Explicit Low-Weight Bases for BCH Codes*

Elena Grigorescu†
elena_g@csail.mit.edu

Tali Kaufman‡
kaufmant@mit.edu.

Abstract

We exhibit explicit bases for BCH codes of designed distance 5. While BCH codes are some of the most studied families of codes, only recently Kaufman and Litsyn (FOCS, 2005) showed that they admit bases of small weight codewords. Furthermore, Grigorescu, Kaufman and Sudan (RANDOM, 2009) and Kaufman and Lovett (FOCS, 2011) proved that in fact BCH codes can admit very structured bases of small weight codewords (i.e. bases that can be fully specified by a single codeword and its orbit under the affine group). The existence of such structured bases has applications in property testing, and motivates our search for a fully explicit description of low weight codewords, and in particular of codewords that generate a basis for BCH codes. In this work we describe the support of basis-generating codewords under affine transformations of the domain for the very specific case of binary (extended) BCH$(2, n)$. We believe that extending these findings to general BCH codes merits further investigation.

1 Introduction

Error-correcting codes often admit multiple equivalent representations which in turn could lead to different applications. Motivated by applications in property testing, we investigate the possibility of explicitly representing binary BCH codes by bases of low weight vectors. For other common families of codes (e.g. Hadamard, Reed-Solomon, Reed-Muller) the low weight codewords are well understood, while (as far as we are aware) explicit low-weight codewords and low-weight bases for BCH codes have not been previously shown. Standard counting arguments imply the existence of low weight codewords, and even though BCH codes are some of the most studied families of codes, only recently Kaufman and Litsyn [6] proved that BCH codes have bases of small weight codewords. The bases provided there are however arbitrary, which brings up the question of how explicitly can one specify codewords and bases of BCH codes.

The extent of explicitness that we would like to achieve is to be able to fully specify the support of a codeword (or even of a set of codewords generating the code as a vector space). To exemplify this

*This work appeared in Elena Grigorescu's PhD Thesis [3].

†Georgia Institute of Technology, 266 Ferst Drive, Atlanta, GA 30332. Research conducted when this author was at MIT CSAIL. Research supported in part by NSF grant CCR-0829672 and NSF award 1019343 to the Computing Research Association for the CI Fellows Project.

‡Bar-Ilan University and the Weizmann Institute of Science, Israel. Research conducted when this author was at MIT CSAIL. Research supported in part by NSF grant CCR-0829672 and by the Alon Fellowship.

requirement, consider for instance the Hadamard code $\mathcal{H}_n = \{h_a : \mathbb{F}_2^n \to \mathbb{F}_2, h_a(x) = a \cdot x, a \in \mathbb{F}_2^n\}$. Its dual, the Hamming code, is generated as a vector space by codewords of weight 3, and these codewords are supported at tuples $\langle a, b, a+b\rangle$, for $a, b \in \mathbb{F}_2^n$. Moreover, since the Hadamard/Hamming codes are invariant under linear transformations of the domain $\mathbb{F}_2^n$, the Hamming code can be in fact specified by a single codeword of weight 3 (and the invariance group of the code), namely the codeword supported at $\langle e_1, e_2, e_1 + e_2\rangle$, where e_1, e_2 are the standard basis vectors in $\mathbb{F}_2^n$.

BCH codes are a classical family of cyclic codes and subfield subcodes of Reed-Solomon codes. In this work we will use an alternate view of BCH codes as evaluations of Trace polynomials. BCH codes are invariant under linear transformations of the domain $\mathbb{F}_{2^n}^*$. The extended BCH (eBCH) codes are obtained by appending a parity check bit to BCH codes, and they are invariant under affine transformations of $\mathbb{F}_{2^n}$. The works of [5, 7] largely reduce the complexity of specifying these codes by showing that they admit a very structured basis, similar to the one for the Hamming codes described above. Namely, eBCH codes must contain a codeword of small support whose shifts under affine transformations of $\mathbb{F}_{2^n}$ generate the code as a vector space (we will call such a codeword a *single orbit generator*). This property was initially defined in [8] and it is in fact shared by a few other common families of codes (Reed-Muller [3, 1], and duals of sparse affine-invariant codes [5, 7]).

