Optimal Codebooks From Binary Codes Meeting the Levenshtein Bound

Can Xiang, Cunsheng Ding, *Senior Member, IEEE*, and Sihem Mesnager

***Abstract*— In this paper, a generic construction of codebooks based on binary codes is introduced. With this generic construction, a few previous constructions of optimal codebooks are extended, and a new class of codebooks almost meeting the Levenshtein bound is presented. Exponentially many codebooks meeting or almost meeting the Levenshtein bound from binary codes are obtained in this paper. The codebooks constructed in this paper have alphabet size 4. As a byproduct, three bounds on the parameters of binary codes are derived.**

***Index Terms*— Codebooks, signal sets, Levenshtein bounds, codes, bent functions, semi-bent functions.**

I. Introduction

LET $\mathcal{B} = \{\mathbf{b}_0, \ldots, \mathbf{b}_{N-1}\}$, where each $\mathbf{b}_\ell$ is a unit norm $1 \times n$ complex vector over an alphabet A. Such a set $\mathcal{B}$ is called an (N, n) codebook (also called a signal set). The size of A is called the alphabet size of $\mathcal{B}$. As a performance measure of a codebook in practical applications, the maximum crosscorrelation amplitude of an (N, n) codebook $\mathcal{B}$ is defined by

$$I_{\max}(\mathcal{B}) = \max_{0 \le i < j \le N-1} \left| \mathbf{b}_i \mathbf{b}_j^H \right|$$

where $\mathbf{b}^H$ stands for the conjugate transpose of the complex vector $\mathbf{b}$. For $I_{\max}(\mathcal{B})$, we have the following well-known Welch bound [39].

Lemma 1: For any (N, n) codebook $\mathcal{B}$ with $N \ge n$,

$$I_{\max}(\mathcal{B}) \ge \sqrt{\frac{N-n}{(N-1)n}}. \tag{1}$$

Furthermore, the equality in (1) is achieved if and only if

$$\left| \mathbf{b}_i \mathbf{b}_j^T \right| = \sqrt{\frac{N-n}{(N-1)n}}$$

for all pairs (i, j) with $i \ne j$.

Manuscript received March 30, 2015; revised August 2, 2015; accepted September 25, 2015. Date of publication October 6, 2015; date of current version November 18, 2015. The work of C. Ding was supported by the Hong Kong Research Grants Council under Grant 16301114.

C. Xiang is with the College of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China (e-mail: cxiangcxiang@hotmail.com).

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: cding@ust.hk).

S. Mesnager is with the Laboratoire Analyse, Géométrie et Applications, Department of Mathematics, Sorbonne Paris Cité and Télécom ParisTech, University of Paris VIII, Saint-Denis 93526, France (e-mail: smesnager@univ-paris8.fr).

Communicated by K. Yang, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2015.2487451

A codebook achieving the equality in (1) is referred to as a maximum-Welch-bound-equality (MWBE) codebook [41]. The MWBE codebook is also known as an equiangular tight frame [7]. The construction of MWBE codebooks is equivalent to line packing in Grassmannian spaces [38]. The known MWBE codebooks can be summarized as follows [12], [21].

1) (N, N) orthogonal MWBE codebooks for any $N > 1$ [37], [41].
2) $(N, N-1)$ MWBE codebooks for $N > 1$ generated from discrete Fourier transformation matrices [37], [41], or m-sequences [37].
3) (N, n) MWBE codebooks from conference matrices [8], [38], where $N = 2n = 2^{d+1}$ or $N = 2n = p^d + 1$, where p is a prime number and d is a positive integer.
4) (N, n) MWBE codebooks from (N, n, λ) difference sets in cyclic groups [41] and abelian groups [10], [12].
5) MWBE codebooks from $(2, k, v)$-Steiner systems [16].

Besides MWBE codebooks, codebooks nearly meeting the Welch bound have also received a lot of attention (see [19], [21], [42]–[45], and references therein).

The following lemma shows that the Welch bound cannot be achieved when N is large.

Lemma 2 [38]: If $N > n(n+1)/2$, no (N, n) real codebook $\mathcal{B}$ can meet the Welch bound of (1); and if $N > n^2$, no (N, n) codebook $\mathcal{B}$ can meet the Welch bound of (1).

When N is large, the following Levenshtein bounds are better than the Welch bound.

Lemma 3 [23], [28]: For any real-valued codebook $\mathcal{B}$ with $N > n(n+1)/2$, we have

$$I_{\max}(\mathcal{B}) \ge \sqrt{\frac{3N - n^2 - 2n}{(n+2)(N-n)}}. \tag{2}$$

For any complex-valued codebook $\mathcal{B}$ with $N > n^2$, we have

$$I_{\max}(\mathcal{B}) \ge \sqrt{\frac{2N - n^2 - n}{(n+1)(N-n)}}. \tag{3}$$

It is noticed that a special case of the bounds of (2) and (3) was already presented in [9] using the language of line-sets.

Constructing codebooks achieving the Levenshtein bounds looks very hard in general. The known codebooks meeting the Levenshtein bound are listed as follows.

1) $(2^{2m-1} + 2^m, 2^m)$ codebooks generated from Kerdock codes and bent functions [2], [40], [46], where m is even. These two classes of real-valued codebooks are optimal with respect to the Levenshtein bound of (2) and have alphabet size 4.

2) $(p^{2m}+p^m, p^m)$ codebooks generated from planar functions [14], [40], and those from a family of p-ary bent functions [46], where p is an odd prime. These two classes of codebooks are optimal with respect to the Levenshtein bound of (3) and has alphabet size $p+2$.

Codebooks meeting the Welch bound or the Levenshtein bounds are much preferred in many practical applications, for example, unitary space-time modulations, multiple description coding over erasure channels, code-division multiple-access (CDMA) systems, and coding theory [2], [31]. According to Sarwate [37], it is desirable to employ codebooks with a small alphabet size in applications.

While many constructions of codebooks meeting or almost meeting the Welch bound are available in the literature, only a few constructions of codebooks meeting or almost meeting the Levenshtein bounds are known. The two objectives of this paper are to extend earlier constructions and present new constructions of exponentially many codebooks meeting or almost meeting the Levenshtein bound of (2). All the constructions of such codebooks in this paper are related to sets of bent functions and semi-bent functions satisfying certain conditions. Open problems are also presented in this paper.

II. Bent Functions, Semi-Bent Functions and Almost Bent Functions

Let f be a Boolean function from GF(2^m) to GF(2). The *support* of f is defined to be

$$D_f = \{x \in \mathrm{GF}(2^m) : f(x) = 1\} \subseteq \mathrm{GF}(2^m).$$

In this paper, we let $n_f = |D_f|$, which is called the (Hamming) weight of f.

The *Walsh transform* of f is defined by

$$\hat{f}(w) = \sum_{x \in \mathrm{GF}(2^m)} (-1)^{f(x)+\mathrm{Tr}_1^m(wx)} \tag{4}$$

where $w \in \mathrm{GF}(2^m)$. The *Walsh spectrum* of f is the following multiset

$$\left\{\hat{f}(w) : w \in \mathrm{GF}(2^m)\right\}.$$

A function f from GF(2^m) to GF(2) is called *linear* if $f(x+y) = f(x) + f(y)$ for all $(x, y) \in \mathrm{GF}(2^m)^2$. A function f from GF(2^m) to GF(2) is called *affine* if f or $f-1$ is linear.

A function from GF(2^m) to GF(2) is called *bent* if $|\hat{f}(w)| = 2^{m/2}$ for every $w \in \mathrm{GF}(2^m)$. Bent functions exist only for even m, and were coined by Rothaus in [36].

A subset D with κ elements of an abelian group $(A, +)$ of order v is called an (v, κ, λ) difference set in $(A, +)$ if the multiset $\{x - y : x \in D, y \in D\}$ contains every nonzero element of A exactly λ times. It is well-known that a function f from GF(2^m) to GF(2) is bent if and only if D_f is a Hadamard difference set in (GF(2^m), +) with the following parameters

$$(2^m,\ 2^{m-1} \pm 2^{(m-2)/2},\ 2^{m-2} \pm 2^{(m-2)/2}). \tag{5}$$

The information about difference sets can be found in [11].

Let f be bent. Then by definition $\hat{f}(0) = \pm 2^{m/2}$. It then follows that

$$n_f = |D_f| = 2^{m-1} \pm 2^{(m-2)/2} \tag{6}$$

There are many constructions of bent functions available in the literature (see, for example, [5], [32], [33], [35]). However, for the construction of codebooks meeting the Levenshtein bound of (2), we need a set of bent functions described in the following research problem.

