2-TRANSITIVITY IS INSUFFICIENT FOR LOCAL TESTABILITY

Elena Grigorescu, Tali Kaufman, and Madhu Sudan

Abstract. A basic goal in Property Testing is to identify a minimal set of features that make a property testable. For the case when the property to be tested is membership in a binary linear error-correcting code, Alon, Kaufman, Krivelevich, Litsyn and Ron (Transactions on Information Theory, 2005) had conjectured that the presence of a *single* low weight codeword in the dual, and "2-transitivity" of the code (i.e., the code being invariant under a 2-transitive group of permutations on the coordinates of the code) suffice to get local testability. We refute this conjecture by giving a family of error correcting codes where the coordinates of the codewords form a large field of characteristic two, and the code is invariant under affine transformations of the domain. This class of properties was introduced by Kaufman and Sudan (STOC, 2008) as a setting where many results in algebraic property testing generalize. Our result shows a complementary virtue: This family also can be useful in producing counterexamples to natural conjectures.

Keywords. Affine invariance, locally-testable codes, 2-transitivity

Subject classification. 68Q01

1. Introduction

Property testing deals with the task of testing, in very little time, if a huge function $f : D \to R$ satisfies some property P. A property P is usually specified by the family of functions $\mathcal{F}$ which satisfy P. The goal is to design probabilistic tests which, given oracle access to f, accept if $f \in \mathcal{F}$ while rejecting with constant probability if f is *far* from $\mathcal{F}$. In addition, it is desirable that the tests make a constant number of queries (independent of $|D|$) into f, in which case they are called *local*, and hence the properties they can decide are *locally testable*.

The first modern-day property test was given by Blum, Luby and Rubinfeld (Blum *et al.* 1993). (One can count the classical polls as folklore tests for

the "majority is in favor" property.) Property testing also played a central role in results on multiprover interactive proofs Babai *et al.* (1991a,b); Feige *et al.* (1996) and PCPs Arora *et al.* (1998); Arora & Safra (1998), etc. Property testing was formalized in Rubinfeld & Sudan (1996). Most early properties were algebraic in nature and led to tests for membership in "error-correcting codes". A systematic study of property testing was started by Goldreich, Goldwasser, and Ron (Goldreich *et al.* 1998) who expanded its scope to combinatorial and graph-theoretic properties. Today a vast collection of properties are known to be locally testable very efficiently. In particular, the class of properties that can be tested with constant number of queries in the dense graph model is now almost fully understood Alon *et al.* (2009); Borgs *et al.* (2006).

In terms of testing membership in error-correcting codes however, the knowledge is not very complete. Some attempts to remedy this were proposed by Alon *et al.* (2005) who suggested that properties that satisfy sufficiently rich "invariance" conditions (along with some other obviously necessary conditions) may be testable. In particular Alon *et al.* (2005) made a formal conjecture (which we call the AKKLR-conjecture) that the property of membership in a "binary error-correcting code that is 2-transitive and has a small weight vector in its dual" may be testable with $O(1)$ locality. (We formalize their statement below). In their work Alon *et al.* (2005) they supported this conjecture by showing that it holds for the particular case of families of small degree polynomials over finite fields.

In this work, we refute the AKKLR conjecture. We show a family of error-correcting codes that satisfy nice invariance properties (and in particular 2-transitivity) and yet do not have very local tests. (See Conjecture 2.4 and Theorem 2.5 below.)

Our counterexample comes from the family of "affine-invariant" properties, whose study was introduced by Kaufman & Sudan (2008). Affine-invariant families form natural generalizations of the class of low-degree multivariate polynomials over finite fields. It is shown in Kaufman & Sudan (2008) that this class of families were locally testable for some choices of the parameters giving some weak confirmation of the AKKLR-conjecture. In this work we use other settings of parameters to give a counterexample to the AKKLR conjecture, thus complementing the results of Kaufman & Sudan (2008). Together these works highlight the power of affine-invariant families in illustrating the power and limitations of property testing in an algebraic/coding-theoretic context.

2. Preliminaries and Results

We will use $\mathbb{F}_q$ to denote the finite field of cardinality q. For a finite set D, $x \leftarrow D$ will denote a random variable distributed uniformly over D. We will mostly be interested in Boolean functions over D. We will use $\mathbb{F}_2$ (the finite field on 2 elements) to denote the range. We use $\{D \to \mathbb{F}_2\}$ to denote the set of all functions from the set D to $\mathbb{F}_2$. We will use the notation $\langle v_i \rangle_{i \in U}$ to denote a vector indexed by elements of some finite universe U. The notation $k < \infty$ means that k is finite.

2.1. Distance, Local Testability, Constraints, and Characterizations. For a finite set D and functions $f, g : D \to \mathbb{F}_2$, we define the (normalized Hamming) distance between f and g, denoted $\delta(f, g)$, to be $\Pr_{x \leftarrow D}[f(x) \neq g(x)]$. For a function $f : D \to \mathbb{F}_2$ we let the weight of f, denoted $\mathrm{wt}(f)$, be the number of $x \in D$ such that $f(x) \neq 0$. For a family of functions $\mathcal{F} \subseteq \{D \to \mathbb{F}_2\}$, define $\delta(f, \mathcal{F})$ to be $\min_{g \in \mathcal{F}}\{\delta(f, g)\}$. We say f is δ-far from $\mathcal{F}$ if $\delta(f, \mathcal{F}) > \delta$ and f is δ-close otherwise.

The central goal of this paper is to analyze the local testability of the property of membership in a given ensemble of families $\mathcal{F} = \{\mathcal{F}_n\}_n$ with $\mathcal{F}_n \subseteq \{D_n \to \mathbb{F}_2\}$, where $|D_n| \to \infty$ as $n \to \infty$. We will sometimes call $\mathcal{F}_n$ a *property* and $\mathcal{F} = \{\mathcal{F}_n\}_n$ an *ensemble of properties.*

Definition 2.1 (k-local test). *For integer k and reals $0 \leq \epsilon_1 < \epsilon_2$ and $\delta > 0$, a* $(k, \epsilon_1, \epsilon_2, \delta)$-local test *for a property $\mathcal{F}' \subseteq \{D \to \mathbb{F}_2\}$ is a probabilistic algorithm that, given oracle access to a function $f \in \{D \to \mathbb{F}_2\}$, queries f on k locations (probabilistically, possibly adaptively), and* accepts *$f \in \mathcal{F}'$ with probability at least $1 - \epsilon_1$, while* accepting *functions f that are δ-far from $\mathcal{F}'$ with probability at most $1 - \epsilon_2$. Property $\mathcal{F}'$ is called* $(k, \epsilon_1, \epsilon_2, \delta)$- locally testable *if it has a* $(k, \epsilon_1, \epsilon_2, \delta)$*-local test.*

Given an ensemble of families $\mathcal{F} = \{\mathcal{F}_n\}_n$, we say $\mathcal{F}$ is k-locally testable *if there exist $0 \leq \epsilon_1 < \epsilon_2$ and $\delta > 0$ such that for every n, $\mathcal{F}_n$ is $(k, \epsilon_1 + o(1), \epsilon_2 - o(1), \delta)$-locally testable (where the $o(1)$ term goes to zero as $n \to \infty$).*

While eventually our main theorem gives an ensemble of properties that is not testable according to the definition above, our proof first rules out a more restrictive class of local tests, called "non-adaptive", "perfect" tests. We define these notions next. A tester is *non-adaptive* if the sequence of queries it makes is independent of the function f that is being tested (and depends only on the randomness of the tester). A tester for a property $\mathcal{F} \subset \{D \to \mathbb{F}_2\}$ is *perfect* if it accepts every function $f \in \mathcal{F}$ with probability 1.