The proofs in [5, 7] only determine the existence of a single orbit generating codeword and they do not imply specifics about the support elements, which would be useful in applications to the local testability of dual-BCH codes. In this work we provide low weight single orbit generators for BCH (and eBCH codes) of designed distance 5. We start by stating our main theorem.

Theorem 1 *For every $n > n_0$, with probability $1 - 2^{-O(n)}$ over the choice of $\alpha \in \mathbb{F}_{2^n}$, the codeword supported at*

$$\langle 0, 1, 1+\alpha^4, \alpha+\alpha^2+\alpha^4, \alpha^2+\alpha^3+\alpha^4, \alpha+\alpha^3+\alpha^4\rangle$$

is a 6-single-orbit generator for eBCH$(2, n)$*,*

We remark that for n large enough there is always a primitive element that could be used for α.

While this result is a modest contribution, we believe that the questions it raises regarding extensions to general BCH codes are worthy of further investigation. We state these directions below.

Problem 2 *Exhibit explicit low weight codewords, and bases of low weight codewords for* BCH(t, n) *for arbitrary t, n. Exhibit explicit single orbit generators for* BCH(t, n)*.*

Regarding our techniques, we first analyze sufficient conditions for a code to admit a single orbit generator in terms of certain 'diagonal' systems of equations. These equations bear a resemblance to the equations arising in the so-called Waring problem. A version of the Waring problem studies ways to express a polynomial as sums of d-th powers of some special polynomials. Our explicit description is inspired by some results of Paley [10] from the 1930s on the Waring problem. There he describes families of explicit polynomials that satisfy conditions similar to those required by the single orbit property.

2 Preliminaries

We start with some standard notation. For integer $t > 0$ we denote by $[t]$ the set $\{1, 2, \ldots, t\}$. $\mathbb{F}_{2^n}$ denotes the field with 2^n elements. A *primitive* element w is one such that $\mathbb{F}_{2^n} = \{0, 1, w, w^2, \ldots, w^{2^n-2}\}$. For $x, y \in \mathbb{F}_2^{2^n}$ $\langle x, y\rangle = \sum x_i y_i$ denotes the inner product between x, y. A binary code $C \subseteq \{0,1\}^{2^n}$ is a set of vectors, called *codewords*. $\mathcal{C} \subseteq \{0,1\}^{2^n}$ is a *linear* code if $c_1, c_2 \in \mathcal{C}$ implies $c_1 + c_2 \in \mathcal{C}$. The *dual* of a linear code $\mathcal{C}$, (denoted $\mathcal{C}^\perp$) is $\mathcal{C}^\perp = \{c' | \langle c, c'\rangle = 0, \forall c \in \mathcal{C}\}$. The codewords in $\mathcal{C} \subseteq \{\mathbb{F}_{2^n} \to \mathbb{F}_2\}$ are indexed by the elements of $\mathbb{F}_{2^n}$ in the cyclic order $0, 1, w, w^2, \ldots, w^{2^n-2}$, where w is a primitive element. Alternately, we also view a code C as a family of functions $\mathcal{F} \subseteq \{f : \mathbb{F}_{2^n} \to \mathbb{F}_2\}$ such that $\mathcal{C} = \{\langle f(x)\rangle_{x \in \mathbb{F}_{2^n}} | f \in \mathcal{F}\}$. We will alternate between these notations without further comment. The *support* of $c \in \mathcal{C}$ is $\mathrm{Supp}(c) = \{\alpha | c_\alpha \neq 0\}$, and the *weight* of a vector c is $\mathrm{wt}(c) = |\mathrm{Supp}(c)|$.

For a positive integer $d = \sum d_i 2^i$, with $d_i \in \{0, 1\}$, its binary weight is $\mathrm{bwt}(d) = |\{i | d_i = 1\}|$. The *shadow* of d, denoted Δd, is the set $\{d' = \sum d'_i 2^i | d'_i \leq d_i, \forall i\}$. The shadow of a set of integers D is $\Delta D = \{d' | \exists d \in D \text{ s.t. } d' \in \Delta d\}$. A set of integers $D \subseteq \{0\} \cup [2^n - 2]$ is *shadow closed* if $D = \Delta D$. For $d \in \{1, \ldots, 2^n - 2\}$, let

$$\mathrm{orb}(d) = \{d, 2d \pmod{2^n - 1}, 4d \pmod{2^n - 1}, \ldots, 2^{n-1}d \pmod{2^n - 1}\},$$

and let min-orb(d) denote the smallest integer in orb(d). Define

$$\mathcal{D} = \{\text{min-orb}(d) \mid d \in \{1, \ldots, 2^n - 2\}\} \cup \{2^n - 1\}.$$

