New Families of Codebooks Achieving the Levenstein Bound

Zhengchun Zhou, Cunsheng Ding, *Senior Member, IEEE*, and Nian Li

***Abstract*— In this paper, a construction of codebooks based on a set of bent functions satisfying certain conditions is introduced. It includes some earlier constructions of codebooks meeting the Levenstein bound as special cases. With this construction, two new families of codebooks achieving the Levenstein bound are obtained. The codebooks constructed in this paper could have a very small alphabet size.**

***Index Terms*— Codebook, signal set, packing, Levenstein bound, bent function.**

I. Introduction

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

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

where $\mathbf{c}^H$ stands for the conjugate transpose of the complex vector $\mathbf{c}$. For $I_{\max}(\mathcal{C})$, we have the following well known Welch bound [30].

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

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

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

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

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

A codebook achieving the equality in (1) is referred to as a maximum-Welch-bound-equality (MWBE) codebook [32]. The MWBE codebook is also known as an equiangular tight frame [5]. The construction of MWBE codebooks is equivalent to line packing in Grassmannian spaces [28]. As pointed out by Sarwate [27], the construction of an MWBE codebook is very hard in general. The known MWBE codebooks can be summarized as follows [8], [15].

1) (N, N) orthogonal MWBE codebooks for any $N > 1$ [27], [32].
2) $(N, N-1)$ MWBE codebooks for $N > 1$ generated from discrete Fourier transformation matrices [27], [32], or m-sequences [27].
3) (N, K) MWBE codebooks from conference matrices [6], [28], where $N = 2K = 2^{d+1}$ or $N = 2K = p^d + 1$, where p is a prime number and d is a positive integer.
4) (N, K) MWBE codebooks from (N, K, λ) difference sets in cyclic groups [32] and abelian groups [7], [8].
5) MWBE codebooks from $(2, k, v)$-Steiner systems [12].

Besides MWBE codebooks, codebooks nearly meeting the Welch bound have also received a lot of attention (see [14], [15], [33], [34], [36], [37], and references therein).

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

Lemma 2 ([28]): If $N > K(K+1)/2$, no (N, K) real codebook $\mathcal{C}$ can meet the Welch bound of (1); and if $N > K^2$, no (N, K) codebook $\mathcal{C}$ can meet the Welch bound of (1).

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

Lemma 3 ([17], [20]): For any real-valued codebook $\mathcal{C}$ with $N > K(K+1)/2$, we have

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

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

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

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

1) $(2^{2m-1} + 2^m, 2^m)$ codebooks generated from Kerdock codes [2], [31], where m is even. This class of real-valued codebooks is optimal with respect to the Levenstein bound of (2) and has alphabet 4.
2) $(p^{2m} + p^m, p^m)$ codebooks generated from perfect nonlinear functions [9], [31], where p is an odd prime.

Manuscript received May 15, 2014; revised August 19, 2014; accepted August 22, 2014. Date of publication September 4, 2014; date of current version October 16, 2014. Z. Zhou was supported by the Natural Science Foundation of China under Grant 61201243 and Grant 61373009. C. Ding was supported by the Research Grants Council, Hong Kong, under Project 600812.

Z. Zhou is with the School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China, and also with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: zzc@home.swjtu.edu.cn).

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

N. Li is with the Department of Mathematics, Hong Kong University of Science and Technology, Hong Kong (e-mail: nianli.2010@gmail.com).

Communicated by T. Helleseth, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2014.2353052

This class of codebooks is optimal with respect to the Levenstein bound of (3) and has alphabet size $p+2$.

Codebooks meeting the Welch bound or the Levenstein bound are preferred in many practical applications, for example, unitary space-time modulations, multiple description coding over erasure channels, direct spread CDMA communications, and coding theory [2], [25]. According to Sarwate [27], it is desirable to employ codebooks with a small alphabet size in applications.

In this paper, we give a construction of codebooks using a set of bent functions satisfying certain conditions. It includes aforementioned constructions of codebooks meeting the Levenstein bound as special cases. With this construction, two new families of codebooks achieving the Levenstein bounds are obtained. The codebooks constructed in this paper could have a very small alphabet size.