Research Problem 1: Let m be even. Construct a set $\{f_a(x)\}$ of $2^{m-1}-1$ bent functions on GF(2^m) *such that the difference $f_a(x) - f_b(x)$ of any two distinct bent functions f_a and f_b in the set $\{f_a(x)\}$ is again a bent function.*

Let m be odd. Then there is no bent Boolean function on GF(2^m). A function f from GF(2^m) to GF(2) is called *semi-bent* if $\hat{f}(w) \in \{0, \pm 2^{(m+1)/2}\}$ for every $w \in \mathrm{GF}(2^m)$.

Let f be a semi-bent function from GF(2^m) to GF(2). It then follows from the definition of semi-bent functions that

$$n_f = |D_f| = \begin{cases} 2^{m-1} - 2^{(m-1)/2} & \text{if } \hat{f}(0) = 2^{(m+1)/2}, \\ 2^{m-1} + 2^{(m-1)/2} & \text{if } \hat{f}(0) = -2^{(m+1)/2}, \\ 2^{m-1} & \text{if } \hat{f}(0) = 0. \end{cases} \tag{7}$$

There are many constructions of semi-bent functions available in the literature (see, for example, [1], [5], [34]). However, for the construction of codebooks almost meeting the Levenshtein bound of (2), we need a set of semi-bent functions described in the following research problem.

Research Problem 2: Let m be odd. Construct a set $\{f_a(x)\}$ of 2^m-1 semi-bent functions on GF(2^m) *such that the difference $f_a(x) - f_b(x)$ of any two distinct semi-bent functions f_a and f_b in the set $\{f_a(x)\}$ is again a semi-bent function.*

For any function g from GF(2^m) to GF(2^m), we define

$$\lambda_g(a, b) = \sum_{x \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_1^m(ag(x)+bx)}, \quad a,\ b \in \mathrm{GF}(2^m).$$

A function g from GF(2^m) to GF(2^m) is called *almost bent* if $\lambda_g(a, b) = 0$, or $\pm 2^{(m+1)/2}$ for every pair (a, b) with $a \neq 0$. By definition, almost bent functions over GF(2^m) exist only for odd m.

By definition, any almost bent function $g(x)$ from GF(2^m) to GF(2^m) gives a set of $2^m - 1$ semi-bent functions

$$\{\mathrm{Tr}_1^m(ag(x)) : a \in \mathrm{GF}(2^m) \setminus \{0\}\},$$

meeting the requirements in Research Problem 2. This is the only known construction of such semi-bent function families in the literature. In this paper, we will present another construction and will employ it for the construction of codebooks almost meeting the Levenshtein bound.

III. The Construction of Codebooks From Binary Codes

Throughout this paper, let $\mathcal{E}_n$ denote the set formed by the standard basis of the n-dimensional Hilbert space:

$$(1,0,0,\cdots,0,0),$$
$$(0,1,0,\cdots,0,0),$$
$$\vdots$$
$$(0,0,0,\cdots,0,1).$$

An (n, M) binary code $\mathcal{C}$ is a subset of $\mathrm{GF}(2)^n$ with cardinality M. An (n, M, d) binary code $\mathcal{C}$ is a subset of $\mathrm{GF}(2)^n$ with cardinality M and minimum Hamming distance d between all pairs of distinct codewords in $\mathcal{C}$. Given any (n, M) binary code $\mathcal{C}$, we define a set

$$\mathcal{S}_n(\mathcal{C}) = \left\{ \frac{1}{\sqrt{n}}(-1)^{\mathbf{c}} : \mathbf{c} \in \mathcal{C} \right\}, \tag{8}$$

where $(-1)^{\mathbf{c}}$ denotes the vector $((-1)^{c_0}, (-1)^{c_1}, \ldots, (-1)^{c_{n-1}})$ for any codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathcal{C}$, and then define a codebook $\mathcal{B}(\mathcal{C})$ by

$$\mathcal{B}(\mathcal{C}) = \mathcal{E}_n \cup \mathcal{S}_n(\mathcal{C}). \tag{9}$$

The parameters of the codebook $\mathcal{B}(\mathcal{C})$ are given in the following theorem.

Theorem 4: For any (n, M) binary code $\mathcal{C}$, the set $\mathcal{B}(\mathcal{C})$ of (9) is an $(M + n, n)$ codebook with the maximum crosscorrelation amplitude

$$I_{\max}(\mathcal{B}(\mathcal{C})) = \frac{\max\{n - 2d_{\min},\ \sqrt{n},\ 2d_{\max} - n\}}{n}, \tag{10}$$

where $d_{\min}$ and $d_{\max}$ denote the minimum and maximum Hamming distance of the code $\mathcal{C}$, respectively.

Proof: The length and the size of the codebook follow from its definition and the parameters of the binary code $\mathcal{C}$. For any $\mathbf{e} \in \mathcal{E}_n$ and $\mathbf{s} \in \mathcal{S}_n(\mathcal{C})$, we have

$$\left| \mathbf{e}\, \mathbf{s}^H \right| = \frac{1}{\sqrt{n}} = \frac{\sqrt{n}}{n}.$$

For any pair of distinct vectors $\mathbf{s}_i = \frac{1}{\sqrt{n}}(-1)^{\mathbf{c}_i} \in \mathcal{S}_n(\mathcal{C}))$, where $\mathbf{c}_i \in \mathcal{C}$, we have

$$\left| \mathbf{s}_1\, \mathbf{s}_2^H \right| = \frac{1}{n} \left| \sum_{i=0}^{n-1} (-1)^{c_{1,j} - c_{2,j}} \right|$$
$$= \frac{1}{n} |n - 2\mathrm{dist}(\mathbf{c}_1, \mathbf{c}_2)|,$$

where $\mathrm{dist}(\mathbf{c}_1, \mathbf{c}_2)$ denotes the Hamming distance of the two vectors $\mathbf{c}_i = (c_{i,0}, c_{i,1}, \ldots, c_{i,n-1})$ in $\mathcal{C}$.

The desired conclusion on $I_{\max}(\mathcal{B}(\mathcal{C})))$ then follows. □

We have the following remarks on the construction of the codebook $\mathcal{B}(\mathcal{C})$.

1) The construction is an extension and generalization of previous constructions from finite geometry, bent functions, almost bent functions, and planar functions (see, for example, [2], [14], [46]).
2) It can be extended to p-ary codes by replacing -1 with a complex p-th primitive root of unity. However, the maximum crosscorrelation amplitude $I_{\max}(\mathcal{B}(\mathcal{C}))$ does not have the simple expression of Theorem 4.
3) It will be demonstrated later that the binary code $\mathcal{C}$ has to be chosen properly in order for the codebook $\mathcal{B}(\mathcal{C})$ to have good parameters.

TABLE I
The Weight Distribution of the Kerdock Code

Weight w	Multiplicity A_w
0	1
$2^{m-1} - 2^{(m-2)/2}$	$2^m(2^{m-1} - 1)$
2^{m-1}	$2^{m+1} - 2$
$2^{m-1} + 2^{(m-2)/2}$	$2^m(2^{m-1} - 1)$
2^m	1

Our main objective of this paper is to construct codebooks with the best possible parameters from binary codes. As a byproduct, we employ the Welch bound and Levenshtein bounds to derive the following new bounds on binary codes.

Theorem 5: Let $\mathcal{C}$ be an (n, M) binary code with

A) $d_{\min} + d_{\max} \le n$ *and*

B) $d_{\min} \le \frac{n - \sqrt{n}}{2}$,

where $d_{\min}$ and $d_{\max}$ denote the minimum and maximum Hamming distance of the code $\mathcal{C}$, respectively. Then

1) $d_{\min} \le \left(n - \sqrt{\frac{nM}{n+M-1}} \right)/2$, *provided that $M > n$;*
2) $d_{\min} \le \left(n - \sqrt{\frac{(3M+n-n^2)n^2}{(n+2)M}} \right)/2$, *provided that $M > n(n-1)/2$; and*
3) $d_{\min} \le \left(n - \sqrt{\frac{(2M+n-n^2)n^2}{(n+2)M}} \right)/2$, *provided that $M > n^2 - n$.*

Proof: Consider the codebook $\mathcal{B}(C)$ defined by $\mathcal{C}$ in (9). It follows from Conditions A) and B) and Theorem 4 that

$$I_{\max}(\mathcal{B}(\mathcal{C}))) = \frac{n - 2d_{\min}}{n}.$$

The bounds then follow from the Welch bound and the Levenshtein bounds. □

These bounds on binary codes apply for only a special class of binary codes satisfying conditions A) and B). Though they are derived easily, they are useful. Later, we will demonstrate that these bounds can be achieved. With these bounds, we will be able to prove that certain binary codes are optimal.