The Trace function is defined as $\mathrm{Trace} : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $\mathrm{Trace}(x) = x + x^2 + \ldots + x^{2^{n-1}}$. The Trace function is linear (i.e. $\mathrm{Trace}(\alpha + \beta) = \mathrm{Trace}(\alpha) + \mathrm{Trace}(\beta)$), and has the property that $\mathrm{Trace}(\alpha^2) = \mathrm{Trace}(\alpha)$, $\forall \alpha \in \mathbb{F}_{2^n}$.

Definition 3 (Affine invariance) *A function $\pi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an* affine permutation *if there exist $\alpha \in \mathbb{F}_{2^n}^*$ and $\beta \in \mathbb{F}_{2^n}$ such that $\pi(x) = \alpha x + b$. A code $\mathcal{C} \subseteq \{f : \mathbb{F}_{2^n} \to \mathbb{F}_2\}$ is said to be* affine invariant *if $f \in \mathcal{C}$ if and only if $f \circ \pi \in \mathcal{C}$ for all affine permutations $\pi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.*

We will make use of the following fact about the structure of affine invariant families (See for example [8, 5, 4]).

Proposition 4 *For every affine invariant code $\mathcal{C} \subseteq \{\mathbb{F}_{2^n} \to \mathbb{F}_2\}$ there exists a set $D \subseteq \mathcal{D}$ such that $D \cup \{0\}$ is shadow closed and $\mathcal{C} = \{\mathrm{Trace}(f) |\ \ f(x) = \sum a_d x^d$, where $a_d \in \mathbb{F}_{2^n}$ and $d \in D \cup \{0\}\}$. Conversely, for any shadow closed set $D \cup \{0\}$ (with $D \subseteq \mathcal{D}$), the code $\mathcal{C} = \{\mathrm{Trace}(f) |\ f(x) = \sum a_d x^d,\ a_d \in \mathbb{F}_{2^n},\ d \in D \cup \{0\}\}$ is affine invariant. In this case we will say that D* describes *$\mathcal{C}$.*

BCH codes We define BCH codes using Proposition 4. The extended dual BCH code (denoted $\mathrm{eBCH}(t, n)^\perp$) is the affine invariant code $\mathrm{eBCH}(t, n)^\perp \subseteq \{\mathbb{F}_{2^n} \to \mathbb{F}_2\}$ described by the degree set $\{0\} \cup ([2t] \cap \mathcal{D})$. The dual-BCH code is $\mathrm{BCH}(t, n)^\perp \subseteq \{\mathbb{F}_{2^n}^* \to \mathbb{F}_2\}$ is hence obtained by puncturing one coordinate of $\mathrm{eBCH}(t, n)^\perp$. The BCH code $\mathrm{BCH}(t, n)$ is just the dual of $\mathrm{BCH}(t, n)^\perp$, and its extension by a parity bit is denoted by $\mathrm{eBCH}(t, n) \subseteq \{\mathbb{F}_{2^n} \to \mathbb{F}_2\}$. $\mathrm{BCH}(t, n)$ has minimum distance

$2t+1$ and eBCH(t,n) has minimum distance $2t+2$. A basis for eBCH(t,n) immediately implies a basis for BCH(t,n) where the weight of each vector might drop by at most 1.

In classical terms BCH(t,n) is a cyclic code whose zeros are $\{w, w^2, \ldots, w^{2t}\}$, where w is a primitive element. Expressed as evaluations of Trace functions, BCH$(t,n)^{\perp}$ corresponds to Traces of polynomials of degrees $\leq 2t$ and of constant term equal to 0. Similarly, eBCH$(t,n)^{\perp}$ corresponds to evaluations of traces of polynomials of degrees $\leq 2t$ and arbitrary constant terms. Our alternate description of dual BCH codes as traces of low degree polynomials was first formalized by Delsarte [2]. The set of degrees $\{0\} \cup ([2t] \cap \mathcal{D})$ plays an important role in our proofs, since the support of a single orbit generator exactly characterizes this set in a sense that we describe more precisely in Lemma 6. For a more extensive treatment of BCH codes we refer to [9].