For a special class of properties called "linear" properties, the existence of a k-local test implies the existence of a non-adaptive, perfect k-local test as shown by Ben-Sasson *et al.* (2005). We describe this result next.

THEOREM 2.2 (Ben-Sasson *et al.* 2005, Theorem 3.3). *Let $\mathcal{F} = \{\mathcal{F}_n\}_n$ be an ensemble of linear properties that is k-locally testable. Then $\mathcal{F}$ is k-locally testable by a non-adaptive, perfect tester. Specifically, if $\mathcal{F}_n$ is $(k, \epsilon_1, \epsilon_2, \delta)$-locally testable, then $\mathcal{F}_n$ is $(k, 0, \epsilon_2 - \epsilon_1, \delta)$-locally testable by a non-adaptive tester.*

Theorem 2.2 will be very useful in presenting our counterexample to the AKKLR conjecture.

2.2. Linear Codes, Duals, 2-Transitivity and the Conjecture. We now move towards describing the conjecture by Alon *et al.* (2005) on the testability of a certain class of properties. The properties considered in Alon *et al.* (2005) are for membership in linear codes, and so we define these next.

A property given by a family of functions $\mathcal{F} \subseteq \{D \to \mathbb{F}_2\}$ is *linear* if for every $f, g \in \mathcal{F}$ it is the case that $f + g \in \mathcal{F}$. A natural way to test linear properties is through "low-weight" functions in their "dual". To define this notion, we let $f \cdot g = \sum_{x \in D} f(x) \cdot g(x)$ denote the *inner product* of f and g. (Here and later the summation and product are done over the field $\mathbb{F}_2$.) For a linear property $\mathcal{F}$, its *dual*, denoted $\mathcal{F}^\perp$, is the family of functions $\{g : D \to \mathbb{F}_2 \mid g \cdot f = 0, \forall f \in \mathcal{F}\}$. One way (and by the results of Ben-Sasson *et al.* (2005), essentially the only way) to test a linear property is to pick a function $g \in \mathcal{F}^\perp$ of weight at most k and verify that $f \cdot g = 0$. It is thus natural to examine the structure of the dual $\mathcal{F}^\perp$ to study the testability of $\mathcal{F}$.

DEFINITION 2.3 (2-Transitivity). *The* automorphism group *of a family $\mathcal{F} \subseteq \{D \to \mathbb{F}_2\}$, denoted* $\mathrm{Aut}(\mathcal{F})$*, is the set*

$$\{\pi : D \to D \mid \pi \text{ is a permutation and } f \in \mathcal{F} \Rightarrow f \circ \pi \in \mathcal{F}\}.$$

(It is easy to verify that this set is a group under composition of functions.)

A group G of permutations mapping D to D is 2-transitive *if for every $x, x', y, y' \in D$ such that $x \neq y$ and $x' \neq y'$, there exists $\pi \in G$ such that $\pi(x) = x'$ and $\pi(y) = y'$.*

Abusing notation slightly, we say that $\mathcal{F}$ is 2-transitive if $\mathrm{Aut}(\mathcal{F})$ *is 2-transitive.*

We are now ready to state the AKKLR-conjecture

CONJECTURE 2.4 (Alon *et al.* 2005). *For every $d \in \mathbb{N}$, there exists $k = k(d) < \infty$ such that the following holds: Let $\mathcal{F} = \{\mathcal{F}_n\}_n$ be an ensemble of properties such that for every n,*

(i) $\mathcal{F}_n^\perp$ has a non-zero function of weight at most d, and

(ii) $\mathcal{F}_n$ is 2-transitive.

Then $\mathcal{F}$ is k-locally testable.

We refute this conjecture here.

THEOREM 2.5. *For every $k < \infty$, there is an ensemble of domains $\{D_n\}_n$ and an ensemble of properties $\mathcal{F} = \{\mathcal{F}_n\}_n$ such that the following hold:*

(i) For every n, $\mathcal{F}_n^\perp$ has a non-zero function of weight at most 8.

(ii) For every n, $\mathcal{F}_n$ is 2-transitive.

(iii) $\mathcal{F}$ is not k-locally testable.

As pointed out earlier, we plan to prove this theorem by ruling out a restrictive class of tests that are non-adaptive and perfect and then using Theorem 2.2. However to use their theorem we need to ensure that our property is linear. The following theorem gives the more technical result that we show.

THEOREM 2.6. *For every $k < \infty$, there is an ensemble of domains $\{D_n\}_n$ and an ensemble of properties $\mathcal{F} = \{\mathcal{F}_n\}_n$ such that the following hold:*

(i) $\mathcal{F}$ is linear.

(ii) For every n, $\mathcal{F}_n^\perp$ has a non-zero function of weight at most 8.

(iii) For every n, $\mathcal{F}_n$ is 2-transitive.

(iv) $\mathcal{F}$ is not k-locally testable by a non-adaptive, perfect tester.

Note that Theorem 2.5 follows immediately by combining Theorem 2.6 and Theorem 2.2. So, in the rest of the paper, we focus on Theorem 2.6.

2.3. The Counterexample. Our counterexample family comes from a broad class of properties introduced by Kaufman & Sudan (2008). These are the class of "affine-invariant" families defined below.

Let $\mathbb{F}$ be some finite field and let $\mathbb{K}$ be a finite extension field of $\mathbb{F}$. For integer m, let $\mathcal{F}$ be a property of functions from $\mathbb{K}^m$ to $\mathbb{F}$. Then $\mathcal{F}$ is said to be *affine-invariant* if for every $\mathbb{K}$-affine map $A : \mathbb{K}^m \to \mathbb{K}^m$ and every $f \in \mathcal{F}$, it is the case that $f \circ A \in \mathcal{F}$.

PROPOSITION 2.7. *For every field $\mathbb{K}$ and integer n, the set of affine permutations from $\mathbb{K}^m \to \mathbb{K}^m$ is 2-transitive.*

PROOF. It suffices to prove that for every $x_1, x_2, y_1, y_2 \in \mathbb{K}^m$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists an affine permutation $A : \mathbb{K}^m \to \mathbb{K}^m$ such that $A(x_1) = y_1$ and $A(x_2) = y_2$. Let A be given by $A(x) = Mx + b$ where $M \in \mathbb{K}^{m \times m}$ and $b \in \mathbb{K}^m$. The condition that it be a permutation implies M should be non-singular, and satisfy $M(x_1 - x_2) = y_1 - y_2$, while $b = y_1 - Mx_1$. It is easy to see that a non-singular M satisfying $M(x_1 - x_2) = y_1 - y_2$ exists. □

It follows that every affine-invariant family is 2-transitive. This gives a rich family of families to examine and to seek sufficient conditions for testability. Of particular interest to us are functions formed by applying the Trace map from $\mathbb{K}$ to $\mathbb{F}$, defined below.