This paper is organized as follows. Section II presents preliminary notation and results which will be needed in subsequent sections. Section III presents a construction of codebooks from sets of bent functions meeting certain conditions. Section IV introduces two new families of codebooks meeting the Levenstein bound. Section V concludes this paper and makes some comments.

II. Preliminaries

Throughout this paper, we adopt the following notation unless otherwise stated:

- p is a prime, m is a positive integer.
- ω_p is a primitive p-th complex root of unity.
- For any positive integer $\ell | m$, $\mathrm{Tr}_\ell^m(x)$ is the trace function from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p^\ell)$.

Let $f : \mathrm{GF}(p^m) \to \mathrm{GF}(p)$ be a p-ary function in m variables. It is said to be a bent function if $|\widehat{f}(\lambda)| = p^{m/2}$ for all $\lambda \in \mathrm{GF}(p^m)$, where

$$\widehat{f}(\lambda) = \sum_{x \in \mathrm{GF}(p^m)} {\omega_p}^{f(x) - \mathrm{Tr}_1^m(\lambda x)}$$

is called the Walsh spectrum of f at the point λ.

A binary bent function (i.e., $p = 2$) is usually called a Boolean bent function. It is well known that a binary bent function only exists for even m [26], while for odd p, p-ary bent functions exist for both even and odd m [19]. Bent functions have been extensively studied for their numerous applications in cryptography, coding theory, combinatorics, and other fields. We refer to [4] and [19] for more information on bent functions.

Identifying $\mathrm{GF}(p^m)$ with the m-dimensional $\mathrm{GF}(p)$-vector space $\mathrm{GF}(p)^m$, a function f from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$ can be regarded as an m-variable polynomial on $\mathrm{GF}(p)$. The former is called a quadratic form over $\mathrm{GF}(p)$ if the latter is a homogeneous polynomial of degree two:

$$f(x_1, x_2, \ldots, x_m) = \sum_{1 \le i \le j \le m} a_{ij} x_i x_j$$

where $a_{ij} \in \mathrm{GF}(p)$, and we use a basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ of $\mathrm{GF}(p^m)$ over $\mathrm{GF}(p)$ and identity $x = \sum_{i=1}^m x_i \beta_i$ with the vector $(x_1, x_2, \ldots, x_m) \in \mathrm{GF}(p)^m$. The rank of the quadratic form $f(x)$ is defined as the codimension of the $\mathrm{GF}(p)$-vector space

$$V = \{y \in \mathrm{GF}(p^m) |\ f(x+y) - f(x) - f(y) = 0 \quad \text{for all } x \in \mathrm{GF}(p^m)\}.$$

That is $|V| = p^{m-r}$ where r is the rank of $f(x)$. Quadratic forms over finite fields have been extensively studied. They can be used to construct bent functions [21], [35], sequences with low correlation [1], [16], [18], [29], and error-correcting codes with excellent minimal distance [10], [24]. The interested reader is referred to [23] for a detailed discussion of the theory of quadratic forms over finite fields.

Lemma 4 ([23]): Let $f(x)$ be a quadratic form from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$ with full rank m. Then

$$\left| \sum_{x \in \mathrm{GF}(p^m)} {\omega_p}^{f(x) - \mathrm{Tr}_1^m(\lambda x)} \right| = p^{m/2}$$

for any $\lambda \in \mathrm{GF}(p^m)$.

Lemma 4 tells us that $f(x)$ is a bent function if it is a quadratic form from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$ with full rank.

III. A Construction of Codebooks From Sets of Bent Functions

In this section, we shall present a generic construction of codebooks. With this construction, both known and new optimal codebooks meeting the Levenstein bound can be generated.

