{Q}_0$ we have:*

- *$f \in \mathcal{P}$ if and only if $G(f) \in S_{\mathcal{P}}$ and*
- *f is $1/4$-far from $\mathcal{P}$ if and only if $G(f) \notin S_{\mathcal{P}}$*

Thus, the above lemma says that testing whether a given $f \in \mathcal{Q}_0$ is in $\mathcal{P}$ or $1/4$-far from $\mathcal{P}$ is exactly the same as deciding if $G(f)$ is in $S_{\mathcal{P}}$.

Let $\mathcal{A}$ be an algorithm that tests if a $f \in \mathcal{Q}_0$ is in $\mathcal{P}$ or $1/4$-far from it. We now describe how to translate queries made by $\mathcal{A}$ to the truth table of f to parity queries to the adjacency matrix of the graph $G(f)$.

Given $y \in \{0,1\}^n$ and a graph G on the vertex set $[n]$, we denote by $G[y]$ the induced graph on the vertex set $\{i|\ y_i = 1\}$. It is not hard to see that the value $f(y)$ is exactly the parity of the number of edges in $G(f)[y]$. Thus, any query to the truth table of f can be translated to a parity query to the adjacency matrix of $G(f)$.

The only difference is that unlike in the case of linear functions, the translation works in only one direction. To be more precise, an arbitrary parity query to the adjacency matrix of $G(f)$ cannot be translated into a query to the truth table of f.

Consider the Boolean function $E_{\mathcal{P}} : \mathcal{G}_n \to \{0,1\}$, where $E_{\mathcal{P}}(H) = 1$ iff $G^{-1}(H) \in \mathcal{P}$. Observe that deciding "is $H \in S_{\mathcal{P}}$?" is same as deciding "is $E_{\mathcal{P}}(H) = 1$?" Combining the observations made above, we have:

[7] Note that the set of $n \times n$ matrices over $\mathbb{F}_2$ can be naturally identified with the set $\{0,1\}^{n^2}$

Lemma 6. *There is an adaptive tester that makes q queries for distinguishing if a given $f \in \mathcal{Q}_0$ satisfies the property $\mathcal{P}$ or is $1/4$-far from satisfying $\mathcal{P}$ only if there is a randomized parity decision that makes q queries for deciding $E_{\mathcal{P}}$. Equivalently, $Q_2(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$.*

Combining Lemma 6 and Observation 7, we get a more general result:

Theorem 11. *There is an adaptive tester that makes q queries for distinguishing if a given f satisfies the property $\mathcal{P}$ or is $1/4$-far from satisfying $\mathcal{P}$ only if there is a randomized parity decision tree that makes q queries for deciding $E_{\mathcal{P}}$. Equivalently, $Q^{1/4}(\mathcal{P}) \geq R_{\oplus}(E_{\mathcal{P}})$.*

4 Characterizing testable properties of linear functions

In this section we give a characterization of properties of linear functions that are testable using only constant number of queries.

Recall that for a Boolean[8] function f, $||\widehat{f}||_1^{\epsilon}$ denotes the minimum possible $||\widehat{g}||_1$ over all g such that $|f(x) - g(x)| \leq \epsilon$ for all x.

We use the following lemma:

Lemma 7.

$$O(\log ||\widehat{f}||_1^{1/4}) \leq R_{\oplus}(f) \leq O((||\widehat{f}||_1^{1/4})^2)$$

Proof. For the first inequality, we obtain from Lemma 2 that $RCC(f(x \oplus y)) \leq 2R_{\oplus}(f)$. Now, it is well known that $RCC(f(x \oplus y)) \geq O(\log ||\widehat{f}||_1^{1/4})$ (see for instance [24]) and thus we have

$$R_{\oplus}(f) \geq 1/2 \cdot RCC(f(x \oplus y)) \geq O(\log ||\widehat{f}||_1^{1/4})$$

To see the second inequality, we will construct a randomized parity decision tree[9] $\mathcal{T}$ with query complexity $O((||\widehat{f}||_1^{1/4})^2)$ that computes f. Let $g : \{0,1\}^n \to \mathbb{R}$ be a function that pointwise $1/4$-approximates f (i.e. for all x, $|f(x) - g(x)| \leq 1/4$) such that $||\widehat{g}||_1$ is the minimum among all functions that $1/4$-approximate f. Let $\mathcal{D}_g$ denote a distribution on subsets of $[n]$ such that a set S has probability $|\hat{g}(S)|/||\widehat{g}||_1$.