We next formalize the notion of explicitness derived from the possible existence of a codeword which can specify the code entirely.

Definition 5 (Single orbit generator) *The code $\mathcal{F} \subseteq \{F_{2^n} \to \mathbb{F}_2\}$ has a* k-single orbit generator *g (under the affine group on $\mathbb{F}_{2^n}$) if* $\mathrm{wt}(g) \leq k$ *and* $\mathcal{F} = \mathrm{Span}(\{g \circ \pi | \pi(x) = ax+b, a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\})$.

3 Proof of the main theorem

The following lemma is the main tool in proving our theorem.

Lemma 6 *Let $\mathcal{F} \subseteq \{\mathbb{F}_{2^n} \to \mathbb{F}_2\}$ be an affine invariant code, and let D be the set of degrees that describes $\mathcal{F}$. If for some $\langle a_1, a_2, \ldots, a_k \rangle \in \mathbb{F}_{2^n}^k$ the following conditions hold*

1. $\sum_{i=1}^{k} a_i^d = 0$ *for all* $d \in D$
2. $\sum_{i=1}^{k} a_i^d \neq 0$ *for all* $d \in \mathcal{D} - D$

then $\mathcal{F}^{\perp}$ has a k-single orbit generator g supported at $\langle a_1, a_2, \ldots, a_k \rangle$.

Proof: We start with a simple helpful claim.

Claim 7 *Let $\mathcal{F} \subseteq \{\mathbb{F}_{2^n} \to \mathbb{F}_2\}$ be an affine invariant code and let D be the set of degrees that describes $\mathcal{F}$. Then a function g supported at $\langle a_1, a_2, \ldots, a_k \rangle \in \mathbb{F}_{2^n}^k$ belongs to $\mathcal{F}^{\perp}$ if and only if*

$$\sum_{i=1}^{k} a_i^d = 0 \text{ for all } d \in D.$$

Proof: By definition, $\mathcal{F} = \{\text{Trace}(\sum_{d\in D} \alpha_d x^d), \alpha_d \in \mathbb{F}_{2^n}\}$. Then $g \in \mathcal{F}^\perp$ if and only if for any $f \in \mathcal{F}$, $\langle f, g\rangle = 0$, that is $\sum_{i=1}^{k} f(a_i) = 0$. Let $f_\alpha(x) = \text{Trace}(\alpha x^d) \in \mathcal{F}$, for some $\alpha \in \mathbb{F}_{2^n}$. Then $0 = \sum_{i=1}^{k} f_\alpha(a_i) = \sum_{i=1}^{k} \text{Trace}(\alpha a_i^d) = \text{Trace}(\alpha \sum_{i=1}^{k} a_i^d)$. Since $f_\alpha \in \mathcal{F}$ for all $\alpha \in \mathcal{F}$, it follows that for $\beta = \sum_{i=1}^{k} a_i^d$, the previous identity holds if and only if $\text{Trace}(\beta\alpha) = 0$ for all $\alpha \in \mathbb{F}_{2^n}$. But the function $\text{Trace}(\beta x)$ is linear, and it is identically null only when $\beta = 0$, which concludes the proof. ∎

By Claim 7, condition 1 immediately implies that $g \in \mathcal{F}^\perp$.

We will show that $\mathcal{F}^\perp$ is the smallest affine invariant code that contains g. Notice that if g belongs to some affine invariant code then the set $\{g \circ \pi, \pi(x) = ax + b\}$ belongs to that code, and by linearity, the set of functions $\text{Span}\{g \circ \pi\}$ is included in the code as well. Therefore, g is a single orbit generator for the smallest affine invariant (linear) code that contains it, which will conclude the proof.

Assume for the sake of contradiction that $g \in \mathcal{C} \subsetneq \mathcal{F}^\perp$ and $\mathcal{C}$ is affine invariant. Then $\mathcal{F} \subsetneq \mathcal{C}^\perp$, and let D' be the shadow-closed set of degrees that characterizes $\mathcal{C}^\perp$, i.e. $\mathcal{C}^\perp = \{\text{Trace}(\sum_{d\in D'} \alpha_d x^d), \alpha_d \in \mathbb{F}_{2^n}\}$. Therefore, $D \subsetneq D'$. Since $g \in \mathcal{C}$, by Claim 7 we must have $\sum_{i=1}^{k} a_i^d = 0$ for all $d \in D'$, and in particular for some $d \in D' \cap (\mathcal{D} - D)$, which contradicts condition 2.