Throughout this section, we use $\xi_0, \xi_1, \ldots, \xi_{p^m-1}$ to denote all of the elements of the finite field $\mathrm{GF}(p^m)$, and use E_{p^m} to denote the set formed by the standard basis of the p^m-dimensional Hilbert space:

$$\begin{gathered}(1,0,0,\ldots,0,0),\\(0,1,0,\ldots,0,0),\\\vdots\\(0,0,0,\ldots,0,1).\end{gathered}$$

Theorem 1: Let $\mathcal{F}$ be a set of bent functions from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$ satisfying the following properties:

1. *each function in $\mathcal{F}$ is bent; and*
2. *the difference of any two distinct functions in $\mathcal{F}$ is also bent.*

Construct a codebook $\mathcal{C}_\mathcal{F}$ as

$$\mathcal{C}_\mathcal{F} = \bigcup_{f \in \mathcal{F}} \mathcal{S}_f \bigcup \mathcal{S}_\mathbf{0} \bigcup E_{p^m} \tag{4}$$

where

$$\mathcal{S}_\mathbf{0} = \left\{ \frac{1}{\sqrt{p^m}} \left(\omega_p^{\mathrm{Tr}_1^m(\lambda\xi_0)}, \omega_p^{\mathrm{Tr}_1^m(\lambda\xi_1)}, \ldots, \omega_p^{\mathrm{Tr}_1^m(\lambda\xi_{p^m-1})} \right) \middle| \lambda \in \mathrm{GF}(p^m) \right\}$$

and for each $f \in \mathcal{F}$,

$$\mathcal{S}_f = \left\{ \frac{1}{\sqrt{p^m}} \left(\omega_p^{f(\xi_0)+\mathrm{Tr}_1^m(\lambda\xi_0)}, \omega_p^{f(\xi_1)+\mathrm{Tr}_1^m(\lambda\xi_1)}, \ldots, \omega_p^{f(\xi_{p^m-1})+\mathrm{Tr}_1^m(\lambda\xi_{p^m-1})} \right) \middle| \lambda \in \mathrm{GF}(p^m) \right\}.$$

Then $\mathcal{C}_{\mathcal{F}}$ is a $((|\mathcal{F}|+1)\cdot p^m + p^m, p^m)$ codebook with $I_{\max}(\mathcal{C}_{\mathcal{F}}) = \frac{1}{\sqrt{p^m}}$ and alphabet size $p+2$.

Proof: The conclusion follows directly from the definition of $\mathcal{C}_{\mathcal{F}}$, and the properties of bent functions, trace functions, and an orthogonal basis. ■

The following theorem shows that the codebook $\mathcal{C}_{\mathcal{F}}$ in Theorem 1 could meet the Levenstein bound provided that the function set $\mathcal{F}$ has an appropriate family size.

Theorem 2: Let $\mathcal{C}_{\mathcal{F}}$ be the codebook in Theorem 1. Then we have the following:

1. *$\mathcal{C}_{\mathcal{F}}$ is an optimal $(2^{2m-1}+2^m, 2^m)$ codebook meeting the bound of (2) if $p=2$ and $|\mathcal{F}| = 2^{m-1}-1$; and*
2. *$\mathcal{C}_{\mathcal{F}}$ is an optimal $(p^{2m}+p^m, p^m)$ codebook meeting the bound of (3) if p is an odd prime and $|\mathcal{F}| = p^m - 1$.*

Proof: When $p=2$ and $|\mathcal{F}| = 2^{m-1}-1$, according to Theorem 1, $\mathcal{C}_{\mathcal{F}}$ is a $(2^{2m-1}+2^m, 2^m)$ codebook with $I_{\max}(\mathcal{C}_{\mathcal{F}}) = \frac{1}{\sqrt{2^m}}$. Note that the alphabet of $\mathcal{C}_{\mathcal{F}}$ is $\{\pm\frac{1}{\sqrt{2^m}}, 0, 1\}$. Thus each vector in $\mathcal{C}_{\mathcal{F}}$ is real-valued. Take $N = 2^{2m-1}+2^m$ and $K = 2^m$. The Levenstein bound of (2) then becomes

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

Therefore the codebook $\mathcal{C}_{\mathcal{F}}$ meets the Levenstein bound of (2) and is thus optimal. Similarly, When p is odd and $|\mathcal{F}| = p^m - 1$, we can prove that $\mathcal{C}_{\mathcal{F}}$ meets the Levenstein bound of (3) and is thus optimal. ■

It can be seen from Theorem 2 that the key to the construction of an optimal codebook is to obtain a set of bent functions satisfying aforementioned properties with family size $2^{m-1}-1$ for $p=2$ and p^m-1 for odd p.