We define the randomized parity decision tree $\mathcal{T}$ as follows. $\mathcal{T}$ makes d (the parameter will be fixed later) random parity queries $S_1, S_2 \ldots S_d$, such that each S_i is distributed according to $\mathcal{D}_g$. Let $X_1, X_2, \ldots X_d$ be random variables such that

$$X_i = \frac{\text{sign}(\hat{g}(S_i))(-1)^{\sum_{j \in S_i} x_j}}{||\widehat{g}||_1}$$

Here the sign function sign(x) outputs -1 is $x < 0$, and 1 otherwise. Finally, the tree outputs sign$(\sum_{i=1}^{d} X_i)$.

[8] For the purpose of this section, it will be convenient to assume that the range of a Boolean function is $\{-1, +1\}$.

[9] We shall assume that $\mathcal{T}$'s range is $\{-1, +1\}$

The first thing to note is that

$$\mathbb{E}[X_i] = \sum_{S \subseteq [n]} \frac{\text{sign}(\hat{g}(S_i))(-1)^{\sum_{j \in S_i} x_j}}{||\widehat{g}||_1} \frac{|\hat{g}(S)|}{||\widehat{g}||_1} = \frac{g(x)}{(||\widehat{g}||_1)^2}$$

Let $X = \sum_{i=1}^{d} X_i$. Then, $\mathbb{E}[X] = d \cdot g(x)/(||\widehat{g}||_1)^2$. Setting $d = 100 \cdot (||\widehat{g}||_1)^2$, we get $\mathbb{E}[X] = 100 \cdot g(x)$.

Now each X_i is bounded and lies in $[-1/||\widehat{g}||_1, +1/||\widehat{g}||_1]$. Thus by Hoeffding's inequality we have

$$\Pr[|X - \mathbb{E}[X]| \geq 50] \leq \exp\left(\frac{-2 \cdot (50)^2}{400}\right) = \exp\left(\frac{-25}{2}\right). \tag{1}$$

Since g pointwise 1/4-approximates f, $\text{sign}(g(x)) = \text{sign}(f(x)) = f(x)$. Also, it is easy to see that, if $|X - \mathbb{E}[X]| \leq 50$, $\text{sign}(X) = \text{sign}(\mathbb{E}[X]) = \text{sign}(g(x))$. Thus, by Equation 1, $\text{sign}(X) = f(x)$ with very high probability.

The above argument shows that $\mathcal{T}$ is a randomized decision tree that computes f with high probability and makes $O((||\widehat{g}||_1)^2) = O((||\widehat{f}||_1^{1/4})^2)$ queries. This proves that

$$R_{\oplus}(f) \leq O((||\widehat{f}||_1^{1/4})^2)$$

Let $\mathcal{P}$ be a property of linear functions, and $Q_1(\mathcal{P})$ denote the query complexity of testing $\mathcal{P}$ when the input function is promised to be linear. Then, from the above lemma and Theorem 9, we have that

$$O(\log ||\widehat{E_{\mathcal{P}}}||_1^{1/4}) \leq Q_1(\mathcal{P}) \leq O((||\widehat{E_{\mathcal{P}}}||_1^{1/4})^2)$$

Using Observation 7 and 8, we then get, for $\epsilon \in (0, 1/4)$:

$$O(\log ||\widehat{E_{\mathcal{P}}}||_1^{1/4}) \leq Q^{1/4}(\mathcal{P}) \leq Q^{\epsilon}(\mathcal{P}) \leq O_{\epsilon}\left((||\widehat{E_{\mathcal{P}}}||_1^{1/4})^2 \log\left(||\widehat{E_{\mathcal{P}}}||_1^{1/4}\right)\right)$$

Thus, we can conclude the following.

Theorem 12. *A property $\mathcal{P}$ of linear functions is testable using constant number of queries if and only if $||\widehat{E_{\mathcal{P}}}||_1^{1/4}$ is constant.*

5 Testing k-linearity

In this section we apply the result from Section 3 to prove a lower bound for testing k-linearity. Recall that a function is k-linear if it can be expressed as $\sum_{i \in S} x_i \pmod 2$ for some S such that $|S| = k$. Let $\mathcal{P}$ denote the set of k-linear functions on n variables.

Let $E_k : \{0,1\}^n \to \{0,1\}$ denote the Boolean function that outputs 1 if and only if the number of 1s is *exactly* k.

Recall a notation from Section 3: for any linear function f we can define a string $B(f) \in \{0,1\}^n$ such that $B(f)_i = 1$ iff $f(e_i) = 1$. We observe the following:

Observation 13 *A Boolean function f is k-linear if and only if $B(f)$ has exactly k 1s.*

Thus, $E_{\mathcal{P}}$ is exactly the function E_k. Using Theorem 9 we have the following lemma.