∎

We next show a quick application of Lemma 6

Corollary 8 *Let w be a primitive element of $\mathbb{F}_{2^n}$. Then the function supported on $\langle 0, 1, w, 1 + w\rangle$ is a 4-single orbit generator for* eBCH$(1, n)$.

Proof: Notice that the set of degrees that characterizes eBCH$(1, n)^\perp$ is $D = \{1\}$. Then condition 1 of Lemma 6 is trivially satisfied.

To verify condition 2 of Lemma 6, for $d \in \mathcal{D} - D$, we distinguish the cases: $\text{bwt}(d) = 2$ and $\text{bwt}(d) \geq 3$. In the former case, suppose $d = 2^\ell + 1$ for some $\ell > 0$, and notice that $1 + w^{2^\ell+1} + (1 + w)^{2^\ell+1} = w + w^{2^\ell} \neq 0$. Indeed, otherwise $w^{2^\ell-1} = 1$, which would imply that w belongs to a subfield of size 2^ℓ, contradicting the assumption that w is a primitive element.

Finally, if d with $\text{bwt}(d) \geq 3$ satisfies condition 1 of Lemma 6, then any affine invariant code characterized by a set D' of degrees containing d must also contain the shadow of the degree d (by Proposition 4). In particular, D' should contain some degree of binary weight 2. This contradicts the fact that there is no degree of weight 2 satisfying condition 1 and concludes the proof. ∎

4 Explicit single orbit for the eBCH$(2, n)$

In this section we prove our main theorem. We note that similar techniques can be used to show the existence of explicit single orbit generators under the affine group on $\mathbb{F}_{2^n}$ for RM codes (See [3, 1]).

Proof of Theorem 1: Notice that $D = \{1, 3\}$ is the set of degrees that characterizes eBCH$(2, n)^{\perp}$. We will show that there exists $\alpha \in \mathbb{F}_{2^n}$ (in fact there exist many α's) such that $a_1 = 0$, $a_2 = 1$, $a_3 = 1 + \alpha^4$, $a_4 = \alpha + \alpha^2 + \alpha^4$, $a_5 = \alpha^2 + \alpha^3 + \alpha^4$, $a_6 = \alpha + \alpha^3 + \alpha^4$, satisfy the conditions of Lemma 6 and therefore they form the support of a 6-single orbit generator for eBCH$(2, n)$.

A simple calculation shows that condition 1 of Lemma 6 is satisfied by *any* α.

We now proceed to verify condition 2. To that end, for each $2 \leq \ell \leq \lfloor n/2 \rfloor + 1$ define the polynomial

$$P_\ell(x) = 1 + (1 + x^4)^{2^\ell+1} + (x + x^2 + x^4)^{2^\ell+1} + (x^2 + x^3 + x^4)^{2^\ell+1} + (x + x^3 + x^4)^{2^\ell+1}.$$

Also let,

$$Q(x) = \prod_{\ell=2}^{\lfloor n/2 \rfloor+1} P_\ell(x).$$

We will argue that $Q(x)$ is not identically 0 over $\mathbb{F}_{2^n}$, which implies the existence of many $\alpha \neq 0, 1$ such that $Q(\alpha) \neq 0$. This will be enough to complete the proof.

First notice that the degree in each P_ℓ is at most $4(2^\ell + 1)$, and thus the total degree of Q is at most $4(2^{n/2+1} + 1)n/2 < 2^n - 1$, for large enough n. Hence, no degree is too large to wrap around modulo $x^{2^n} - x$ and cause cancellations with smaller degree terms from the expansion of Q.