DEFINITION 2.8. *Let $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{K} = \mathbb{F}_{q^n}$ be finite fields. Then the Trace function* $\mathrm{Trace} = \mathrm{Trace}_{\mathbb{K},\mathbb{F}} : \mathbb{K} \to \mathbb{F}$ *is given by* $\mathrm{Trace}(x) = x + x^q + x^{q^2} + \cdots x^{q^{n-1}}$.

A fairly rich class of affine-invariant families can be constructed by starting with a carefully chosen set of monomials over m variables with coefficients from $\mathbb{K}$, and then taking their Trace and then closure under addition and affine transformations.

We get our family similarly. We will work with the fields $\mathbb{F} = \mathbb{F}_2$ and $\mathbb{K} = \mathbb{F}_{2^n}$ and we fix m to 1. We then consider monomials of the form x^{2^i+1} and take a moderate sized subset of these and take their traces and affine closures. The resulting family is described below.

The Counterexample For positive integers $k < n$, let

$$\mathcal{F}^*_{k,n} = \left\{ \begin{array}{l} f : \mathbb{F}_{2^n} \to \mathbb{F}_2 \mid \exists \beta, \beta_0, \ldots, \beta_k \in \mathbb{F}_{2^n} \text{ s.t.} \\ f(x) = \mathrm{Trace}(\beta + \beta_0 x + \sum_{i=1}^{k} \beta_i x^{2^i+1}) \end{array} \right\}.$$

In the following section we confirm that for every k, n, the family $\mathcal{F}^*_{k,n}$ is affine-invariant (and hence 2-transitive) — see Lemma 3.2. We also show the basic property that $\mathcal{F}^*_{k,n} \subseteq \mathcal{F}^*_{k+1,n}$. We also show that this containment is strict if $k < \lfloor n/2 \rfloor$. Both properties are straightforward to show.

We then use an alternate definition of the most common definition of Reed-Muller functions of order 2 (denoted $\mathrm{RM}(2, n)$) (see for instance Alon *et al.* (2005)) to show that $\mathrm{RM}(2, n)$ contains $\mathcal{F}^*_{k,n}$ for every k. The duals of these $\mathrm{RM}(2, n)$ families always contain functions of weight 8. As a result we get that the families $\mathcal{F}^*_{k,n}$ satisfy the low-dual-weight condition of the AKKLR

conjecture. We also note that these functions have large pairwise distance, i.e., for every $f \neq g \in \mathrm{RM}(2,n)$, $\delta(f,g) \geq 1/7$.

This leads us to the central question: Do these families have local testers? We show that this is not the case. This part of our analysis is novel. We show that any function in the dual of $\mathcal{F}^*_{k,n}$ of weight at most k is also a word in the dual of $\mathrm{RM}(2,n)$. We then use this to conclude that $\mathcal{F}^*_{k,n}$ has no k-local tests (Lemma 3.11).

Putting these results together we immediately get a proof of Theorem 2.6 (see Section 3.4).

3. Proof of Main Theorem

3.1. Basic properties of $\mathcal{F}^*_{k,n}$. We start with the simple claim that $\mathcal{F}^*_{k,n}$ is linear.

LEMMA 3.1. *For every k,n, $\mathcal{F}^*_{k,n}$ is linear.*

PROOF. Follows from the definition of $\mathcal{F}^*_{k,n}$ and the fact that the Trace function is linear, i.e., $\mathrm{Trace}(x+y) = \mathrm{Trace}(x) + \mathrm{Trace}(y)$. □

Next we show the affine invariance of $\mathcal{F}^*_{k,n}$.

LEMMA 3.2. *For every k,n, $\mathcal{F}^*_{k,n}$ is affine-invariant.*

PROOF. Fix an affine transformation $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ given by $A(x) = ax + b$ for $a, b \in \mathbb{F}_{2^n}$. Fix also $f \in \mathcal{F}^*_{k,n}$ given by $f(x) = \mathrm{Trace}(c + b_0 x + \sum_{i=1}^{k} b_i x^{2^i+1})$ for some $b_i,\ c \in \mathbb{F}_{2^n}$, $0 \leq i \leq k$. We need to show that $f \circ A \in \mathcal{F}^*_{k,n}$.

Note that $(f \circ A)(x) = f(ax+b) = \mathrm{Trace}(c + b_0(ax+b) + \sum_{i=1}^{k} b_i (ax+b)^{2^i+1})$. By the linearity of the Trace function, we have $(f \circ A)(x) = \mathrm{Trace}(c) + \mathrm{Trace}(b_0(ax+b)) + \sum_{i=1}^{k} \mathrm{Trace}(b_i(ax+b)^{2^i+1})$. By the linearity of $\mathcal{F}^*_{k,n}$ (Lemma 3.1), it suffices to prove that each individual summand is in $\mathcal{F}^*_{k,n}$.

This is verified easily for $\mathrm{Trace}(c)$ as well as $\mathrm{Trace}(b_0(ax+b)) = \mathrm{Trace}(b_0 ax) + \mathrm{Trace}(b_0 b)$. We thus turn to the term $\mathrm{Trace}(b_i(ax+b)^{2^i+1})$. We have

$$\begin{aligned}
&\mathrm{Trace}(b_i(ax+b)^{2^i+1}) \\
&\quad = \mathrm{Trace}(b_i(ax+b)^{2^i}(ax+b)) \\
&\quad = \mathrm{Trace}(b_i(a^{2^i}x^{2^i} + b^{2^i})(ax+b)) \\
&\quad = \mathrm{Trace}(b_i(a^{2^i+1}x^{2^i+1} + a^{2^i}bx^{2^i} + ab^{2^i}x + b^{2^i+1})) \\
&\quad = \mathrm{Trace}(b_i a^{2^i+1}x^{2^i+1}) + \mathrm{Trace}(b_i a^{2^i} b x^{2^i}) \\
&\qquad + \mathrm{Trace}(b_i a b^{2^i} x) + \mathrm{Trace}(b_i b^{2^i+1}))
\end{aligned}$$

The first, third, and fourth terms in the final expression above are again syntactically in the class $\mathcal{F}^*_{k,n}$. For the second term, note that it is of the form $\text{Trace}(\beta x^{2^i}) = \text{Trace}(\beta^2 x^{2^{i+1}}) = \cdots = \text{Trace}(\beta^{2^{n-i}} x^{2^n}) = \text{Trace}(\beta^{2^{n-i}} x)$ and thus $\text{Trace}(\beta x^{2^i}) \in \mathcal{F}^*_{k,n}$ also. Using the linearity of $\mathcal{F}^*_{k,n}$ we thus conclude that $\text{Trace}(b_i(ax+b)^{2^i+1}) \in \mathcal{F}^*_{k,n}$ and this suffices to conclude that $f \circ A \in \mathcal{F}^*_{k,n}$. □

LEMMA 3.3. *For every $k < n-1$, $\mathcal{F}^*_{k,n} \subseteq \mathcal{F}^*_{k+1,n}$. If $k < \lfloor n/2 \rfloor$ then $\mathcal{F}^*_{k,n} \subsetneq \mathcal{F}^*_{k+1,n}$.*

PROOF. The proof of the first containment follows from the definition. The second part can be derived from, for instance, (MacWilliams & Sloane 1981, Chapter 9, Theorem 7). For the sake of completeness we include a proof here.