Lemma 8. $Q_1(\mathcal{P}) = R_{\oplus}(E_k)$

Thus, if we can obtain a lower bound of $\Omega(k \log k)$ on the randomized parity decision tree complexity of E_k then we would obtain a tight bound for adaptive k-linearity testing (This would follow from Observation 7: $Q^{1/2}(\mathcal{P}) \geq Q_1(\mathcal{P})$). Unfortunately we are unable to obtain such a lower bound yet. Instead we can obtain a lower bound of $\Omega(k)$ that matches the previous known lower bound for k-linearity testing [7].

Using Lemma 2, we have that $R_{\oplus}(E_k) \geq \frac{1}{2} RCC(E_k(x \oplus y))$. Furthermore, Huang et al. [22] show that[10]:

Lemma 9. $RCC(E_k(x \oplus y)) = \Omega(k)$

Using Lemma 8 and 9, we have $Q_1(\mathcal{P}) = \Omega(k)$. Finally, Observation 7 gives us $Q^{1/2}(\mathcal{P}) = \Omega(k)$:

Theorem 14. *Any adaptive two-sided tester for $1/2$-testing k-linearity must make $\Omega(k)$ queries.*

Thus we obtain a lower bound of $\Omega(k)$ using the lower bound for the randomized communication complexity of the XOR function $E_k(x \oplus y)$. Note that using this method we cannot expect to obtain a better lower bound as there is a upper bound of $O(k)$ on the communication complexity. But there is hope that one may be able to obtain a better lower bound for the parity decision tree complexity of E_k directly.

On the other hand, if one is able to construct a randomized parity decision tree of depth $O(k)$ for deciding E_k, Lemma 8 immediately implies a tester[11] for k-linearity that makes $O(k)$ queries.

6 Testing affine isomorphism to the inner product function

The main result of this section is that $1/4$-testing affine isomorphism to the inner product function $\mathbf{IP}_n(x)$[12] requires $\Omega(n^2)$ queries. As a corollary, we show that testing the set of Bent functions requires $\Omega(n^2)$ queries.

Let $\mathcal{B}$ denote the set of Bent functions. The following is an easy consequence of Dickson's lemma (We give a proof in Appendix C.2):

[10] Actually, Huang et al. show that $RCC(E_{>k}(x \oplus y)) = \Omega(k)$, but their proof can be used to obtain the same lower bound for $RCC(E_k(x \oplus y))$.

[11] See the remark in Section 2.2

[12] For the rest of the section we shall assume that the number of variables n is even

Lemma 10. *Let $Q(n)$ denote the the query complexity of $1/4$-testing affine isomorpism to the inner product function. Then $Q^{1/4}(\mathcal{B} \cap \mathcal{Q}) = O(Q(n))$.*

Thus, it is sufficient to lower bound $Q^{1/4}(\mathcal{B} \cap \mathcal{Q})$. In fact, by Observation 7, $Q^{1/4}(\mathcal{B} \cap \mathcal{Q}) \geq Q_2(\mathcal{B} \cap \mathcal{Q})$, and thus we can restrict out attention to lower bounding $Q_2(\mathcal{B} \cap \mathcal{Q})$

Recall from Section 3 that we can associate a graph $G(f)$ with every function $f \in \mathcal{Q}_0$. We now state a well-known criterion that follows from a result due to Rothaus [28] for a quadratic function to be Bent.

Lemma 11. *A function $f \in \mathcal{Q}_0$ is Bent iff the adjacency matrix of $G(f)$ is nonsingular.*

We give a proof of Lemma 11 in Appendix B.

Recall from Section 3 that $\mathcal{G}_n \subseteq \{0,1\}^{n^2}$ is the set of graphs on the vertex set $[n]$. Let $\mathcal{P} := \mathcal{B} \cap \mathcal{Q}$, and let $E_n : \mathcal{G}_n \to \{0,1\}$ be a Boolean function such that $E_n(G) = 1$ iff the adjacency matrix of G is nonsingular. Due to Lemma 11, $E_{\mathcal{P}}$ turns out to be exactly equal to E_n. Combining with Theorem 5, we have

Lemma 12. $Q_2(\mathcal{P}) \geq R_{\oplus}(E_n)$

As in the case of E_k, analyzing the decision tree complexity of E_n directly is hard, and we turn to communication complexity. Lemma 2 tells us that $R_{\oplus}(E_n) \geq \frac{1}{2} RCC(E_n(x \oplus y))$.

Let $M_n(\mathbb{F}_2)$ denote the set of $n \times n$ matrices over $\mathbb{F}_2$, and $Det_n : M_n(\mathbb{F}_2) \to \{0,1\}$ be the function such that $Det_n(A) = 1$ iff $A \in M_n(\mathbb{F}_2)$ is nonsingular. The following result from [30] analyzes the communication complexity of Det_n.