IV. Optimal Codebooks From Subcodes of the Kerdock Codes

Let $m \ge 4$ be even. The Kerdock code $\mathcal{K}(m)$ is a nonlinear code with parameters $(2^m, 2^{2m}, 2^{m-1} - 2^{(m-2)/2})$ and the weight distribution of Table I [25].

Now we give a brief introduction of the Kerdock code $\mathcal{K}(m)$. Let $\mathrm{Tr}_1^{m-1}(x)$ denotes the trace function from $\mathrm{GF}(2^{m-1})$ to $\mathrm{GF}(2)$. For any $(u, v, a, b) \in \mathrm{GF}(2) \times \mathrm{GF}(2) \times \mathrm{GF}(2^{m-1}) \times \mathrm{GF}(2^{m-1})$, we define the following functions

on GF(2^{m-1}):

$$Q(x) = \sum_{j=1}^{(m-2)/2} \mathrm{Tr}_1^{m-1}(x^{2^j+1}),$$
$$f(x) = u + \mathrm{Tr}_1^{m-1}(ax) + Q(bx),$$
$$g(x) = u + v + \mathrm{Tr}_1^{m-1}((a+b)x) + Q(bx).$$

Then the Kerdock code $\mathcal{K}(m)$ consists of all the codewords

$$\mathbf{c}_{(u,v,a,b)} = \Big(f(0), f(1), f(\alpha), \ldots, f(\alpha^{2^{m-1}-2}), g(0), g(1), g(\alpha), \ldots, g(\alpha^{2^{m-1}-2})\Big) \quad (11)$$

where (u, v, a, b) ranges over all the elements in GF(2) $\times$ GF(2) $\times$ GF(2^{m-1}) $\times$ GF(2^{m-1}). A detailed analysis of the Kerdock code $\mathcal{K}(m)$ can be found in [30, Cha. 15].

For the Kerdock code $\mathcal{K}(m)$, it follows from the description above that

$$d_{\max} = 2^m \text{ and } d_{\min} = 2^{m-1} - 2^{(m-2)/2}.$$

It then follows from Theorem 4 that

$$I_{\max}(\mathcal{B}(\mathcal{K}(m))) = 1.$$

Hence, the codebook defined by the Kerdock code $\mathcal{K}(m)$ has the worst crosscorrelation magnitude and is thus one of the worst codebooks. However, the codebook of certain subcodes of $\mathcal{K}(m)$ is optimal with respect to the Levenshtein bound. Below we describe these subcodes of $\mathcal{K}(m)$ and their optimal codebooks.

$\mathcal{K}(m)$ is *self-complementary* in the sense that the complement $\mathbf{1} + \mathbf{c}$ of $\mathbf{c}$ is also a codeword of $\mathcal{K}(m)$ if $\mathbf{c}$ is a codeword of $\mathcal{K}(m)$, where $\mathbf{1} = (1, 1, \ldots, 1)$. We now partition the codewords of $\mathcal{K}(m)$ into 2^{2m-1} pairs $\{\mathbf{c}, \mathbf{1} + \mathbf{c}\}$, and then define a subcode $\widetilde{\mathcal{K}}(m)$ that is composed of one and only one element from each pair $\{\mathbf{c}, \mathbf{1} + \mathbf{c}\}$ of codewords in $\mathcal{K}(m)$. The total number of such subcodes $\widetilde{\mathcal{K}}(m)$ of $\mathcal{K}(m)$ is $2^{2^{2m-1}}$.

Theorem 6: Let $m \geq 4$ be even, and let $\widetilde{\mathcal{K}}(m)$ be one of the subcodes defined above. Then $\mathcal{B}(\widetilde{\mathcal{K}}(m))$ is an optimal $(2^{2m-1} + 2^m, 2^m)$ codebook with $I_{\max}(\mathcal{B}(\widetilde{\mathcal{K}}(m))) = 2^{-m/2}$.

Proof: In the Kerdock code $\mathcal{K}(m)$, the Hamming distance between any pair of distinct codewords takes on one of the following values:

$$2^{m-1} - 2^{(m-2)/2},\ 2^{m-1},\ 2^{m-1} + 2^{(m-2)/2},\quad 2^m.$$

By the definition of $\widetilde{\mathcal{K}}(m)$, the Hamming distance between any pair of distinct codewords in $\widetilde{\mathcal{K}}(m)$ takes on one of the following values:

$$2^{m-1} - 2^{(m-2)/2},\ 2^{m-1},\quad 2^{m-1} + 2^{(m-2)/2}.$$

It then follows that for the code $\widetilde{\mathcal{K}}(m)$, we have $d_{\min} = 2^{m-1} - 2^{(m-2)/2}$. Note that $d_{\max} \leq 2^{m-1} + 2^{(m-2)/2}$. From Theorem 4, we then deduce that $I_{\max}(\mathcal{B}(\widetilde{\mathcal{K}}(m))) = 2^{-m/2}$. By definition, $\widetilde{\mathcal{K}}(m)$ has 2^{2m-1} codewords. One can easily verify that this codebook meets the Levenshtein bound of (2). This completes the proof. □

We have the following comments on the codebooks $\mathcal{B}(\widetilde{\mathcal{K}}(m))$.

- For each Kerdock code $\mathcal{K}(m)$, we can select $2^{2^{2m-1}}$ subcodes $\widetilde{\mathcal{K}}(m)$. Each of the subcodes $\widetilde{\mathcal{K}}(m)$ gives an optimal codebook with alphabet size 4.
- Some of the subcodes $\widetilde{\mathcal{K}}(m)$ were employed to define extremal Euclidean line-sets (real-valued codebooks in the language of finite geometry) (see [2], [3], [27]). Hence, the construction of this section is a substantial extension of earlier ones.

We inform that all the subcodes $\widetilde{\mathcal{K}}(m)$ of the Kerdock codes $\mathcal{K}(m)$ meet the third bound in Theorem 5. There are also codes meeting the remaining two bounds in Theorem 5. Thus, the bounds in Theorem 5 are tight and useful in coding theory.

V. Asymptotically Optimal Codebooks With Respect to the Levenshtein Bound

The Levenshtein bounds are not tight in certain ranges, and thus cannot be met. In this section, we extend earlier constructions and present a new construction of codebooks that almost meet the Levenshtein bound and are asymptotically optimal with respect to the Levenshtein bound of (2). Throughout this section, m is odd.

A. A Generic Construction

Our objective of this section is to present a generic construction of exponentially many codebooks almost meeting the Levenshtein bound of (2) with a binary code having special parameters. Our construction is given in the following theorem.

Theorem 7: Let $\mathcal{C}$ be a $(2^m, 2^{2m})$ binary code such that

$$d_{\min} = 2^{m-1} - 2^{\frac{m-1}{2}} \text{ and } d_{\max} = 2^{m-1} + 2^{\frac{m-1}{2}}. \quad (12)$$

Let $\widetilde{\mathcal{C}}$ be the set consisting of one and only one of the elements in $\{\mathbf{c}, \mathbf{1}+\mathbf{c}\}$ for every codeword $\mathbf{c}$ in $\mathcal{C}$. Then the set $\mathcal{B}(\widetilde{\mathcal{C}})$ is a $(2^{2m} + 2^m, 2^m)$ codebook with the maximum crosscorrelation magnitude

$$I_{\max}(\mathcal{B}(\widetilde{\mathcal{C}})) = \sqrt{\frac{1}{2^{m-1}}}.$$

Proof: It follows from the assumptions on the code $\mathcal{C}$ that $\widetilde{\mathcal{C}}$ is a $(2^m, 2^{2m})$ binary code, where the Hamming distances $\mathrm{dist}(\widetilde{\mathbf{c}}_1, \widetilde{\mathbf{c}}_2)$ between any pair of distinct codewords $\widetilde{\mathbf{c}}_1$ and $\widetilde{\mathbf{c}}_2$ in $\widetilde{\mathcal{C}}$ satisfies

$$2^{m-1} - 2^{\frac{m-1}{2}} \leq \mathrm{dist}(\widetilde{\mathbf{c}}_1, \widetilde{\mathbf{c}}_2) \leq 2^{m-1} + 2^{\frac{m-1}{2}},$$

and at least one of $2^{m-1} \pm 2^{\frac{m-1}{2}}$ is the Hamming distance between two codewords in $\widetilde{\mathcal{C}}$. The desired conclusions on the codebook $\mathcal{B}(\widetilde{\mathcal{C}})$ are then deduced from Theorem 4. □

For any real-valued $(2^{2m} + 2^m, 2^m)$ codebook $\mathcal{B}$, the Levenshtein bound of (2) is

$$B_m = \sqrt{\frac{1}{2^{m-1}} - \frac{3}{(2^m+2)2^m}}.$$

Hence, the codebook $\mathcal{B}(\mathcal{C})$ of Theorem 8 almost meets the Levenshtein bound B_m above. In addition, we have

$$\lim_{m\to\infty} \frac{I_{\max}(\mathcal{B}(\mathcal{C}))}{B_m} = 1.$$

Hence, the codebook $\mathcal{B}(\mathcal{C})$ of Theorem 8 is asymptotically optimal with respect to the Levenshtein bound.