We claim that for distinct $1 \le i, j < n/2$, the functions $\text{Trace}(x^{2^i+1})$ and $\text{Trace}(x^{2^j+1})$ have disjoint support, when viewed as polynomials of degree at most $2^n - 1$. This suffices, since it implies that the function $\text{Trace}(x^{2^k+1}) \notin \mathcal{F}^*_{k-1,n}$. We prove the claim below.

Note that the function $\text{Trace}(x^{2^i+1})$ has support on the monomials x^d for $d = 2^{i+\ell} + 2^\ell \pmod{2^n-1}$ and similarly $\text{Trace}(x^{2^j+1})$ is supported by the monomials x^d for $d = 2^{j+m} + 2^m \pmod{2^n-1}$ (here we use the phrase mod non-conventionally to refer to the unique integer in $[2^n-1]$ from the equivalence class). Suppose for contradiction that $2^{i+\ell}+2^\ell = 2^{j+m}+2^m \pmod{2^n-1}$. Then, by multiplying both sides by $2^{s-\ell}$ and reducing modulo 2^n-1, we see that we have $2^i + 1 = 2^{j+m'} + 2^{m'} \pmod{2^n-1}$ (where $m' = m - \ell$). Now we consider two cases: If $m' \le n/2$, then the unique integer between 1 and 2^n-1 equal to $2^{j+m'} + 2^{m'} \pmod{2^n-1}$ is $2^{j+m'} + 2^{m'}$. But then $2^{j+m'} + 2^{m'} \neq 2^i + 1$ unless $m' = 0$ and $i = j$ (violating distinctness of i and j). In the other case, if $m' > n/2$, then the unique integer in $[2^n-1]$ equal to $2^{m'}+2^{j+m'} > 2^{n/2} > 2^i+1$. So again the modular equivalence can not hold. This proves the claim, and thus the lemma. □

3.2. Reed-Muller of Order 2 Family. As already discussed, the counterexample family defined above is included in RM codes of order 2. This is not immediately obvious from the usual definition of RM codes as low degree polynomials.

DEFINITION 3.4.

$$\text{RM}(d,n) = \left\{ f : \mathbb{F}_2^n \to \mathbb{F}_2 | f = \sum a_{d_1,d_2,\ldots,d_n} x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}, a_i \in \mathbb{F}_2, \text{ with } \sum d_i \le d \right\}.$$

Notice that it is enough to consider $d_i \in \{0,1\}$, since over $\mathbb{F}_2$ $x^i = x$ for $i \geq 2$. Also, for positive integer d denote by $\mathrm{wt}(d)$ the number of non-zeros in the binary representation of d. We use an alternate definition of RM codes:

DEFINITION 3.5.

$$\mathcal{C}(d,n) = \left\{ f : \mathbb{F}_{2^n} \to \mathbb{F}_2 | f(x) = \mathrm{Trace}(\sum b_i x^{d_i}), b_i \in \mathbb{F}_{2^n}, \text{ with } \mathrm{wt}(d_i) \leq d. \right\}$$

LEMMA 3.6. *Definition 3.4 and 3.5 are equivalent. Specifically, for any integer $n > 0$, there exists a bijection $\pi : \mathbb{F}_2^n \to \mathbb{F}_{2^n}$ such that for every integer $d \geq 0$, $f \in \mathcal{C}(d,n)$ if and only if $f \circ \pi \in \mathrm{RM}(d,n)$.*

Lemma 3.6 is a standard result in coding theory and we refer to Ben-Sasson *et al.* (2011a) for a simple proof.

The following is now a straightforward consequence of Lemma 3.6.

PROPOSITION 3.7. *For every $k < n$, $\mathcal{F}^*_{k,n} \subseteq \mathrm{RM}(2,n)$.*

It is a well-known fact that $\mathrm{RM}(2,n)$ has weight 8 functions in its dual. We will include a proof here for completeness. We will further need the following notation. For points $x_0, x_1, \ldots, x_\ell \in \mathbb{F}_{2^n}$, define $A(x_0; x_1, \ldots, x_\ell)$ to be the affine subspace generated by $x_1, \ldots, x_\ell$ through x_0. I.e., $A(x_0; x_1, \ldots, x_\ell) = \{x_0 + \sum_{i=1}^{\ell} a_i x_i | a_1, \ldots, a_\ell \in \mathbb{F}_2\}$.

PROPOSITION 3.8. *For $n \geq 3$, $\mathrm{RM}(2,n)^\perp$ contains weight 8 functions.*

PROOF. Using the linearity of the Trace function ($\mathrm{Trace}(x+y) = \mathrm{Trace}(x) + \mathrm{Trace}(y)$) we note that it suffices to show that every $f \in \{\mathrm{Trace}(\beta), \mathrm{Trace}(\beta_0 x), \mathrm{Trace}(\beta_1 x^{2^1+1}), \ldots, \mathrm{Trace}(\beta_k x^{2^k+1})\}$ satisfies the "$\mathrm{RM}(2,n)$" constraint of weight 8: $\sum_{z \in A(x_0;x_1,x_2,x_3)} f(z) = 0$ for every $x_0, x_1, x_2, x_3 \in \mathbb{F}_{2^n}$.

For $f = \mathrm{Trace}(\beta)$ and $f = \mathrm{Trace}(\beta_0 x)$ this is straightforward, since $f(x+y) = f(x) + f(y)$ and so the $\sum_{z \in A(x_0;x_1,x_2,x_3)} f(z) = 8f(x_0) + 4f(x_1) + 4f(x_2) + 4f(x_3) = 0$ (since we are performing the arithmetic modulo 2).

Now consider $\mathrm{Trace}(\beta x^{2^i+1})$. We will show that $\sum_{z \in A(x_0;x_1,\ldots,x_3)} z^{2^i+1} = 0$. It then follows that $\sum_z \mathrm{Trace}(\beta z^{2^i+1}) = \mathrm{Trace}(\beta(\sum_z z^{2^i+1})) = \mathrm{Trace}(0) = 0$. Note further that $(x+y)^{2^i+1} = x^{2^i+1} + y^{2^i+1} + x^{2^i}y + y^{2^i}x$. Using this expansion

we have:

$$\begin{aligned}
&\sum_{z\in A(x_0;x_1,\ldots,x_3)} z^{2^i+1} \\
&= \sum_{w\in A(x_0;x_1,x_2)} w^{2^i+1} + (w+x_3)^{2^i+1} \\
&= \sum_{w\in A(x_0;x_1,x_2)} (wx_3^{2^i} + w^{2^i}x_3 + x_3^{2^i+1}) \\
&= x_3^{2^i} \sum_{w\in A(x_0;x_1,x_2)} w + x_3 \sum_{w\in A(x_0;x_1,x_2)} w^{2^i} + 0 \\
&= x_3^{2^i}(4x_0+2x_1+2x_2) + x_3(4x_0^{2^i} + 2x_1^{2^i} + 2x_2^{2^i}) \\
&= 0
\end{aligned}$$

□

COROLLARY 3.9. *For every $n > 3$ and $k < n$, $\mathcal{F}_{k,n}^{*\perp}$ contains weight 8 codewords.*

PROOF. By Proposition 3.7 $\mathcal{F}_{k,n} \subset \mathrm{RM}(2,n)$ and so $\mathrm{RM}(2,n)^\perp \subset \mathcal{F}_{k,n}^\perp$. Proposition 3.8 finishes the proof. □

Finally we show that members of the Reed-Muller family are far apart from each other. While a careful examination would probably yield a better bound on this distance, here we get a weaker bound, with a simpler argument.