Lemma 13. $RCC(Det_n(x \oplus y)) = \Omega(n^2)$

It turns out that the communication complexity of Det_n relates to that of E_n.

Lemma 14. $= RCC(Det_n(x \oplus y)) \leq RCC(E_{2n}(x \oplus y))$

Proof. Let $A \in M_n(\mathbb{F}_2)$. Consider the $2n \times 2n$ matrix A' given by $\begin{pmatrix} 0 & A^t \\ A & 0 \end{pmatrix}$. $A' \in \mathcal{G}_{2n}$ by construction and it can be easily verified that A' is nonsingular iff A is nonsingular.
Now, let the inputs to Alice and Bob be A and B respectively. Since $(A \oplus B)' = A' \oplus B'$, $Det_n(A \oplus B) = 1$ iff $E_{2n}((A \oplus B)') = 1$ iff $E_{2n}(A' \oplus B') = 1$. Thus, to determine if $Det_n(A \oplus B)$ is 1, Alice and Bob can construct A' and B' from A and B respectively, and run the protocol for E_{2n} on A' and B'. This completes the proof.

Thus, using Lemma 13, we have $RCC(E_n(x \oplus y)) = \Omega(n^2)$. Using Lemma 2 and Lemma 12, we have that $Q_2(\mathcal{P}) = \Omega(n^2)$.
Thus, based on eariler observations, we can conclude:

Theorem 15. *Any adaptive two-sided tester for $1/4$-testing affine isomorphism to the inner product function $\mathbf{IP}_n(x)$ requires $\Omega(n^2)$ queries.*

Corollary 2 tells us that our result is tight. Thus, $\mathbf{IP}_n(x)$ is an example of a function for which the trivial bound for testing affine isomorphism is the best possible.

We have shown that $Q^{1/4}(\mathcal{B} \cap \mathcal{Q}) = \Omega(n^2)$. We now state a result due to Chen et al.(Lemma 2 in [15]) in a form that is suitable for application in our setting:

Lemma 15. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two properties of Boolean functions that have testers (possibly two-sided) T_1 and T_2 respectively. Let the query complexity of tester T_i be $q_i(\epsilon, n)$. Suppose $dist(\mathcal{P}_1 \setminus \mathcal{P}_2, \mathcal{P}_2 \setminus \mathcal{P}_1) \geq \epsilon_0$ for some absolute constant ϵ_0. Then, $\mathcal{P}_1 \cap \mathcal{P}_2$ is ϵ-testable with query complexity*

$$O(max\{q_1(\epsilon, n), q_1(\frac{\epsilon_0}{2}, n)\} + max\{q_2(\epsilon, n), q_2(\frac{\epsilon_0}{2}, n)\})$$

In its original form, the lemma has been proven for the case when T_1, T_2 are one-sided, and q_1, q_2 are independant of n, but the proof can be easily adapted to this more general setting. We discuss this in Appendix D.

Another easy consequence of Dickson's lemma is the following (We give a proof in Appendix C.3):

Lemma 16. *Let f, g be Boolean functions. If $f \in \mathcal{B} \setminus \mathcal{Q}$ and $g \in \mathcal{Q} \setminus \mathcal{B}$, then $dist(f, g) \geq 1/4$.*

We are now ready to prove a lower bound for testing Bent functions.

Theorem 16. *Any adaptive two-sided tester that $1/8$-tests the set of Bent functions requires $\Omega(n^2)$ queries.*

Proof. It is well known via [2] that $\mathcal{Q}$ is testable with constant number of queries (say $q_1(\epsilon)$). Suppose there is a tester that tests $\mathcal{B}$ using $q_2(\epsilon, n)$ queries. From Lemma 16, we know that $dist(\mathcal{B} \setminus \mathcal{Q}, \mathcal{Q} \setminus \mathcal{B}) \geq \frac{1}{4}$. Thus, by Lemma 15, we have that there is a tester that makes $O(max\{q_1(\epsilon), q_1(\frac{1}{8})\} + max\{q_2(\epsilon, n), q_2(\frac{1}{8}, n)\})$ queries to ϵ-test $\mathcal{B} \cap \mathcal{Q}$.

Setting $\epsilon = \frac{1}{4}$, we have a tester that makes $O(q_1(\frac{1}{8}) + q_2(\frac{1}{8}, n))$ queries to test if a given f is in $\mathcal{B} \cap \mathcal{Q}$, or $1/4$-far from it. Since $Q^{1/4}(\mathcal{B} \cap \mathcal{Q}) = \Omega(n^2)$ and $q_1(\frac{1}{8})$ is a constant, we get $q_2(\frac{1}{8}, n) = \Omega(n^2)$, which completes the proof.