Open Problem 1: Let m be odd. Is there any real-valued codebook $\mathcal{B}$ with parameters $(2^{2m}+2^m, 2^m)$ and maximum crosscorrelation magnitude

$$I_{\max}(\mathcal{B}) < \sqrt{\frac{1}{2^{m-1}}}?$$

Open Problem 2: Let m be odd. Is there any real-valued codebook $\mathcal{B}$ with parameters $(M, 2^m)$ and maximum cross-correlation magnitude

$$I_{\max}(\mathcal{B}) = \sqrt{\frac{1}{2^{m-1}}}$$

such that $M > 2^{2m}+2^m$?

We have the following remarks about the extended construction of Theorem 7.

1) The code $\mathcal{C}$ required in Theorem 7 may be linear or nonlinear. In subsequent sections, we will demonstrate examples of both linear and nonlinear codes with the required properties.
2) One given binary code $\mathcal{C}$ satisfying the conditions of Theorem 7 yields $2^{2^{2m}}$ binary codes $\widetilde{\mathcal{C}}$, and thus $2^{2^{2m}}$ codebooks $\mathcal{B}(\widetilde{\mathcal{C}})$, which almost meet the Levenshtein bound and are asymptotically optimal. So, Theorem 7 is a substantial extension of the construction in [14].
3) Among the $2^{2^{2m}}$ binary codes $\widetilde{\mathcal{C}}$ given by a binary code $\mathcal{C}$, at most one of them is linear.

In the next two subsections, we present examples of both linear and nonlinear codes meeting the requirements of Theorem 7. In this way, we will be able to show the usefulness of Theorem 7.

B. An Extension of an Earlier Construction

Theorem 8: Let m be odd. Let $\mathcal{C}$ be a binary linear code with length 2^m and dimension $2m$ such that the minimum nonzero Hamming weight and maximum Hamming weight are given by

$$w_{\min} = 2^{m-1} - 2^{\frac{m-1}{2}} \text{ and } w_{\max} = 2^{m-1} + 2^{\frac{m-1}{2}}.$$

Then the set $\mathcal{B}(\mathcal{C})$ is a $(2^{2m}+2^m, 2^m)$ codebook with the maximum crosscorrelation magnitude

$$I_{\max}(\mathcal{B}(\mathcal{C})) = \frac{2^{(m+1)/2}}{2^m} = \sqrt{\frac{1}{2^{m-1}}}. \tag{13}$$

Proof: The conclusions on the length and the number of cordewords in $\mathcal{B}(\mathcal{C})$ follow from those of the linear code $\mathcal{C}$ and the definition of the codebook. Since $\mathcal{C}$ is linear, we have

$$d_{\min} = w_{\min} \text{ and } d_{\max} = w_{\max}.$$

Then the desired conclusion on the maximum crosscorrelation magnitude follows from Theorem 7. □

We now introduce a construction of binary linear codes satisfying the conditions of Theorems 7 and 8, which dates back many years ago.

TABLE II
THE WEIGHT DISTRIBUTION OF THE CODES $\mathcal{C}_g$

Weight w	Multiplicity A_w
0	1
$2^{m-1}-2^{(m-1)/2}$	$(2^m-1)(2^{m-2}+2^{(m-3)/2})$
2^{m-1}	$(2^m-1)(2^{m-1}+1)$
$2^{m-1}+2^{(m-1)/2}$	$(2^m-1)(2^{m-2}-2^{(m-3)/2})$

For any function g from GF(2^m) to GF(2^m) with $g(0)=0$, we define the following linear code

$$\mathcal{C}_g = \{\mathrm{Tr}_1^m(ag(x)+bx)_{x\in \mathrm{GF}(2^m)},\ a,\ b \in \mathrm{GF}(2^m)\}. \tag{14}$$

When g is almost bent, by definition $ag(x)+bx$ is semi-bent for any $a \neq 0$ and b. In this case it follows that the dimension of the code $\mathcal{C}_g$ is $2m$ and $\mathcal{C}_g$ has only the following nonzero weights:

$$2^{m-1} - 2^{\frac{m-1}{2}},\ 2^{m-1},\quad 2^{m-1} + 2^{\frac{m-1}{2}}. \tag{15}$$

The weight distribution of the code $\mathcal{C}_g$ is given in Table II [6].

The following is a list of almost bent functions on GF(2^m), where m is odd.

1) $g(x) = x^{2^i+1}$, $\gcd(i,m)=1$ [17].
2) $g(x) = x^{2^{2i}-2^i+1}$, $\gcd(i,m)=1$ [24].
3) $g(x) = x^{2^{(m-1)/2}+3}$ [24].
4) $g(x) = x^{2^{(m-1)/2}+2^{(m-1)/4}-1}$, $m \equiv 1 \pmod 4$ [4], [18], [20].
5) $g(x) = x^{2^{(m-1)/2}+2^{(3m-1)/4}-1}$, $m \equiv 3 \pmod 4$ [4], [18], [20].
6) $g(x) = x^{2^i+1} + (x^{2^i}+x)\mathrm{Tr}_1^m(x^{2^i+1}+x)$, $m > 3$ and $\gcd(i,m)=1$ [1].

Hence, we have at least five families of linear codes $\mathcal{C}_g$ satisfying the conditions of Theorems 7 and 8. These codebooks $\mathcal{B}(\mathcal{C}_g))$ were already described in [14]. Therefore, the construction of Theorem 8 is an extension of the one proposed in [14]. Note that each code $\mathcal{C}_g$ defined by an almost bent function can be plugged into Theorem 7 to obtain $2^{2^{2m}}$ codebooks that are asymptotically optimal with respect to the Levenshtein bound.

C. A New Class of Codebooks Almost Meeting the Levenshtein Bound

In [46], sets of bent functions meeting the requirements in Research Problem 1 were constructed and employed to construct codebooks meeting the Levenshtein bound of (2). In this section, we modify the construction of bent functions in [46], and obtain sets of semi-bent functions meeting the requirements in Research problem 2, and will then employ these sets of semi-bent functions to construct a number of codebooks almost meeting the Levenshtein bound of (2).

Let $m = e\ell$ be odd, where $e \geq 1$ and $3 \leq \ell \leq m$, and let k be a positive integer with $\gcd(k,m) = 1$. Let $\gamma \in \mathrm{GF}(2^e)$ with $\gamma \neq 1$. We define the following functions

over GF(2^m):

$$P(x) = \sum_{i=1}^{(m-1)/2} \mathrm{Tr}_1^m(x^{2^{ki}+1}),$$
$$Q(x) = \sum_{i=1}^{(\ell-1)/2} \mathrm{Tr}_1^m(x^{2^{ei}+1}),$$
$$f_a(x) = P(ax) + Q(\gamma ax), \ \ a \in \mathrm{GF}(2^m).$$

Lemma 9: For every $a \in \mathrm{GF}(2^m)^*$, $f_a(x)$ is semi-bent.

Proof: Note that $f_a(x) = f_1(ax)$ and semi-bent property is preserved under affine transformation. It suffices to prove that $f_1(x)$ is semi-bent. Nevertheless, we prefer to prove the semi-bent property of $f_a(x)$ for every a directly.