PROPOSITION 3.10. *For every $f \neq g \in \mathrm{RM}(2,n)$, $\delta(f,g) \geq 1/7$.*

PROOF. Consider any function $f \in \mathrm{RM}(2,n)$ and let h be such that $\delta(f,h) < 1/14$. We claim that h uniquely specifies f: In particular the algorithm: Pick x_1, x_2, x_3 at random and output $\sum_{z\in A(x;x_1,x_2,x_3)-\{x\}} h(z)$, outputs $f(x)$ with probability at least $1 - 7\delta(f,h) > 1/2$ and thus defines f uniquely.

We thus conclude that there can not exist $f, g \in \mathrm{RM}(2,n)$ such that $\delta(f,g) < 1/7$. □

3.3. Key Lemma. Finally we move to the main lemma of the paper. The goal of this section is to prove the following lemma.

LEMMA 3.11 (Main Lemma). *Suppose $g \in (\mathcal{F}^*_{k,n})^\perp$ has weight $t \leq k$. Then $g \in \mathrm{RM}(2,n)^\perp$.*

To prove this lemma we first state three useful sub-lemmas, which yield the main lemma easily. We prove the sub-lemmas later.

The sub-lemmas refer to a positive integer m and the set $U = \{(i,j)|0 \leq i < j \leq m \text{ or } i = j = 0\}$. Note that $|U| = 1 + \binom{m+1}{2}$. We also use b_0 to denote the zero of $\mathbb{F}_{2^n}$.

LEMMA 3.12. *Let $a_1, \ldots, a_t \in \mathbb{F}_{2^n}$ be such that $\sum_{i=1}^t f(a_i) = 0$ for every $f \in \mathcal{F}^*_{k,n}$. Further, suppose there exists $g \in \mathrm{RM}(2,n)$ such that $\sum_{i=1}^t g(a_i) \neq 0$. Then there exists $m \leq t$, $\mathbb{F}_2$-linearly independent elements $b_1, \ldots, b_m \in \mathbb{F}_{2^n}$, and a non-zero vector $\langle \lambda_{ij} \rangle_{(i,j)\in U} \in \mathbb{F}_2^{|U|}$ such that $\sum_{(i,j)\in U} \lambda_{ij} f(b_i + b_j) = 0$, for every $f \in \mathcal{F}^*_{k,n}$.*

LEMMA 3.13. *Suppose $b_1, \ldots, b_m \in \mathbb{F}_{2^n}$ are $\mathbb{F}_2$-linearly independent elements, and $\langle \lambda_{ij} \rangle_{(i,j)\in U} \in \mathbb{F}_2^{|U|}$ is a non-zero vector such that $\sum_{(i,j)\in U} \lambda_{ij} f(b_i + b_j) = 0$ for every $f \in \mathcal{F}^*_{k,n}$. Then there exists a non-empty set $E \subseteq \{(i,j)|1 \leq i < j \leq m\}$ such that for every $d \in [k]$ it is the case that $\sum_{(i,j)\in E} \left(b_i^{2^d} b_j + b_j^{2^d} b_i \right) = 0$.*

Finally we show that the conclusion of the previous lemma implies that $m > k + 1$.

LEMMA 3.14. *Suppose $b_1, \ldots, b_m \in \mathbb{F}_{2^n}$ are $\mathbb{F}_2$-linearly independent elements and suppose $E \subseteq \{(i,j)|1 \leq i < j \leq m\}$ is a non-empty set such that for every $d \in [k]$, $\sum_{(i,j)\in E} \left(b_i^{2^d} b_j + b_j^{2^d} b_i \right) = 0$. Then $m > k + 1$.*

We first show that Lemma 3.11 follows from the three sublemmas.

PROOF. **(of Lemma 3.11)** Let $h \in (\mathcal{F}^*_{k,n})^\perp$ and suppose $h \notin \mathrm{RM}(2,n)^\perp$. We wish to show $t > k$. (We actually show $t > k + 1$, but we state the weaker bound for notational simplicity.)

Let $a_1, \ldots, a_t \in \mathbb{F}_{2^n}$ be the points such that $h(a_i) = 1$. By definition of $(\mathcal{F}^*_{k,n})^\perp$ we have that $0 = \sum_{x\in\mathbb{F}_{2^n}} f(x)h(x) = \sum_{i=1}^t f(a_i)$. Since $h \notin \mathrm{RM}(2,n)^\perp$, there must exist a function $g \in \mathrm{RM}(2,n)$ such that $\sum_{i=1}^t g(a_i) \neq 0$. Using Lemma 3.12 we get that there exist $m \leq t$, linearly independent points $b_1, \ldots, b_m \in \mathbb{F}_{2^n}$, and a non-zero vector $\langle \lambda_{ij} \rangle_{(i,j)\in U} \in \mathbb{F}_2^{|U|}$ such that $\sum_{(i,j)\in U} \lambda_{ij} f(b_i + b_j) = 0$ for every $f \in \mathcal{F}^*_{k,n}$, where $b_0 = 0$. Applying Lemma 3.13 we get that there exists a non-empty set $E \subseteq \{(i,j)|1 \leq i < j \leq m\}$ such that

for every $d \in [k]$ we have $\sum_{(i,j)\in E}\left(b_i^{2^d}b_j + b_j^{2^d}b_i\right) = 0$. Applying Lemma 3.14 we then get that $m > k$ and thus $t \geq m > k$ as desired. □

We now turn to proving the three sub-lemmas. Again the crucial result here is Lemma 3.14 and the other two are just to pin the problem down.

PROOF. **(of Lemma 3.12)** Let $b_1, \ldots, b_m$ be the largest linearly independent subset of points among $a_1, \ldots, a_t$ and let $g \in \mathrm{RM}(2,n)$ be the function satisfying $\sum_{i=1}^{t} g(a_i) \neq 0$.