References

1. Alon, N., Fischer, E., Newman, I., Shapira, A.: A combinatorial characterization of the testable graph properties: It's all about regularity. SIAM J. Comput. 39(1), 143–167 (2009)
2. Alon, N., Kaufman, T., Krivelevich, M., Litsyn, S., Ron, D.: Testing low-degree polynomials over gf(2). In: RANDOM-APPROX 2003. pp. 188–199
3. Bhattacharyya, A., Fischer, E., Hatami, H., Hatami, P., Lovett, S.: Every locally characterized affine-invariant property is testable. In: Proceedings of the 45th annual ACM symposium on Symposium on theory of computing. pp. 429–436. STOC '13, ACM, New York, NY, USA (2013), http://doi.acm.org/10.1145/2488608.2488662

4. Bhattacharyya, A., Grigorescu, E., Shapira, A.: A unified framework for testing linear-invariant properties. In: In Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science. pp. 478–487 (2010)
5. Bhrushundi, A.: On testing bent functions. Electronic Colloquium on Computational Complexity (ECCC) 20, 89 (2013)
6. Blais, E.: Testing juntas nearly optimally. In: Proc. ACM symposium on the Theory of computing. pp. 151–158. ACM, New York, NY, USA (2009)
7. Blais, E., Brody, J., Matulef, K.: Property testing via communication complexity. Proc. CCC (2011)
8. Blais, E., Kane, D.M.: Tight bounds for testing k-linearity. In: APPROX-RANDOM. pp. 435–446 (2012)
9. Blais, E., Weinstein, A., Yoshida, Y.: Partially symmetric functions are efficiently isomorphism-testable. In: FOCS. pp. 551–560 (2012)
10. Blum, M., Luby, M., Rubinfeld, R.: Self-testing/correcting with applications to numerical problems. In: STOC. pp. 73–83 (1990)
11. Buhrman, H., García-Soriano, D., Matsliah, A., de Wolf, R.: The non-adaptive query complexity of testing k-parities. CoRR abs/1209.3849 (2012)
12. Chakrabarty, D., Seshadhri, C.: A o(n) monotonicity tester for boolean functions over the hypercube. CoRR abs/1302.4536 (2013)
13. Chakraborty, S., Fischer, E., García-Soriano, D., Matsliah, A.: Junto-symmetric functions, hypergraph isomorphism and crunching. In: IEEE Conference on Computational Complexity. pp. 148–158 (2012)
14. Chakraborty, S., Kulkarni, R.: Testing properties of linear functions via parity decision trees (2013), (Unpublished)
15. Chen, V., Sudan, M., Xie, N.: Property testing via set-theoretic operations. In: ICS. pp. 211–222 (2011)
16. Fischer, E.: The art of uninformed decisions: A primer to property testing. Science 75, 97–126 (2001)
17. Fischer, E., Kindler, G., Ron, D., Safra, S., Samorodnitsky, A.: Testing juntas. Journal of Computer and System Sciences 68(4), 753 – 787 (2004), special Issue on FOCS 2002
18. Fischer, E., Lehman, E., Newman, I., Raskhodnikova, S., Rubinfeld, R., Samorodnitsky, A.: Monotonicity testing over general poset domains. In: STOC. pp. 474–483 (2002)
19. Goldreich, O.: On testing computability by small width obdds. In: APPROX-RANDOM. pp. 574–587 (2010)
20. Grigorescu, E., Wimmer, K., Xie, N.: Tight lower bounds for testing linear isomorphism. In: APPROX-RANDOM. pp. 559–574 (2013)
21. Håstad, J., Wigderson, A.: The randomized communication complexity of set disjointness. Theory of Computing 3(1), 211–219 (2007)
22. Huang, W., Shi, Y., Zhang, S., Zhu, Y.: The communication complexity of the hamming distance problem. Inf. Process. Lett. 99(4), 149–153 (2006)
23. Kaufman, T., Sudan, M.: Algebraic property testing: the role of invariance. In: STOC. pp. 403–412 (2008)
24. Lee, T., Shraibman, A.: Lower bounds in communication complexity. Foundations and Trends in Theoretical Computer Science 3(4), 263–398 (2009)
25. Lidl, R., Niederreiter, H.: Finite fields / Rudolf Lidl, Harald Niederreiter ; foreword by P.M. Cohn. Cambridge University Press Cambridge ; New York, 2nd ed. edn. (1997), http://www.loc.gov/catdir/toc/cam029/96031467.html

26. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes (North-Holland Mathematical Library). North Holland Publishing Co. (Jun 1988), http://www.worldcat.org/isbn/0444851933
27. Neumann, T.: Bent functions (2006), (Master's thesis)
28. Rothaus, O.: On bent functions. Journal of Combinatorial Theory, Series A 20(3), 300 – 305 (1976), http://www.sciencedirect.com/science/article/pii/0097316576900248
29. Rubinfeld, R., Shapira, A.: Sublinear time algorithms. Electronic Colloquium on Computational Complexity (ECCC) 11(013) (2011)
30. Sun, X., Wang, C.: Randomized communication complexity for linear algebra problems over finite fields. In: STACS. pp. 477–488 (2012)
31. Wimmer, K., Yoshida, Y.: Testing linear-invariant function isomorphism. In: ICALP (1). pp. 840–850 (2013)
32. Zhang, Z., Shi, Y.: On the parity complexity measures of boolean functions. Theor. Comput. Sci. 411(26-28), 2612–2618 (2010)

A Proof of Observation 8

Let $\mathcal{A}$ be a tester (possibly adaptive) that tests the property $\mathcal{P}$ under the promise that the input is a linear Boolean function. Suppose $\mathcal{A}$ makes Q queries in the worst case.

Let $\epsilon \in (0, 1/4)$. We now build a tester $\mathcal{A}'$ to ϵ-test $\mathcal{P}$ even when there is no promise on the input. On input f, $\mathcal{A}'$ first runs a linearity test [10] and ensures that the function f is ϵ-close to a linear function with high probability. After that $\mathcal{A}'$ simulates $\mathcal{A}$ except that when $\mathcal{A}$ queries f at a particular x, instead of querying f at x directly, $\mathcal{A}'$ obtains the value of $L_f(x)$ by self correcting, where L_f is the unique linear function closest to f (L_f is unique since $\epsilon \in (0, 1/4)$). By using standard self-correcting techniques one can ensure that if f is ϵ-close to L_f, by making $O_\epsilon(\log Q)$ queries, one can obtain the value of L_f at x with probability $O(1 - 1/O_\epsilon(Q))$. Since $\mathcal{A}$ anyway makes at most Q queries, by union bound, one can see that with constant probability $\mathcal{A}'$ behaves on f just as $\mathcal{A}$ would behave on L_f.

If f is ϵ-far from $\mathcal{P}$ then either f is ϵ-far from every linear function or f is ϵ-close to L_f but L_f is not in $\mathcal{P}$. In the first case the function is rejected during the linearity test and in the second case, since $\mathcal{A}$ would reject L_f, so would $\mathcal{A}'$ with high probability. And if f is in $\mathcal{P}$ then f is linear and in that case $\mathcal{A}'$ works exactly same as $\mathcal{A}$. So for any $\epsilon \in (0, 1/4)$, $\mathcal{A}'$ gives a test for the property $\mathcal{P}$, without any assumption on the input. The query complexity of $\mathcal{A}'$ is $O_\epsilon(Q \log Q)$. Thus, for all $\epsilon \in (0, 1/4)$, $Q^\epsilon(\mathcal{P}) \leq O_\epsilon(Q \log Q)$.

B Proof of Lemma 11

The following is a result due to Rothaus [28]:

Theorem 17. *Let f be a Boolean function. Then f is Bent iff every non-zero derivative $\Delta_u(f)$ of f is balanced i.e.* $\forall u \in \mathbb{F}_2^n \backslash \{0\}$, $\mathbb{E}_x \Delta_u(f) = \mathbb{E}_x (-1)^{f(x)+f(x+u)} = 0$.

Let G be a simple graph on the vertex set $[n]$, and $c : [n] \to \{0,1\}$ be an assignment of colors to the vertices. Then c is called a 2-$\oplus$-coloring of G if:

- $\exists i \in V(G)$, $c(i) = 1$
- For every vertex i, the number of 1-colored neighbours of vertex i is even.