We now point out that some earlier optimal constructions can be viewed as special cases of Theorem 1.

- Let $p=2$ and m be even. For any $a \in \mathrm{GF}(2^{m-1})^*$, define a function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ as

  $$f_a(x) = R(ax_1) + x_2\mathrm{Tr}_1^{m-1}(ax_1)$$

  where we identify $\mathrm{GF}(2^m)$ with $\mathrm{GF}(2^{m-1})\times\mathrm{GF}(2)$, $x=(x_1,x_2)$ with $x_1\in\mathrm{GF}(2^{m-1})$ and $x_2\in\mathrm{GF}(2)$, and $R(x)$ is a function from $\mathrm{GF}(2^{m-1})$ to $\mathrm{GF}(2)$ given by

  $$R(x_1) = \sum_{i=1}^{(m-2)/2} \mathrm{Tr}_1^{m-1}(x_1^{2^i+1}). \tag{5}$$

  It turns out (see [24, Th. 18, p. 460]) that each $f_a(x)$ is a bent function, and for each nonzero $a \neq b$, the difference $f_a(x) - f_b(x)$ is also a bent function. Define

  $$\mathcal{F} = \{f_a(x) | a \in \mathrm{GF}(2^{m-1})^*\}.$$

  Note that $\mathcal{F}$ has family size $2^{m-1}-1$. The set $\mathcal{C}_{\mathcal{F}}$ is an optimal $(2^{2m-1}+2^m, 2^m)$ codebook. This class of real-valued codebooks are exactly the ones constructed from Kerdock codes by Calderbank *et al.* [2].
- Let p be an odd prime. A function $f(x)$ from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p^m)$ is referred to as perfect nonlinear if

  $$\max_{a\in\mathrm{GF}(p^m)^*}\max_{b\in\mathrm{GF}(p^m)} |\{x\in\mathrm{GF}(p^m) | f(x+a)-f(x)=b\}| = 1.$$

  Let $\pi(x)$ be a perfect nonlinear function from $\mathrm{GF}(p^m)$ to itself. It is easily checked that

  $$\mathcal{F} = \{\mathrm{Tr}_1^m(a\pi(x)) : a \in \mathrm{GF}(p^m)^*\}$$

  is a set of bent functions from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$, and the difference of any two distinct functions in $\mathcal{F}$ is also bent. The codebook $\mathcal{C}_{\mathcal{F}}$ generated from $\mathcal{F}$ is thus an optimal $(p^{2m}+p^m, p^m)$ codebook. When $\pi(x)=x^2$, the codebook $\mathcal{C}_{\mathcal{F}}$ was proposed by Wootters and Fields [31]. The codebooks for general perfect nonlinear function $\pi(x)$ were suggested by Ding and Yin in [9].

IV. Two New Families of Codebooks Meeting the Levenstein Bounds

In this section, we present two new families of codebooks meeting the Levenstein bound by employing the construction in Theorem 1.

A. The First Family of Optimal Codebooks

In this subsection, we present a family of real-valued codebooks with alphabet size 4.

Theorem 3: Let $p=2$, m be even with $m-1=\ell e$ for two positive integers ℓ and e, and k be any positive integer with $\gcd(k, m-1)=1$. Let γ be a fixed element in $\mathrm{GF}(2^e)$ with $\gamma \neq 1$. Define a set of functions from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ as

$$\mathcal{F} = \{f_a(x) | a \in \mathrm{GF}(2^{m-1})^*\}.$$

Herein,

$$f_a(x) = P(ax_1) + Q(\gamma ax_1) + x_2\mathrm{Tr}_1^{m-1}(ax_1) \tag{6}$$

where we identify $\mathrm{GF}(2^m)$ with $\mathrm{GF}(2^{m-1})\times\mathrm{GF}(2)$, $x=(x_1,x_2)$ with $x_1\in\mathrm{GF}(2^{m-1})$ and $x_2\in\mathrm{GF}(2)$, $P(x_1)$ and $Q(x_1)$ are respectively given by

$$P(x_1) = \sum_{i=1}^{(m-2)/2} \mathrm{Tr}_1^{m-1}(x_1^{2^{ki}+1}) \tag{7}$$

and

$$Q(x_1) = \sum_{i=1}^{(\ell-1)/2} \mathrm{Tr}_1^{m-1}(x_1^{2^{eki}+1}). \tag{8}$$

Let $\mathcal{C}_{\mathcal{F}}$ be the codebook defined in (4). Then $\mathcal{C}_{\mathcal{F}}$ is an optimal real-valued $(2^{2m-1}+2^m, 2^m)$ codebook with alphabet size 4.