We first claim that for every function $f \in \mathcal{F}^*_{k,n}$ at least one of the following must hold: (1) $f(0) \neq g(0)$, or (2) there exists $i \in [m]$ such that $f(b_i) \neq g(b_i)$, or (3) there exist $(i,j) \in [m] \times [m]$ such that $f(b_i + b_j) \neq g(b_i + b_j)$. To see this claim, assume otherwise, for some $f \in \mathcal{F}^*_{k,n}$. Note that we can prove, by induction on the size of the set S, that for every set $S \subseteq [m]$ we have $f(\sum_{i\in S} b_i) = g(\sum_{i\in S} b_i)$. Indeed, this is obviously true for $|S| \leq 2$. Now consider a set $S = T \cup \{i,j\}$ where $i,j \notin T$. Let $b = \sum_{\ell\in T} b_\ell$. Now note that

$$\begin{aligned} & f(b + b_i + b_j) \\ &= f(0) + f(b) + f(b_i) + f(b_j) + f(b + b_i) \\ &\qquad + f(b + b_j) + f(b_i + b_j) \\ &= g(0) + g(b) + g(b_i) + g(b_j) + g(b + b_i) \\ &\qquad + g(b + b_j) + g(b_i + b_j) \\ &= g(b + b_i + b_j), \end{aligned}$$

where the first and third inequalities follow from the fact that both $f, g \in \mathrm{RM}(2,n)$ while the middle equality is by induction. But then, we have that f and g agree on the entire subspace, which contradicts the fact that $\sum_{i=1}^{t} f(a_i) \neq \sum_{i=1}^{t} g(a_i)$. Hence our claim must be true.

Consider the set $V = \{\langle f(b_i + b_j)\rangle_{(i,j)\in U} | f \in \mathcal{F}^*_{k,n}\}$. V is a linear subspace of $\mathbb{F}_2^{|U|}$ since $\mathcal{F}^*_{k,n}$ is a linear subspace; but $V \neq \mathbb{F}_2^{|U|}$ (since in particular $\langle g(b_i + b_j)\rangle_{(i,j)\in U} \notin V$. Thus there must be a non-trivial constraint $\langle \lambda_{ij}\rangle_{(i,j)\in U}$ such that every vector $x \in V$ satisfies $\sum_{(i,j)\in U} \lambda_{ij} x_{ij} = 0$. This yields the lemma. □

PROOF. **(of Lemma 3.13)** We use the basis functions to establish this lemma. Let $b_0, b_1, \ldots, b_m$ and $\langle \lambda_{ij}\rangle_{i,j}$ be as given.

This proof also relies on the linearity of the the Trace function, and the additional fact that $\mathrm{Trace}(ax) = 0$ for every $x \in \mathbb{F}_{2^n}$ if and only if $a = 0$. (This is easily seen since $\mathrm{Trace}(ax)$ is a non-zero polynomial of degree 2^{n-1} in x, if $a \neq 0$.)

First consider the constant function $1 = \text{Trace}(\beta)$ for some $\beta \in \mathbb{F}_{2^n}$. Since $\text{Trace}(\beta) \in \mathcal{F}^*_{k,n}$ we have $\sum_{i,j} \lambda_{ij} = \sum_{i,j} \lambda_{ij}\text{Trace}(\beta) = 0$, and thus $\lambda_{00} = \sum_{(i,j)\in U-(0,0)} \lambda_{ij}$.

Next we consider the functions $\text{Trace}(\beta_0 x) \in \mathcal{F}^*_{k,n}$. We have

$$\begin{aligned} 0 &= \sum_{i,j} \lambda_{ij}\text{Trace}(\beta_0(b_i + b_j)) \\ &= \text{Trace}\left(\beta_0 \sum_{i,j} \lambda_{ij}(b_i + b_j)\right). \end{aligned}$$

Using the aforementioned property of the Trace function, we have that the above identity holds for every $\beta_0 \in \mathbb{F}_{2^n}$ only if $\sum_{i,j} \lambda_{i,j}(b_i + b_j) = 0$. Let $\tau_i = \sum_{j<i} \lambda_{ji} + \sum_{j>i} \lambda_{ij}$. (For simplicity of notation below, we will assume $\lambda_{ij} = \lambda_{ji}$.) Then we have $0 = \sum_{i,j} \lambda_{ij}(b_i + b_j) = \sum_{i=0}^{m} \tau_i b_i = \sum_{i=1}^{m} \tau_i b_i$ (where the last equality follows from $b_0 = 0$). But $b_1, \ldots, b_m$ are linearly independent over $\mathbb{F}_2$ and $\tau_i, \lambda_{ij} \in \mathbb{F}_2$, so the only way $\sum_{i=1}^{m} \tau_i b_i = 0$ is if $\tau_i = 0$ for every i. Thus we get $\lambda_{0i} = \sum_{j\neq 0} \lambda_{ji}$ for every $i \in [m]$

Finally we consider $\text{Trace}(\beta_d x^{2^d+1}) \in \mathcal{F}^*_{k,n}$ for $d \in [k]$. We have $0 = \sum_{i,j} \lambda_{ij}\text{Trace}\left(\beta_d(b_i + b_j)^{2^d+1}\right) = \text{Trace}\left(\beta_d \sum_{i,j} \lambda_{ij}(b_i + b_j)^{2^d+1}\right)$. Again, we have that the above identity holds for every $\beta_d \in \mathbb{F}_{2^n}$ only if $\sum_{i,j} \lambda_{i,j}(b_i + b_j)^{2^d+1} = 0$. Expanding $(x + y)^{2^d+1}$ as $x^{2^d+1} + y^{2^d+1} + x^{2^d}y + xy^{2^d}$, we get

$$\begin{aligned} 0 &= \sum_{i,j} \lambda_{ij}\left(b_i^{2^d+1} + b_j^{2^d+1} + b_i^{2^d}b_j + b_i b_j^{2^d}\right) \\ &= \sum_{i=1}^{m} \tau_i b_i^{2^d+1} + \sum_{1\leq i<j\leq m} \lambda_{ij}(b_i^{2^d}b_j + b_i b_j^{2^d}) \\ &= \sum_{(i,j)\in E} (b_i^{2^d}b_j + b_i b_j^{2^d}), \end{aligned}$$

where $E = \{(i,j) | 1 \leq i < j \leq m \text{ s.t. } \lambda_{ij} \neq 0\}$ as required for the lemma statement. The only remaining issue is to show that $E \neq \emptyset$.

We claim that if $E = \emptyset$ we have $\lambda_{ij} = 0$ for every i, j. For $i, j \geq 1$ this follows from the definition of E. For $i \neq 0$ and $j = 0$ this follows from the identity above that $\lambda_{0i} = \sum_{j\neq 0} \lambda_{ji} = 0$. For $i = j = 0$, we also have $\lambda_{00} = \sum_{(i,j)\in U-(0,0)} \lambda_{ij} = 0$. But this contradicts the hypothesis that $\langle \lambda_{ij} \rangle \neq 0$, and so we conclude $E \neq \emptyset$. □

PROOF. **(of Lemma 3.14)** This is the crux of our analysis and uses a mix of linear and polynomial algebra arguments. Assume for contradiction that $m \leq k+1$.

Recall we are given that for every $d \in [k]$ $\sum_{(i,j)\in E}(b_i^{2^d} b_j + b_i b_j 2^d) = 0$. Note further that we also trivially have this condition for $d = 0$, since $\sum_{(i,j)\in E}(b_i^{2^d} b_j + b_i b_j 2^d) = \sum_{(i,j)\in E}(b_i b_j + b_i b_j) = \sum_{(i,j)\in E} 0$.