The Walsh transform of $f_a(x)$ is given by

$$\hat{f}_a(w) = \sum_{x \in \mathrm{GF}(2^m)} (-1)^{f_a(x)+\mathrm{Tr}_1^m(wx)},$$

where $w \in \mathrm{GF}(2^m)$. We have then

$$\begin{aligned}\left(\hat{f}_a(w)\right)^2 &= \sum_{x \in \mathrm{GF}(2^m)} \sum_{z \in \mathrm{GF}(2^m)} (-1)^{f_a(x)+f_a(z)+\mathrm{Tr}_1^m(w(x+z))} \\ &= \sum_{y \in \mathrm{GF}(2^m)} \sum_{x \in \mathrm{GF}(2^m)} (-1)^{f_a(x)+f_a(x+y)+\mathrm{Tr}_1^m(wy)} \\ &= \sum_{x \in \mathrm{GF}(2^m)} (-1)^{f_a(x)+\mathrm{Tr}_1^m(wx)} \sum_{y \in \mathrm{GF}(2^m)} (-1)^{B_{f_a}(x,y)},\end{aligned} \tag{16}$$

where $B_{f_a}(x, y) := f_a(x) + f_a(y) + f_a(x + y)$. Since $\gcd(k, m) = 1$, it can be verified that

$$\begin{aligned}&B_{f_a}(x, y) \\ &\quad = f_a(x) + f_a(y) + f_a(x + y) \\ &\quad = P(ax) + Q(\gamma ax) + P(ay) + Q(\gamma ay) \\ &\qquad + P(a(x + y)) + Q(\gamma a(x + y)) \\ &\quad = \mathrm{Tr}_1^m\left(y\left[a\mathrm{Tr}_1^m(ax) + a^2(1 + \gamma^2)x + a\gamma^2\mathrm{Tr}_e^m(ax)\right]\right).\end{aligned} \tag{17}$$

We now prove that the following linear equation

$$\mathrm{Tr}_1^m(ax) + a(1 + \gamma^2)x + \gamma^2\mathrm{Tr}_e^m(ax) = 0 \tag{18}$$

has exactly two solutions $x \in \mathrm{GF}(2^m)$. Note that $\gamma \in \mathrm{GF}(2^e)$ and $1 + \gamma^2 \neq 0$. It then follows from (18) that $ax \in \mathrm{GF}(2^e)$ and

$$\mathrm{Tr}_e^m(ax) = ax\mathrm{Tr}_e^m(1) = ax. \tag{19}$$

Combining (18) and (19), we obtain

$$\mathrm{Tr}_1^m(ax) + ax = 0.$$

Hence, $ax \in \mathrm{GF}(2)$. Therefore, $x = 0$ and $x = a^{-1}$ are the only solutions of (18). It then follows from (16) and (17) that $(\hat{f}_a(w))^2 \in \{0, 2^{m+1}\}$. Therefore, f_a is semi-bent. □

Note that the weight of $f_1(x)$ can take on any of the three elements in $\{2^{m-1}, 2^{m-1} \pm 2^{(m-1)/2}\}$, depending on m and the choice of γ.

We will need the following auxiliary result whose proof is given in the Appendix.

TABLE III
THE WALSH SPECTRUM OF $f_1(x)$

$\hat{f}_1(w)$	Multiplicity
0	2^{m-1}
$2^{(m+1)/2}$	$2^{m-2}+2^{(m-3)/2}$
$-2^{(m+1)/2}$	$2^{m-2}-2^{(m-3)/2}$

TABLE IV
THE WEIGHTS AND MULTIPLICITY OF $\{f_1(x) + \mathrm{Tr}_1^m(bx) : b \in \mathrm{GF}(2^m)\}$

Hamming weight	Multiplicity
$2^{m-1}-2^{(m-1)/2}$	$2^{m-2}+2^{(m-3)/2}$
2^{m-1}	2^{m-1}
$2^{m-1}+2^{(m-1)/2}$	$2^{m-2}-2^{(m-3)/2}$

Lemma 10: For any pair of distinct elements a and b in $\mathrm{GF}(2^m)^*$, $g_{(a,b)}(x) := f_a(x) + f_b(x)$ is semi-bent.

We now define a binary code $\mathcal{C}$ by

$$\begin{aligned}&\mathcal{C}(e, \ell, \gamma, k) \\ &\quad = \{(f_a(x) + \mathrm{Tr}_1^m(bx))_{x \in \mathrm{GF}(2^m)} : a \text{ and } b \in \mathrm{GF}(2^m)\}.\end{aligned} \tag{20}$$

Note that $f_a(x)$ depends on the selection of e, ℓ, γ and k, so does the code $\mathcal{C}(e, \ell, \gamma, k)$.

Theorem 11: The set $\mathcal{C}(e, \ell, \gamma, k)$ of (20) is a $(2^m, 2^{2m})$ binary code and the Hamming distance between any pair of distinct codewords in $\mathcal{C}(e, \ell, \gamma, k)$ takes on one of the following three values:

$$2^{m-1} - 2^{\frac{m-1}{2}}, \ 2^{m-1}, \ \ 2^{m-1} + 2^{\frac{m-1}{2}}.$$

In addition, the weight distribution of the code $\mathcal{C}(e, \ell, \gamma, k)$ is given in Table II.

Proof: By Lemma 9, $f_a(x) + \mathrm{Tr}_1^m(bx)$ is either semi-bent or linear. By Lemma 10, $(f_{a_1}(x) + \mathrm{Tr}_1^m(b_1x)) - (f_{a_2}(x) + \mathrm{Tr}_1^m(b_2x))$ is either semi-bent or linear. The desired conclusions on the Hamming distance follows from the size of the support of semi-bent functions and linear functions.

We now prove the conclusion on the weight distribution of the code $\mathcal{C}(e, \ell, \gamma, k)$. Note that $f_1(x)$ is a quadratic semi-bent function. Then the Walsh spectrum of the Boolean semi-bent function $f_1(x)$ is given in Table III [30, 441].

Hence, the weights of the following set

$$\{f_1(x) + \mathrm{Tr}_1^m(bx) : b \in \mathrm{GF}(2^m)\}$$

of Boolean functions and their multiplicities are given in Table IV. It is easily seen that the Hamming weight of the Boolean function $f_a(x) + \mathrm{Tr}_1^m(bx)$ is equal to that of $f_1(x) + \mathrm{Tr}_1^m(a^{-1}bx)$ for each $a \in \mathrm{GF}(2^m)^*$. The desired conclusion on the weight distribution then follows. □

It is noticed that the codes $\mathcal{C}(e, \ell, \gamma, k)$ of (20) are not linear. Thus, both linear and nonlinear codes meeting the conditions of Theorem 7 are demonstrated in this paper. It is interesting to observe that the nonlinear codes $\mathcal{C}(e, \ell, \gamma, k)$ of (20) have the same weight distribution as the linear code $\mathcal{C}_g$ defined by any almost bent function g on $\mathrm{GF}(2^m)$.

The following theorem describes a class of binary nonlinear codes, which may be viewed as an analogue of the Kerdock codes for odd m, and derives directly from Theorem 11.

TABLE V
THE WEIGHT DISTRIBUTION OF THE CODES IN THEOREM 12

Weight w	Multiplicity A_w
0	1
$2^{m-1}-2^{(m-1)/2}$	$(2^m-1)2^{m-1}$
2^{m-1}	$(2^m-1)(2^m+2)$
$2^{m-1}+2^{(m-1)/2}$	$(2^m-1)2^{m-1}$
2^m	1

Theorem 12: Define

$$\overline{\mathcal{C}(e,\ell,\gamma,k)} = \mathcal{C}(e,\ell,\gamma,k) \cup \{\mathbf{1}+\mathbf{c} : \mathbf{c} \in \mathcal{C}(e,\ell,\gamma,k)\}.$$

Then $\overline{\mathcal{C}(e,\ell,\gamma,k)}$ *is a* $(2^m, 2^{2m+1}, 2^{m-1}-2^{(m-1)/2})$ *nonlinear binary code with the weight distribution of Table V.*

The following theorem then deduces from Theorems 11 and 4.

Theorem 13: The set $\mathcal{B}(\mathcal{C}(e,\ell,\gamma,k))$ *of the binary code* $\mathcal{C}(e,\ell,\gamma,k)$ *of (20) is a* $(2^{2m}+2^m, 2^m)$ *codebook with the maximum crosscorrelation magnitude*

$$I_{\max}(\mathcal{B}(\mathcal{C}(e,\ell,\gamma,k))) = \sqrt{\frac{1}{2^{m-1}}}.$$

We have the following comments on the construction of this section.