Secondly, we argue that each factor is a non-zero polynomial. Hence the product of minimum degree monomials in each P_ℓ results in a non-zero term of $Q(x)$ that cannot be canceled by other terms in the expansion. Indeed, one can easily check that the minimum degree monomial in each P_ℓ is $x^{2^\ell+2}$. Therefore, the monomial of degree $\sum_{\ell=2}^{\lfloor n/2 \rfloor+1} 2^\ell + 2 < 2^{n/2+3} + n < 2^n - 1$ is the minimum degree term of Q in the expansion. Since $Q(x)$ is a non-zero polynomial over $\mathbb{F}_{2^n}$, there must exist $\alpha \in \mathbb{F}_{2^n}$ such that $Q(\alpha) \neq 0$ and thus $P_\ell(\alpha) \neq 0$ for all $2 \leq \ell \leq \lfloor n/2 \rfloor + 1$. Further notice that for $\ell > \lfloor n/2 \rfloor + 1$ it is the case that $2^\ell + 1 \notin \mathcal{D}$. Indeed, for $\ell > \lfloor n/2 \rfloor + 1$, $2^\ell + 1 = 2^\ell + 2^n = 2^\ell(1 + 2^{n-\ell}) \pmod{2^n - 1}$ and therefore $2^\ell + 1 \in \text{orb}(2^{n-\ell} + 1)$. In fact there are at least $2^n - 1 - (2^{n/2+2} + 2)n$ many α's satisfying the conditions of Lemma 6.

Finally, as in the proof of Corollary 8, for a fixed such α, if there exists a degree $d \in \mathcal{D} - D$ with $\text{bwt}(d) \geq 3$ for which $\langle a_1 \ldots, a_6 \rangle$ satisfy condition 1 of Lemma 6, then any affine invariant code characterized by D' with $d \in D'$ must contain at least 2 degrees of weight 2 in the shadow of d. By Claim 7 these degrees must satisfy condition 1, which contradicts the above argument, implying that condition 2 of Lemma 6 is satisfied, and thus concluding the proof.

Note that if the total degree of Q is smaller than the number of primitive elements of $\mathbb{F}_{2^n}$ (namely, $\phi(2^n - 1)$, where ϕ is the Euler function) then there exists some primitive element that is a non-root of Q and which could be used for α. For large enough n, $\phi(2^n - 1) > (2^{n/2+2} + 2)n$, and so in this case there exists a primitive element α that implies a single orbit generator.

∎

5 Discussion

The main reason why we could specify the support of a codeword for *any* large enough n is because the 5 explicit polynomials in α, namely 1, $1+\alpha^4$, $\alpha+\alpha^2+\alpha^4$, $\alpha^2+\alpha^3+\alpha^4$ and $\alpha+\alpha^3+\alpha^4$ imply null polynomials in condition 1 of Lemma 6 for the set of degrees $\{1,3\}$. Moreover, these 5 polynomials are of small degrees (at most 4) independent of n, which allows us to argue that the polynomial Q in the proof of Theorem 1 has small degree as well. For these reasons, Theorem 1 holds in fact by the same argument for non-binary BCH codes. Our method could possibly extend to BCH codes of larger designed distance if one could determine similar small sets of explicit polynomials (possibly multivariate) satisfying the two main properties mentioned above.

Acknowledgments

We thank Madhu Sudan for the inspiring discussions and advice throughout the course of this work. We thank the anonymous reviewers for their very helpful comments and suggestions on improving the presentation of the manuscript.

References

[1] Eli Ben-Sasson, Elena Grigorescu, Ghid Maatouk, Amir Shpilka, and Madhu Sudan. On sums of locally testable affine invariant properties. In *APPROX-RANDOM*, pages 400–411, 2011.

[2] Philippe Delsarte. The association schemes of coding theory. *Combinatorics*, pages 143–161, 1975.

[3] Elena Grigorescu. *Symmetries in Algebraic Property Testing.* PhD thesis, MIT, 2010.

[4] Elena Grigorescu, Tali Kaufman, and Madhu Sudan. 2-transitivity is insufficient for local testability. In *CCC*, pages 259–267. IEEE Computer Society, 2008.

[5] Elena Grigorescu, Tali Kaufman, and Madhu Sudan. Succinct representation of codes with applications to testing. In *APPROX-RANDOM*, pages 534–547, 2009.

[6] Tali Kaufman and Simon Litsyn. Almost orthogonal linear codes are locally testable. In *FOCS*, pages 317–326. IEEE Computer Society, 2005.

[7] Tali Kaufman and Shachar Lovett. New extension of the Weil bound for character sums with applications to coding. *FOCS*, page (to appear), 2011.

[8] Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In *STOC*, pages 403–412, 2008.

[9] Florence J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes.* Elsevier/North-Holland, Amsterdam, 1981.

[10] R. E. A. C. Paley. Theorems on polynomials in a Galois field. *Q J Math*, os-4(1):52–63, 1933.