The following is an equivalent way of looking at the Rothaus criterion for homogenous quadratic functions:

Lemma 17. *$f \in \mathcal{Q}_0$ is bent iff $G(f)$ is not 2-$\oplus$-colorable.*

Proof. ($\Rightarrow$) Suppose f is bent. For sake of contradiction, let us assume that $G(f)$ has a 2-$\oplus$-coloring $c \in \{0,1\}^n$. Let us fix some variable x_i that occurs in the polynomial representation of f. Note that f can be written as $f(x_1, \ldots, x_n) = x_i(\sum_{j \in N(i)} x_j) + f'$, where $N(i)$ denotes the neighbours of i in $G(f)$, and f' is a quadratic function which does not depend on x_i. Also, $\Delta_c(f) = \Delta_c(x_i(\sum_{j \in N(i)} x_j)) + \Delta_c(f')$.
We know that

$$\Delta_c(x_i(\sum_{j \in N(i)} x_j)) = x_i(\sum_{j \in N(i)} x_j) + (x_i + c_i)(\sum_{j \in N(i)} (x_j + c_j)).$$
$$= x_i(\sum_{j \in N(i)} c_j) + c_i(\sum_{j \in N(i)} x_j)$$

Notice that the coefficient of x_i in the above expression i.e. $\sum_{j \in N(i)} c_j$, is the parity of the number of 1-colored neighbours of i, and since c is a 2-$\oplus$-coloring, it must be zero. Thus, the derivative $\Delta_c(f)$ does not depend on x_i.
Since our choice of i was arbitrary, the above argument would imply that $\Delta_c(f)$ does not depend on any of the n variables, making it a constant. By Theorem 17, this is a contradiction since c is a non-zero direction and f was assumed to be bent.
($\Leftarrow$) This direction can be proved using a similar argument: if the derivative of f in some non-zero direction u is unbalanced, u can be interpreted as a 2-$\oplus$-coloring of $G(f)$.

It turns out that the 2-$\oplus$-colorability of a graph G can be related to the invertability of its adjacency matrix.

Lemma 18. *A simple graph G is 2-$\oplus$-colorable iff its adjacency matrix A_G is singular.*

Proof. Assume that the vertex set of G is $[n]$. The color assignment is a vector $c \in \{0,1\}^n$. For every vertex i, introduce the equation $\sum_{j \in N(i)} c_i = 0$, where $N(i)$ denotes the neighbourhood of i. This equation essentially says that the number of 1-colored neighbours of vertex i is even. The graph is 2-$\oplus$-colorable iff the above system of equations has a non-zero solution which happens iff A_G is singular.

Combining Lemma 17 and 18, we get that $f \in \mathcal{Q}_0$ is bent iff the adjacency matrix of $G(f)$ is invertible.

C Consequences of Dickson's lemma

C.1 Structure of quadratic functions

For the remainder of this section, we shall assume the number of variables n is even. An important fact that we shall use is that the function $\mathbf{IP}_n(x)$ is Bent (This follows from the criteria stated in Appendix B).
A useful fact about the Fourier transform of Boolean functions is the following:

Observation 18 *Let f be a Boolean function, and let $g = f \circ T + c$ for an invertible affine transformation T, and $c \in \mathbb{F}_2$. Then, $(|\hat{f}(S)|)_{S \subseteq [n]}$ and $(|\hat{g}(S)|)_{S \subseteq [n]}$ are the same upto permutation.*

We now state the structure theorem[13] for quadratic functions over $\mathbb{F}_2$ (Theorem 6.21, 6.30 in [25]).

Theorem 19. *For every quadratic Boolean function f, there exists an invertible affine transformation T and constants $c, a_1, a_2, \ldots a_{n/2} \in \mathbb{F}_2$ such that*

$$f \circ T = \sum_{i=1}^{n/2} a_i x_i x_{n/2+i} + c$$

Since $\mathbf{IP}_n(x) = \sum_{i=1}^{n/2} x_i x_{n/2+i}$ is Bent, we have the following:

Lemma 19. *Let f be a function of the form $\sum_{i=1}^{n/2} a_i x_i x_{n/2+i} + c$. If exactly $\frac{k}{2}$ of the a_i's are zero, f has exactly 2^{n-k} non-zero Fourier coefficients each having absolute value $\frac{1}{2^{\frac{n-k}{2}}}$.*

Putting together Theorem 19, Lemma 19 and Observation 18, we obtain a standard fact about quadratic Boolean functions.

Lemma 20. *Let p be a quadratic Boolean function. There is an even integer $k \in [n]$ such that p has exactly 2^{n-k} non-zero Fourier coefficients each having absolute value $\frac{1}{2^{\frac{n-k}{2}}}$.*

C.2 Proof of Lemma 10

As before, let $\mathcal{B}$ denote the set of Bent functions, and $\mathcal{Q}$ the set of quadratic Boolean functions.
For a Boolean function g, let $\mathcal{O}_g := \{g \circ T + c |\ T \in \mathrm{Aff}_n,\ c \in \mathbb{F}_2\}$, where Aff_n denotes the group of invertible affine transformation on $\mathbb{F}_2^n$.

Lemma 21. $B \cap \mathcal{Q} = \mathcal{O}_{IP_n}$.

[13] This is theorem is also known as Dickson's lemma.