For $i \in [m]$, let $\rho_i = \sum_{\{j|(i,j) \text{ or } (j,i)\in E\}} b_j$. Then we can rewrite $\sum_{(i,j)\in E}(b_i^{2^d} b_j + b_i b_j 2^d)$ as $\sum_{i=1}^m \rho_i b_i^{2^d}$ and so we have, for every $d \in \{0, 1, \ldots, k\}$ as $\sum_{i=1}^m \rho_i b_i^{2^d} = 0$.

Consider the $m \times m$ matrix $A = (a_{ij})$ with $a_{ij} = b_j^{2^{i-1}}$. Then the previous paragraph implies that $A \cdot \rho = 0$ for the column vector $\rho = \langle \rho_1, \ldots, \rho_m \rangle$. (In particular, we have that the ith entry of $A \cdot \rho$ equals $\sum_{j=1}^m b_j^{2^{i-1}} \rho_j$ which is 0 for every $i \in \{1, \ldots, k+1\} \supseteq \{1, \ldots, m\}$.)

Next we note that $\rho \neq 0$. This is true since for at least one $i \in [m]$ the summation $\sum_{\{j|(i,j) \text{ or } (j,i)\in E\}} b_j$ sums over a non-empty set of indices j (since $E \neq \emptyset$). But now the linear independence of $b_1, \ldots, b_m$ over $\mathbb{F}_2$ implies that the summation, and hence ρ_i, is non-zero.

We conclude that the matrix A is singular. We now use this fact to infer that A has a non-zero vector in its left kernel, i.e., there exists a non-zero row vector $\lambda = \langle \lambda_1, \ldots, \lambda_m \rangle$ such that $\lambda A = 0$. But now consider the polynomial $\Lambda(x) = \sum_{i=1}^m \lambda_i x^{2^{i-1}}$. Using this notation, we have $\lambda A = \langle \Lambda(b_1), \ldots, \Lambda(b_m) \rangle$. Thus the condition $\lambda A = 0$ implies that $\Lambda(b_j) = 0$ for every $j \in \{1, \ldots, m\}$.

But now, we have that $\Lambda(x)$ is a non-zero polynomial (since λ is a non-zero vector), of degree at most 2^{m-1}. Furthermore Λ is a linearized polynomial and satisfies $\Lambda(x+y) = \Lambda(x) + \Lambda(y)$. This implies that $\Lambda(b_S) = 0$ for every $S \subseteq [m]$, where $b_S = \sum_{i\in S} b_i$. The linear independence of $b_1, \ldots, b_m$ furthermore implies that the b_S's are all distinct and thus we get that Λ is a non-zero polynomial of degree at most 2^{m-1} with 2^m distinct roots, yielding the desired contradiction. □

3.4. Putting it together. We now use the main lemma of the previous subsection to claim that membership in $\mathcal{F}^*_{k,n}$ is not testable with a non-adaptive, one-sided error, k-local test. This part is more or less standard and follows, for instance, from the methods in Ben-Sasson *et al.* (2005). We include the full details for completeness.

We first summarize our arguments from the previous section in a slightly more convenient form.

LEMMA 3.15. *Fix $a_1, \ldots, a_t \in \mathbb{F}_{2^n}$. For $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ let $\pi(f) = \pi_{a_1,\ldots,a_t}(f) = \langle f(a_1), \ldots, f(a_t)\rangle$ be the projection of f to $a_1, \ldots, a_t$. Let $V \subseteq \mathbb{F}_2^t$ be the set $V = \{\pi(f) | f \in \mathcal{F}^*_{k,n}\}$, and let $W = \{\pi(f) | f \in \mathrm{RM}(2,n)\}$. If $t \leq k$, then $V = W$.*

PROOF. We first note that V and W are linear subspaces of $\mathbb{F}_2^t$. This follows from the fact that $\mathcal{F}^*_{k,n}$ and $\mathrm{RM}(2,n)$ are linear spaces. Since $\mathcal{F}^*_{k,n} \subsetneq \mathrm{RM}(2,n)$, it also follows that $V \subseteq W$. Suppose $V \neq W$. Then it follows, by linear algebra, that there exist vectors $u, w \in \mathbb{F}_2^t$ such that $u \cdot v = 0$ for every $v \in V$, $u \cdot w \neq 0$ and $w \in W$. Since $w \in W$ there exists $h \in \mathrm{RM}(2,n)$ such that $w = \pi(h)$. Let $a'_1, \ldots, a'_{t'}$ be the subsequence of $a_1, \ldots, a_t$ corresponding to indices i such that $u_i \neq 0$. Then we have $\sum_{i=1}^{t'} h(a'_i) = 1$ while $\sum_{i=1}^{t'} f(a'_i) = 0$ for every $f \in \mathcal{F}^*_{k,n}$. By Lemma 3.11 we have $t \geq t' > k$.

□

We can now prove Theorem 2.6.

PROOF. **(of Theorem 2.6)** For every n, the domain $D_n = \mathbb{F}_{2^n}$. For every n, the family of functions we work with is $\mathcal{F}_n = \mathcal{F}^*_{k,n}$.

First note, by Corollary 3.9 that for every n, $\mathcal{F}_n$ has a non-zero function in its dual of weight 8. Next, by Lemma 3.2 we also have that $\mathcal{F}_n$ is affine invariant and thus (by Proposition 2.7) 2-transitive. It remains to show that $\mathcal{F}$ is not k-locally testable. Assume $\mathcal{F}$ is t-locally testable, i.e., for all sufficiently large n there is a one-sided error, non-adaptive, tester $T = T_n$ that accepts every member of $\mathcal{F}_n$ while rejecting all functions at distance at least, say, $1/7$ from $\mathcal{F}_n$ with positive probability. We argue below that this can not happen if $t \leq k$ and $n > 2k + 1$.

Suppose $t \leq k$. Fix the coins of T to some string R and let $a_1, \ldots, a_t \in \mathbb{F}_{2^n}$ be the queries of the tester T on random string R. Let π, V and W be as in the statement of Lemma 3.15. Since the tester makes one-sided error, it follows that it must accept every pattern in V (i.e., accepts every function f such that $\pi(f) \in V$). By Lemma 3.15 we have $V = W$ and so the tester accepts every element of $\mathrm{RM}(2,n)$ also on random string R. Thus we get that every element of $\mathrm{RM}(2,n)$ is accepted with probability one by the tester T. Since $\mathrm{RM}(2,n) \neq \mathcal{F}^*_{k,n}$ for $k < \lfloor n/2 \rfloor$ (Lemma 3.3) there exists a function $h \in \mathrm{RM}(2,n) - \mathcal{F}^*_{k,n}$ that is accepted with probability one. Furthermore, by the distance of $\mathrm{RM}(2,n)$ (Proposition 3.10) and the fact that $\mathcal{F}^*_{k,n} \subseteq \mathrm{RM}(2,n)$, we have that $\delta(h, \mathcal{F}^*_{k,n}) \geq 1/7$. We conclude that the tester T accepts functions at distance $1/7$ from $\mathcal{F}^*_{k,n}$ with probability one, violating the requirement above. □

4. Conclusions

In the context of "sublinear time algorithms" it is natural to ask: How does the locality lower bound on the test scale with the complexity of the property being tested? Of course, a related question is: How should one measure the complexity of a property being tested?