1) Define

$$\mathcal{F}_{(e,\ell,\gamma,k)} = \{f_a(x) : a \in \mathrm{GF}(2^m)^*\}.$$

Then $\mathcal{F}_{(e,\ell,\gamma,k)}$ is a set of 2^m-1 semi-bent functions such that the difference of any pair of distinct semi-bent functions is also semi-bent.

2) For any odd m, we can choose $(e,\ell)=(1,m)$. In this case, the only choice for γ is $\gamma=0$. This pair $(e,\ell)=(1,m)$ yields $\phi(m)$ codebooks $\mathcal{B}(\mathcal{C}(e,\ell,\gamma,k))$. This is the maximum number of codebooks obtained for every odd $m \geq 3$. If m is a prime, then the total number of codebooks obtained is at most $\phi(m)$, where $\phi(x)$ is the Euler totient function.

3) In general, the total number of codebooks $\mathcal{B}(\mathcal{C}(e,\ell,\gamma,k))$ produced by this construction is at most

$$\phi(m) \sum_{\ell \geq 3,\, \ell | m} (2^{m/\ell}-1), \tag{21}$$

which is a huge number for large m.

We inform the reader that the function

$$\sum_{i=1}^{(m-1)/2} x^{2^{ki}+1} + \sum_{i=1}^{(\ell-1)/2} (\gamma x)^{2^{ek i}+1}$$

is not almost bent, according to our Magma test data. Hence, the construction of this section is really different from the construction of codebooks based on almost bent functions presented in Section V-B.

VI. SUMMARY AND CONCLUDING REMARKS

The contributions of this paper are the following:

1) The binary nonlinear codes in Theorem 12, which can be viewed as analogues of the Kerdock codes for odd m.
2) The generic construction of codebooks $\mathcal{B}(\mathcal{C})$ from binary codes $\mathcal{C}$ described in Theorem 4.
3) The three bounds on binary codes documented in Theorem 5, which are tight.
4) The extension of the previous construction of codebooks with certain subcodes of the Kerdock codes. With this extension the Kerdock code $\mathcal{K}(m)$ gives $2^{2^{2m-1}}$ codebooks meeting the Levenshtein bound. Hence, this is an substantial extension.
5) The generic construction of asymptotically optimal codebooks from a special type of binary codes described in Theorem 7. With this extension, a binary code with required parameters produces $2^{2^{2m}}$ such codebooks.
6) The construction of codebooks with a special type of linear codes given in Theorem 8, which is an extension of the construction of codebooks with almost bent functions proposed in [14].
7) A new construction of codebooks that almost meet the Levenshtein bound, which was documented in Theorem 13. The number of binary codes and codebooks produced by this construction is a huge number and is given in (21).
8) Combining this construction and the extension of Theorem 7, we obtain a total number of at most

$$2^{2^{2m}} \phi(m) \sum_{\ell \geq 3,\, \ell | m} (2^{m/\ell}-1)$$

codebooks with the parameters and the maximum crosscorrelation magnitudes of Theorem 7, which almost meet the Levenshtein bound of (2) and are asymptotically optimal.

Though a lot of bent and semi-bent functions are available in the literature, only a few sets of bent functions satisfying the conditions in Research Problem 1 and a few sets of semi-bent functions meeting the requirements in Research Problem 2 are known. It would be interesting to construct more such sets of bent functions and semi-bent functions.

Certain classes of binary linear codes in the literature may be plugged into the construction of Theorem 4 to obtain codebooks with good and new parameters. However, they may not meet the Welch or Levenshtein bounds, as these bounds are not tight in certain ranges. Below we present a few examples of codebooks with new parameters from a few classes of binary linear codes.

Theorem 14: Let m *be even, and let* $n=(2^m-1)/3$. *Let* $\beta=\alpha^3$, *where* α *is a generator of* $\mathrm{GF}(2^m)^*$. *Define*

$$\mathcal{C}(3,m) = \{(\mathrm{Tr}_1^m(a\beta^i))_{i=0}^{n-1} : a \in \mathrm{GF}(2^m)\}.$$

Then the set $\mathcal{B}(\mathcal{C}(3,m))$ *is a* $(2^{m+2}-1)/3, (2^m-1)/3)$ *codebook with the maximum crosscorrelation magnitude*

$$I_{\max}(\mathcal{B}(\mathcal{C}(3,m))) = \begin{cases} \frac{2^{(m+2)/2}+1}{2^m-1} & \text{if } \equiv 0 \pmod 4, \\ \frac{2^{(m+2)/2}-1}{2^m-1} & \text{if } \equiv 2 \pmod 4. \end{cases} \tag{22}$$

The information about the linear code $\mathcal{C}(3,m)$ can be found in [13].

Theorem 15: Let m *be odd. Let* $\mathcal{C}$ *be a binary linear code with length* $2^{m-1}-1$ *and dimension* m *such that*

$$w_{\min} = 2^{m-2} - 2^{\frac{m-3}{2}} \text{ and } w_{\max} = 2^{m-2} + 2^{\frac{m-3}{2}},$$

where $w_{\min}$ and $w_{\max}$ denote minimum nonzero weight and maximum weight in $\mathcal{C}$, respectively. Then the set $\mathcal{B}(\mathcal{C})$ is a $(3 \times 2^{m-1} - 1, 2^{m-1} - 1)$ codebook with the maximum crosscorrelation magnitude

$$I_{\max}(\mathcal{B}(\mathcal{C})) = \frac{2^{(m-1)/2} + 1}{2^{m-1} - 1}.$$

Linear codes in [15] can be plugged into Theorem 15 to produce codebooks with the parameters in Theorem 15. The codebooks in Theorems 14 and 15 may have the best possible parameters. But we need new and tight bounds to prove the optimality of these codebooks. Hence, an important research problem is to develop new and tight bounds on codebooks.

APPENDIX
PROOF OF LEMMA 10

Proof: The Walsh transform of the Boolean function $g_{(a,b)}(x)$ is given by

$$\hat{g}_{(a,b)}(w) = \sum_{x \in \mathrm{GF}(2^m)} (-1)^{g_{(a,b)}(x) + \mathrm{Tr}_1^m(wx)},$$

where $w \in \mathrm{GF}(2^m)$. We have then

$$\begin{aligned}
&\left(\hat{g}_{(a,b)}(w)\right)^2 \\
&= \sum_{x \in \mathrm{GF}(2^m)} \sum_{z \in \mathrm{GF}(2^m)} (-1)^{g_{(a,b)}(x) + g_{(a,b)}(z) + \mathrm{Tr}_1^m(w(x+z))} \\
&= \sum_{y \in \mathrm{GF}(2^m)} \sum_{x \in \mathrm{GF}(2^m)} (-1)^{g_{(a,b)}(x) + g_{(a,b)}(x+y) + \mathrm{Tr}_1^m(wy)} \\
&= \sum_{x \in \mathrm{GF}(2^m)} (-1)^{g_{(a,b)}(x) + \mathrm{Tr}_1^m(wx)} \sum_{y \in \mathrm{GF}(2^m)} (-1)^{B_{g_{(a,b)}}(x,y)},
\end{aligned} \tag{23}$$

where $B_{g_{(a,b)}}(x, y) := g_{(a,b)}(x) + g_{(a,b)}(y) + g_{(a,b)}(x + y)$. Note that

$$\begin{aligned}
&B_{g_{(a,b)}}(x, y) \\
&= B_{f_a}(x, y) + B_{f_b}(x, y) \\
&= \mathrm{Tr}_1^m\Big(y\Big[a\mathrm{Tr}_1^m(ax) + b\mathrm{Tr}_1^m(bx) + (a^2 + b^2)(1 + \gamma^2)x \\
&\qquad + a\gamma^2\mathrm{Tr}_e^m(ax) + b\gamma^2\mathrm{Tr}_e^m(bx)\Big]\Big).
\end{aligned} \tag{24}$$

We now consider the number of solutions $x \in \mathrm{GF}(2^m)$ of the following linear equation

$$\begin{aligned}
&a\mathrm{Tr}_1^m(ax) + b\mathrm{Tr}_1^m(bx) + (a^2 + b^2)(1 + \gamma^2)x \\
&\qquad + a\gamma^2\mathrm{Tr}_e^m(ax) + b\gamma^2\mathrm{Tr}_e^m(bx) = 0.
\end{aligned} \tag{25}$$

Obviously, $x = 0$ is a solution of (25). If (25) would have no nonzero solution x in $\mathrm{GF}(2^m)$, then by (23) we would have

$$\left(\hat{g}_{(a,b)}(w)\right)^2 = 2^m.$$

Note that $|\hat{g}_{(a,b)}(w)|$ is an integer. However, 2^m is not a square, as m is odd. This is a contradiction. Therefore, (25) has at least one nonzero solution $x \in \mathrm{GF}(2^m)$. Below we assume that x is a nonzero solution of (25) and prove the uniqueness of x.