Remark 1: When $k=1$, $P(x_1)=R(x_1)$, where $R(x_1)$ is defined by (5). Thus, when $k=1$ and $\gamma=0$, the codebook $\mathcal{C}_{\mathcal{F}}$ in Theorem 3 is exactly the codebook from the Kerdock codes reported in [2].

In order to prove Theorem 3, we need the following lemmas.

Lemma 5 ([18],[24]): For the functions $P(x_1)$ and $Q(x_1)$ defined by (7) and (8), we have

$$P(x_1) + P(z_1) + P(x_1+z_1) = \mathrm{Tr}_1^{m-1}(z_1(x_1 + \mathrm{Tr}_1^{m-1}(x_1)))$$

and

$$Q(x_1) + Q(z_1) + Q(x_1+z_1) = \mathrm{Tr}_1^{m-1}(z_1(x_1 + \mathrm{Tr}_e^{m-1}(x_1))).$$

Lemma 6: Let $f_a(x)$ be the function defined by (6). Then $f_a(x)$ is a bent function for any $a \in \mathrm{GF}(2^{m-1})^*$.

Proof: Note that $f_a(x)$ is a quadratic form in m variables for any nonzero a. Thus it is sufficient to prove that $f_a(x)$ has full rank m. To this end, we need to consider the associated symplectic form of $f_a(x)$ which is given by

$$\begin{aligned} B_{f_a}(x,z) &= f_a(x) + f_a(z) + f_a(x+z) \\ &= P(ax_1) + P(az_1) + P(a(x_1+z_1)) + Q(\gamma a x_1) \\ &\quad + Q(\gamma a z_1) + Q(\gamma a(x_1+z_1)) + x_2 \mathrm{Tr}_1^{m-1}(ax_1) \\ &\quad + z_2 \mathrm{Tr}_1^{m-1}(az_1) + (x_2+z_2)\mathrm{Tr}_1^{m-1}(a(x_1+z_1)) \\ &= \mathrm{Tr}_1^{m-1}(z_1(a\mathrm{Tr}_1^{m-1}(ax_1) + a^2(1+\gamma^2)x_1 \\ &\quad + a\gamma^2 \mathrm{Tr}_e^{m-1}(ax_1) + ax_2)) + z_2 \mathrm{Tr}_1^{m-1}(ax_1) \end{aligned} \tag{9}$$

where $x = (x_1, x_2) \in \mathrm{GF}(2^{m-1}) \times \mathrm{GF}(2)$, $z = (z_1, z_2) \in \mathrm{GF}(2^{m-1}) \times \mathrm{GF}(2)$, and the last equality follows from Lemma 5. By (9), it is clear that $B_{f_a}(x,z) = 0$ for all z if and only if

$$\begin{cases} a\mathrm{Tr}_1^{m-1}(ax_1) + a^2(1+\gamma^2)x_1 + a\gamma^2 \mathrm{Tr}_e^{m-1}(ax_1) + ax_2 = 0, \\ \mathrm{Tr}_1^{m-1}(ax_1) = 0 \end{cases} \tag{10}$$

which implies that

$$(1+\gamma^2)ax_1 + \gamma^2 \mathrm{Tr}_e^{m-1}(ax_1) + x_2 = 0.$$

It then can be deduced that $ax_1 \in \mathrm{GF}(2^e)$ since $\gamma \in \mathrm{GF}(2^e)$ and $x_2 \in \mathrm{GF}(2)$. Thus $\mathrm{Tr}_e^{m-1}(ax_1) = ax_1 \mathrm{Tr}_e^{m-1}(1) = ax_1$ since $m-1$ is odd. It then follows from (10) that $ax_1 + x_2 = 0$ and thus $ax_1 \in \mathrm{GF}(2)$. By the second equation of (10), we have $x_2 = ax_1 = \mathrm{Tr}_1^{m-1}(ax_1) = 0$. Thus Equation (10) has only one solution $x = (x_1, x_2) = 0$ in $\mathrm{GF}(2^m)$. This means that the quadratic form $f_a(x)$ has full rank m and is thus a bent function. The proof of this lemma is completed. ■