A crude measure of the complexity (though certainly an upper bound) is the size of the domain. In our case, using $k = \Omega(n)$ the lower bound on the locality of the test for $\mathcal{F}^*_{k,n}$ is $\Omega(n) = \Omega(\log n)$ (where 2^n is the domain size).

But a more refined measure of the complexity of a property being tested is the logarithm of the number of functions having a given property. For $\mathcal{F}^*_{k,n}$ this number is kn. For natural and in particular, for linear, properties, it is easy to see that this measure gives an asymptotic upper bound on the locality of property testing (and indeed we would argue that this test is really not local). Compared against this refined measure, our lower bounds are actually within polynomial factors of the upper bound, which is a more accurate reflection of the tightness (or looseness) of our analysis.

Moving on to the quest for general understanding of property testing, our results do not shed as much light on testability as we would hope, but some of the questions raised in the initial version of this paper were subsequently settled leading to progress in this direction.

For instance, our work actually rules out even a local "characterizations" of the family $\mathcal{F}^*_{k,n}$. Informally, a characterization is a definition of a family in terms of local constraints satisfied by its members. In coding theoretic parlance a locally characterized property corresponds to a "low density parity check" (LDPC) code. (See (Kaufman & Sudan 2008, Definition 2.1) for a formal definition.) While this makes our result even more interesting in the coding theoretic setting, a more interesting property testing question is: Does 2-transitivity and the existence of a *local characterization* could imply property tests? This was open at the time of the initial release of this work. In subsequent work Ben-Sasson *et al.* (2011b) resolve this question in the negative by exhibiting a family of LDPC codes that is affine-invariant and yet is not testable.

A different direction suggested as open in the initial version of this paper was the possibility that there may exist an even simpler counterexample. The specific family suggested was $\mathcal{F}^?_{k,n} = \{\text{Trace}(\beta + \beta_0 x + \beta_k x^{2^k+1}) | \beta, \beta_0, \beta_k \in \mathbb{F}_{2^n}\}$. The family $\mathcal{F}^?_{k,n}$ is a "sparse" one, i.e., has $2^{O(n)}$ codewords and at the time it seemed plausible that there may exist such sparse properties that are not testable. In subsequent works, Grigorescu *et al.* (2009) and then Kaufman

& Lovett (2011) settled this question by showing all sparse properties over prime fields are locally testable. In particular, their result rules out $\mathcal{F}^{?}_{k,n}$ as a potentially simpler counterexample.

Acknowledgements

A preliminary version of this paper appeared in the 23rd IEEE Conference on Computational Complexity, 2008, and in Elena Grigorescu's PhD thesis (Grigorescu 2010). Research conducted when the authors were at MIT CSAIL. Elena Grigorescu's research was supported in part by NSF grant CCR-0829672 and NSF award 1019343 to the Computing Research Association for the Computing Innovation Fellowship Program. Tali Kaufman's research was supported in part by NSF Awards CCF-0514167 and NSF-0729011. Madhu Sudan's research was supported in part by NSF Award CCR-0514915. We thank the anonymous referees for their helpful comments.

References

Noga Alon, Eldar Fischer, Ilan Newman & Asaf Shapira (2009). A Combinatorial Characterization of the Testable Graph Properties: It's All About Regularity. *SIAM Journal of Computing* **39**(1), 143–167.

Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn & Dana Ron (2005). Testing Reed-Muller codes. *IEEE Transactions on Information Theory* **51**(11), 4032–4039.

Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan & Mario Szegedy (1998). Proof verification and the hardness of approximation problems. *Journal of the ACM* **45**(3), 501–555.

Sanjeev Arora & Shmuel Safra (1998). Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM* **45**(1), 70–122.

László Babai, Lance Fortnow, Leonid A. Levin & Mario Szegedy (1991a). Checking computations in polylogarithmic time. In *The Annual ACM Symposium on Theory of Computing*, 21–32.

László Babai, Lance Fortnow & Carsten Lund (1991b). Non-Deterministic Exponential Time has Two-Prover Interactive Protocols. *Computational Complexity* **1**(1), 3–40.

Eli Ben-Sasson, Elena Grigorescu, Ghid Maatouk, Amir Shpilka & Madhu Sudan (2011a). On Sums of Locally Testable Affine Invariant Properties.

Electronic Colloquium on Computational Complexity (ECCC) **18**, 79. (Conference version appeared in RANDOM, 2011).

Eli Ben-Sasson, Prahladh Harsha & Sofya Raskhodnikova (2005). Some 3CNF properties are hard to test. *SIAM Journal on Computing* **35**(1), 1–21.

Eli Ben-Sasson, Ghid Maatouk, Amir Shpilka & Madhu Sudan (2011b). Symmetric LDPC Codes are not Necessarily Locally Testable. In *IEEE Conference on Computational Complexity*, 55–65.

Manuel Blum, Michael Luby & Ronitt Rubinfeld (1993). Self-Testing/Correcting with Applications to Numerical Problems. *Journal of Computer and System Sciences* **47**(3), 549–595.

Christian Borgs, Jennifer T. Chayes, László Lovász, Vera T. Sós, Balázs Szegedy & Katalin Vesztergombi (2006). Graph limits and parameter testing. In *The Annual ACM Symposium on Theory of Computing*, 261–270.

Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra & Mario Szegedy (1996). Interactive proofs and the hardness of approximating cliques. *Journal of the ACM* **43**(2), 268–292.

Oded Goldreich, Shafi Goldwasser & Dana Ron (1998). Property testing and its connection to learning and approximation. *Journal of the ACM* **45**(4), 653–750. ISSN 0004-5411.

Elena Grigorescu (2010). *Symmetries in Algebraic Property Testing*. Ph.D. thesis, MIT.

Elena Grigorescu, Tali Kaufman & Madhu Sudan (2009). Succinct representation of codes with applications to testing. In *Proceedings of RANDOM-APPROX 2009*, volume 5687 of *Lecture Notes in Computer Science*, 534–547. Springer.

Tali Kaufman & Shachar Lovett (2011). New Extension of the Weil Bound for Character Sums with Applications to Coding. In *The Annual IEEE Symposium on Foundations of Computer Science*, 788–796.

Tali Kaufman & Dana Ron (2006). Testing Polynomials over General Fields. *SIAM Journal of Computing* **36**(3), 779–802.

Tali Kaufman & Madhu Sudan (2008). Algebraic property testing: the role of invariance. In *The Annual ACM Symposium on Theory of Computing*, 403–412.

F. J. MacWilliams & Neil J. A. Sloane (1981). *The Theory of Error-Correcting Codes*. Elsevier/North-Holland, Amsterdam.

Ronitt Rubinfeld & Madhu Sudan (1996). Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing* **25**(2), 252–271.

Elena Grigorescu
Department of Computer Science
Purdue University
West Lafayette, IN 47907.
elena-g@purdue.edu

Tali Kaufman
Bar-Ilan University and
Weizmann Institute of Science
Israel.
kaufmant@mit.edu

Madhu Sudan
Microsoft Research New England
One Memorial Drive,
Cambridge, MA 02142.
madhu@mit.edu