Let

$$u = \mathrm{Tr}_e^m(ax) \text{ and } v = \mathrm{Tr}_e^m(bx).$$

Then (25) becomes

$$a\mathrm{Tr}_1^e(u) + b\mathrm{Tr}_1^e(v) + (a^2 + b^2)(1 + \gamma^2)x + a\gamma^2 u + b\gamma^2 v = 0. \tag{26}$$

Since $a \neq b$ and $\gamma \neq 1$, we have $(a^2 + b^2)(1 + \gamma^2) \neq 0$. It then follows from (26) that

$$x = \frac{a\mathrm{Tr}_1^e(u) + b\mathrm{Tr}_1^e(v) + a\gamma^2 u + b\gamma^2 v}{(a^2 + b^2)(1 + \gamma^2)}. \tag{27}$$

Put $c = \mathrm{Tr}_e^m(\frac{a}{a+b})$. We have

$$\begin{cases}
\mathrm{Tr}_e^m(\frac{b}{a+b}) = 1 + c, \\
\mathrm{Tr}_e^m(\frac{a^2}{a^2+b^2}) = c^2, \\
\mathrm{Tr}_e^m(\frac{b^2}{a^2+b^2}) = 1 + c^2, \\
\mathrm{Tr}_e^m(\frac{ab}{a^2+b^2}) = c + c^2.
\end{cases} \tag{28}$$

By (27), we get

$$u = \mathrm{Tr}_e^m(ax) = \mathrm{Tr}_e^m\left[\frac{a^2\mathrm{Tr}_1^e(u) + ab\mathrm{Tr}_1^e(v) + a^2\gamma^2 u + ab\gamma^2 v}{(a^2 + b^2)(1 + \gamma^2)}\right],$$

which gives

$$\begin{aligned}
&u(1 + \gamma^2) \\
&= \mathrm{Tr}_e^m\left[\frac{a^2}{a^2 + b^2}\mathrm{Tr}_1^e(u) + \frac{ab}{a^2 + b^2}\mathrm{Tr}_1^e(v)\right] \\
&\quad + \mathrm{Tr}_e^m\left[\frac{a^2}{a^2 + b^2}\gamma^2 u + \frac{ab}{a^2 + b^2}\gamma^2 v\right] \\
&= c^2\mathrm{Tr}_1^e(u) + (c + c^2)\mathrm{Tr}_1^e(v) + c^2\gamma^2 u + (c + c^2)\gamma^2 v \\
&= \left[\gamma^2(u + v) + \mathrm{Tr}_1^e(u) + \mathrm{Tr}_1^e(v)\right]c^2 + \left[\mathrm{Tr}_1^e(v) + \gamma^2 v\right]c.
\end{aligned} \tag{29}$$

Similarly, it follows from (27) and $v = \mathrm{Tr}_e^m(bx)$ that

$$\begin{aligned}
&v + \mathrm{Tr}_1^e(v) \\
&= \left[\gamma^2(u + v) + \mathrm{Tr}_1^e(u) + \mathrm{Tr}_1^e(v)\right]c^2 + \left[\mathrm{Tr}_1^e(u) + \gamma^2 u\right]c.
\end{aligned} \tag{30}$$

If $c = 0$, then we deduce from (29) and (30) that

$$u = 0 \text{ and } v + \mathrm{Tr}_1^e(v) = 0.$$

Hence,

$$(u, v) = (0, 0) \text{ or } (u, v) = (0, 1).$$

If $(u, v) = (0, 0)$, we would have $x = 0$, a contradiction to our assumption that $x \neq 0$. When $(u, v) = (0, 1)$, it follows from (27) that

$$x = \frac{b}{a^2 + b^2},$$

which is the unique nonzero solution of (25).

We now consider the case that $c \neq 0$. In this case, combining (29) and (30) yields

$$\gamma^2(u + v) + \mathrm{Tr}_1^e(u) + \mathrm{Tr}_1^e(v) = \frac{u(1 + \gamma^2) + v + \mathrm{Tr}_1^e(v)}{c}. \tag{31}$$

Plugging the expression of (31) into (29) and (30) gives

$$\begin{cases} u = c(u+v), \\ v + \mathrm{Tr}_1^e(v) = (u+v+\mathrm{Tr}_1^e(u+v))c. \end{cases} \tag{32}$$

We now claim that $u+v \neq 0$. Otherwise, by (32) we would have $(u,v)=0$ and thus $x=0$, which is contrary to the assumption that $x \neq 0$. Since $u+v \neq 0$, we deduce from (32) that

$$\begin{cases} u = c(u+v), \\ (u+v)^2 = u\mathrm{Tr}_1^e(u) + v\mathrm{Tr}_1^e(v). \end{cases} \tag{33}$$

Below we continue our discussion by distinguishing the following four cases.

Case 1: $(\mathrm{Tr}_1^e(u), \mathrm{Tr}_1^e(v)) = (0,0)$

If this case would happen, it would follow from (27) that

$$x = \frac{a\gamma^2 u + b\gamma^2 v}{(a^2+b^2)(1+\gamma^2)}. \tag{34}$$

By (28), we have

$$\begin{aligned} u &= \mathrm{Tr}_e^m(ax) \\ &= \frac{\gamma^2 u}{1+\gamma^2}\mathrm{Tr}_e^m\left(\frac{a^2}{a^2+b^2}\right) + \frac{\gamma^2 v}{1+\gamma^2}\mathrm{Tr}_e^m\left(\frac{ab}{a^2+b^2}\right) \\ &= \frac{\gamma^2(uc^2+v(c+c^2))}{1+\gamma^2}. \end{aligned} \tag{35}$$

Similarly, we have

$$\begin{aligned} v &= \mathrm{Tr}_e^m(bx) \\ &= \frac{\gamma^2(u(c+c^2)+v(1+c^2))}{1+\gamma^2}. \end{aligned} \tag{36}$$

Note that (35) and (36) form the following system of equations

$$\begin{cases} (1+\gamma^2)u = \gamma^2(uc^2+v(c+c^2)), \\ (1+\gamma^2)v = \gamma^2(u(c+c^2)+v(1+c^2)). \end{cases} \tag{37}$$

If $c=1$, then from (37) we deduce that $(u,v)=(0,0)$ and then $x=0$, which is a contradiction to our assumption that $x \neq 0$. Hence, $c \neq 1$. If $c+c^2 \neq 0$, we can also assume that $u \neq 0$ and $v \neq 0$, otherwise $x=0$. Under these assumptions, one can deduce from (37) that $\gamma = 1$, which is again a contradiction to the assumption that $\gamma \neq 1$.

In summary of the discussions above, we conclude that Case 1 cannot happen if $c \neq 0$.

Case 2: $(\mathrm{Tr}_1^e(u), \mathrm{Tr}_1^e(v)) = (1,1)$

In this case, it follows from (33) that $(u,v) = (c, 1+c)$. Plugging this (u,v) into (27) yields

$$x = \frac{a+b+a\gamma^2+b\gamma^2(1+c)}{(a^2+b^2)(1+\gamma^2)}.$$

If the value of x above is equal to 0, we have reached a contradiction. Otherwise, it is the unique nonzero solution we are looking for.

Case 3: $(\mathrm{Tr}_1^e(u), \mathrm{Tr}_1^e(v)) = (1,0)$

In this case, it follows from (33) that $(u,v) = (c^2, (1+c)c)$. Plugging this (u,v) into (27) yields

$$x = \frac{a+a\gamma^2c^2+b\gamma^2c(1+c)}{(a^2+b^2)(1+\gamma^2)}.$$

If the value of x above is equal to 0, we have reached a contradiction. Otherwise, it is the unique nonzero solution we are looking for.

Case 4: $(\mathrm{Tr}_1^e(u), \mathrm{Tr}_1^e(v)) = (0,1)$

In this case, it follows from (33) that $(u,v) = ((1+c)c, 1+c^2)$. Plugging this (u,v) into (27) yields

$$x = \frac{b+a\gamma^2c(1+c)+b\gamma^2(1+c^2)}{(a^2+b^2)(1+\gamma^2)}.$$

If the value of x above is equal to 0, we have reached a contradiction. Otherwise, it is the unique nonzero solution we are looking for.