Proof. Clearly, $\mathcal{O}_{\mathbf{IP}_n} \subseteq \mathcal{Q}$. Since $\mathbf{IP}_n$ is Bent, we have that $\mathcal{O}_{\mathbf{IP}_n} \subseteq \mathcal{B}$ (f is Bent iff $f \circ T + c$ is Bent). Thus, $\mathcal{O}_{\mathbf{IP}_n} \subseteq \mathcal{B} \cap \mathcal{Q}$.
For the other direction, let $f \in \mathcal{B} \cap \mathcal{Q}$. By Theorem 19, there exists an invertible affine transformation T and constants $c, a_1, a_2, \ldots a_{n/2} \in \mathbb{F}_2$ such that $f \circ T = \sum_{i=1}^{n/2} a_i x_i x_{n/2+i} + c$. Now, if $k/2$ of the a_i's are zero, Lemma 19 and Observation 18 will tell us that f has exactly 2^{n-k} non-zero Fourier coefficients. But since $f \in \mathcal{B}$, every Fourier coefficient is non-zero, and hence $k = 0$. Thus, $f \circ T = \sum_{i=1}^{n/2} x_i x_{n/2+i} + c$ or equivalently, $f = \mathbf{IP}_n \circ T^{-1} + c$. This completes the proof.

Let T be a tester for ϵ-testing affine isomorphism to $\mathbf{IP}_n$ with query complexity $q(n)$. We show that T can be used for ϵ-testing $\mathcal{B} \cap \mathcal{Q}$ with $O(q(n))$ queries.
Suppose the input function is f. The tester T' for $\mathcal{B} \cap \mathcal{Q}$ first runs T on f, and then on $f + 1$. If either of the tests returns a positive answer, T' accepts f, otherwise it rejects f.
In the case $f \in \mathcal{B} \cap \mathcal{Q}$, by Lemma 21, $f \in \mathcal{O}_{\mathbf{IP}_n}$, and T' accepts f since either f or $f + 1$ is isomorphic to $\mathbf{IP}_n$.
Now suppose f is ϵ-far from $\mathcal{B} \cap \mathcal{Q}$. By Lemma 21, f is ϵ-far from $\mathcal{O}_{\mathbf{IP}_n}$. This is the same as both f and $f + 1$ being ϵ-far from all functions that are isomorphic to $\mathbf{IP}_n$, and thus T' rejects f.

C.3 Proof of Lemma 16

Let $f \in \mathcal{B} \setminus \mathcal{Q}$ and $g \in \mathcal{Q} \setminus \mathcal{B}$. We want to show that $dist(f, g) \geq \frac{1}{4}$. We now compute $|\langle f, g \rangle|$:

$$
\begin{aligned}
|\mathbb{E}_x f(x) g(x)| &= |\sum_{S \subseteq [n]} \hat{f}(S)\hat{g}(S)| \\
&\leq \sum_{S \subseteq [n]} |\hat{f}(S)||\hat{g}(S)| \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{S \subseteq [n]} |\hat{g}(S)| \text{ (Since } f \text{ is Bent)}
\end{aligned}
$$

By Lemma 20, we know that for some even $k \in [n]$, exactly 2^{n-k} Fourier coefficients of g are non-zero and have value $\frac{1}{2^{\frac{n-k}{2}}}$. Thus,

$$
\sum_{S \subseteq [n]} |\hat{g}(S)| = 2^{\frac{n-k}{2}}
$$

But $k > 0$, otherwise $g \in \mathcal{B}$, which contradicts our assumption. Also, the quantity $2^{\frac{n-k}{2}}$ is maximum at $k = 2$. Thus, $|\langle f, g \rangle| \leq \frac{1}{2}$.
Note that $|1 - 2 \cdot dist(f, g)| = |\langle f, g \rangle|$. This immediately gives $\frac{1}{4} \leq dist(f, g) \leq \frac{3}{4}$, which completes the proof.

D About the proof of Lemma 15

We suggest how the proof for Proposition 2 in [15] given in Appendix B of [15] can be made to work for Lemma 15.
Note that allowing the query complexity to depend on n does not affect the proof. Thus, we only have to argue that the proof works even when T_1 and T_2 are two-sided.
Let the error probability of both T_1 and T_2 be bounded by δ. The soundness analysis of the proof goes through as it is: when an input function is far from $\mathcal{P}_1 \cap \mathcal{P}_2$, the tester T rejects with error at most δ. For the completness, if the given function is in $\mathcal{P}_1 \cap \mathcal{P}_2$, T accepts with error at most $2 \cdot \delta$. Choosing δ to be $1/6$, ensures that the overall error is bounded by $1/3$.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de