In summary, (25) has only two solutions $x \in \mathrm{GF}(2^m)$. It then follows from (23) and (24) that $\left(\hat{g}_{(a,b)}(w)\right)^2 \in \{0, 2^{m+1}\}$. This completes the proof. □

ACKNOWLEDGMENTS

The authors are very grateful to the reviewers and the Associate Editor, Prof. Kyeongcheol Yang, for their comments and suggestions that very much improved the quality and presentation of this paper.

REFERENCES

[1] L. Budaghyan, C. Carlet, and A. Pott, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1141–1152, Mar. 2006.

[2] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," *Proc. London Math. Soc.*, vol. 75, no. 2, pp. 436–480, 1997.

[3] P. J. Cameron and J. J. Seidel, "Quadratic forms over $GF(2)$," *Indagationes Math.*, vol. 76, no. 1, pp. 1–8, 1973.

[4] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4–8, Jan. 2000.

[5] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397.

[6] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes, Cryptogr.*, vol. 15, no. 2, pp. 125–156, 1998.

[7] O. Christensen, *An Introduction to Frames and Riesz Bases*. Boston, MA, USA: Birkhäuser, 2003.

[8] J. H. Conway, R. H. Hardin, and N. J. A. Sloane, "Packing lines, planes, etc.: Packings in Grassmannian spaces," *Experim. Math.*, vol. 5, no. 2, pp. 139–159, 1996.

[9] P. Delsarte, J. M. Goethals, and J. J. Seidel, "Bounds for systems of lines and Jacobi polynomials," *Philips Res. Rep.*, vol. 30, pp. 91–105, Jan. 1975.

[10] C. Ding, "Complex codebooks from combinatorial designs," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4229–4235, Sep. 2006.

[11] C. Ding, *Codes from Difference Sets*. Singapore: World Scientific, 2015.

[12] C. Ding and T. Feng, "A generic construction of complex codebooks meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4245–4250, Nov. 2007.

[13] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Math.*, vol. 313, no. 4, pp. 434–446, 2013.

[14] C. Ding and J. Yin, "Signal sets from functions with optimum nonlinearity," *IEEE Trans. Commun.*, vol. 55, no. 5, pp. 936–940, May 2007.
[15] K. Ding and C. Ding, "Binary linear codes with three weights," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 1879–1882, Nov. 2014.
[16] M. Fickus, D. G. Mixon, and J. C. Tremain, "Steiner equiangular tight frames," *Linear Algebra Appl.*, vol. 436, no. 5, pp. 1014–1027, 2012.
[17] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154–156, Jan. 1968.
[18] H. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences," *Finite Fields Appl.*, vol. 7, no. 2, pp. 253–286, 2001.
[19] S. Hong, H. Park, J.-S. No, T. Helleseth, and Y.-S. Kim, "Near-optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3698–3705, Jun. 2014.
[20] X.-D. Hou, "A note on the proof of Niho's conjecture," *SIAM J. Discrete Math.*, vol. 18, no. 2, pp. 313–319, 2004.
[21] H. Hu and J. Wu, "New constructions of codebooks nearly meeting the Welch bound with equality," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1348–1355, Feb. 2014.
[22] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p-ary sequences with optimal correlation property and large linear span," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1839–1843, Aug. 2004.
[23] G. A. Kabatjanski and V. I. Levenstein, "Bounds for packing on a sphere and in space," *Probl. Inf. Transmiss.*, vol. 14, pp. 1–17, Jan. 1978.
[24] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed–Muller codes," *Inf. Control*, vol. 18, no. 4, pp. 369–394, 1971.
[25] A. M. Kerdock, "A class of low-rate nonlinear binary codes," *Inf. Control*, vol. 20, no. 2, pp. 182–187, 1972.
[26] S.-H. Kim and J.-S. No, "New families of binary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3059–3065, Nov. 2003.
[27] H. König, "Isometric imbeddings of Euclidean spaces into finite-dimensional ℓ_p-spaces," *Polish Acad. Sci.*, vol. 34, pp. 79–87, 1995.
[28] V. I. Levenshtein, "Bounds for packings of metric spaces and some of their applications," (in Russian), *Problems Cybern.*, vol. 40, pp. 43–110, 1983.
[29] R. Lidl and H. Niederreiter, *Finite Fields* (Encyclopedia of Mathematics and Its Applications), vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1983.
[30] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[31] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II*. New York, NY, USA: Springer-Verlag, 1993, pp. 63–78.
[32] S. Mesnager, "Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5996–6009, Sep. 2011.
[33] S. Mesnager, "Several new infinite families of bent functions and their duals," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4397–4407, Jul. 2014.
[34] S. Mesnager, "On semi-bent functions and related plateaued functions over the Galois field $\mathbb{F}_{2^n}$," in *Open Problems in Mathematics and Computational Science*. Berlin, Germany: Springer-Verlag, 2014, pp. 243–273.
[35] S. Mesnager, *Bent Functions: Fundamentals and Results*. Heidelberg, Germany: Springer-Verlag, 2015.
[36] O. S. Rothaus, "On 'bent' functions," *J. Combinat. Theory, A*, vol. 20, no. 3, pp. 300–305, 1976.
[37] D. V. Sarwate, "Meeting the Welch bound with equality," in *Sequences and Their Applications*. Berlin, Germany: Springer-Verlag, 1999, pp. 79–102.
[38] T. Strohmer and R. W. Heath, Jr., "Grassmannian frames with applications to coding and communication," *Appl. Comput. Harmon. Anal.*, vol. 14, no. 3, pp. 257–275, 2003.
[39] L. Welch, "Lower bounds on the maximum cross correlation of signals (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.
[40] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Ann. Phys.*, vol. 191, no. 2, pp. 363–381, 1989.
[41] P. Xia, S. Zhou, and G. B. Giannakis, "Achieving the Welch bound with difference sets," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1900–1907, May 2005.
[42] N. Y. Yu, "A construction of codebooks associated with binary sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5522–5533, Aug. 2012.
[43] N. Y. Yu, K. Feng, and A. X. Zhang, "A new class of near-optimal partial Fourier codebooks from an almost difference set," *Designs, Codes, Cryptogr.*, vol. 71, no. 3, pp. 493–501, 2014.
[44] A. Zhang and K. Feng, "Two classes of codebooks nearly meeting the Welch bound," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2507–2511, Apr. 2012.
[45] A. Zhang and K. Feng, "Construction of cyclotomic codebooks nearly meeting the Welch bound," *Designs, Codes, Cryptogr.*, vol. 63, no. 2, pp. 209–224, 2012.
[46] Z. Zhou, C. Ding, and N. Li, "New families of codebooks achieving the Levenstein bound," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7382–7387, Nov. 2014.

Can Xiang received the M.S degree in mathematics from Hainan Normal University, Haikou, China, in 2010. She is currently a Ph.D. student in the College of Mathematics and Information Science, Guangzhou University, Guangzhou, China. Her research interests include cryptography, coding theory and information security.

Cunsheng Ding (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are cryptography and coding theory. He has coauthored four research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.

Sihem Mesnager received the Ph.D. degree in Mathematics from the University of Pierre et Marie Curie (Paris VI), Paris, France, in 2002 and the Habilitation to Direct Theses (HDR) in Mathematics from the University of Paris VIII, France, in 2012. Currently, she is an associate Professor in Mathematics at the University of Paris VIII (France) in the laboratory LAGA (Laboratory of Analysis, Geometry and Applications), University of Paris XIII and CNRS. She is also Professor adjoint to Telecom ParisTech (France), research group MIC2 in mathematics of the department INFERES, Telecom ParisTech (ex. National high school of telecommunications). Her research interests include discrete Mathematics, Boolean functions, Cryptology, Coding theory, Commutative Algebra and Computational Algebraic Geometry. She is Editor in Chief of the *International Journal of Information and Coding Theory* (IJOCT) and an Associate Editor for the international journal IEEE TRANSACTIONS ON INFORMATION THEORY (IEEE-IT). She also serves the editorial board of the international journal *Advances in Mathematics of Communications* (AMC), the international journal *Cryptography and Communications Discrete Structures*, *Boolean Functions and Sequences* (CCDS) and the international journal *RAIRO ITA* (Theoretical Informatics and Applications). She was a program co-chair for two International Workshops and served on the board of program comitties of twelve international conferences and workshops. She is (co)-author for more than 56 articles, 2 books and gave approx. 60 national and international conferences. Since 2013, she is vice-president of the french Chapter of IEEE in information theory.