Lemma 7: Let $f_a(x)$ be the function defined by (6). Then $f_a(x) - f_b(x)$ is a bent function for any $a \neq b \in \mathrm{GF}(2^{m-1})^*$.

Proof: Let $g_{(a,b)}(x) = f_a(x) - f_b(x)$. Note that $g_{(a,b)}(x)$ is a quadratic form in m variables for any $a \neq b$. We only need to prove that $g_{(a,b)}(x)$ has full rank m for any given $a \neq b$. A routine computation based on (9) together with the the fact $\gamma \in \mathrm{GF}(2^e)$ shows that

$$\begin{aligned} B_{g_{(a,b)}}(x,z) &= B_{f_a}(x,z) + B_{f_b}(x,z) \\ &= \mathrm{Tr}_1^{m-1}(z_1(a\mathrm{Tr}_1^{m-1}(ax_1) + b\mathrm{Tr}_1^{m-1}(bx_1) \\ &\quad + a\gamma^2 \mathrm{Tr}_1^{m-1}(ax_1) + b\gamma^2 \mathrm{Tr}_e^{m-1}(bx_1) \\ &\quad + (a^2+b^2)(1+\gamma^2)x_1 + (a+b)x_2)) \\ &\quad + z_2 \mathrm{Tr}_1^{m-1}(ax_1 + bx_1) \end{aligned} \tag{11}$$

where $x = (x_1, x_2) \in \mathrm{GF}(2^{m-1}) \times \mathrm{GF}(2)$, $z = (z_1, z_2) \in \mathrm{GF}(2^{m-1}) \times \mathrm{GF}(2)$. It then follows from (11) that $B_{g_{(a,b)}}(x,z) = 0$ for all $z \in \mathrm{GF}(2^m)$ if and only if

$$\begin{cases} a\mathrm{Tr}_1^{m-1}(ax_1) + b\mathrm{Tr}_1^{m-1}(bx_1) + a\gamma^2 \mathrm{Tr}_e^{m-1}(ax_1) \\ + b\gamma^2 \mathrm{Tr}_e^{m-1}(bx_1) + (a^2+b^2)(1+\gamma^2)x_1 + (a+b)x_2 = 0, \\ \mathrm{Tr}_1^{m-1}(ax_1 + bx_1) = 0 \end{cases} \tag{12}$$

which leads to

$$\begin{aligned} (a+b)\mathrm{Tr}_1^{m-1}(ax_1) + a\gamma^2 \mathrm{Tr}_e^{m-1}(ax_1) + b\gamma^2 \mathrm{Tr}_e^{m-1}(bx_1) \\ + (a^2+b^2)(1+\gamma^2)x_1 + (a+b)x_2 = 0. \end{aligned} \tag{13}$$

Let $u = \mathrm{Tr}_e^{m-1}(ax_1)$ and $v = \mathrm{Tr}_e^{m-1}(bx_1)$. It is clear that $\mathrm{Tr}_1^e(u) = \mathrm{Tr}_1^e(v)$ due to the second equation in (12). In terms of u and v, (13) becomes

$$\begin{aligned} (a+b)\mathrm{Tr}_1^e(u) + a\gamma^2 u + b\gamma^2 v + (a^2+b^2)(1+\gamma^2)x_1 \\ + (a+b)x_2 = 0 \end{aligned} \tag{14}$$

which yields

$$x_1 = \frac{(a+b)\mathrm{Tr}_1^e(u) + a\gamma^2 u + b\gamma^2 v + (a+b)x_2}{(a^2+b^2)(1+\gamma^2)}. \tag{15}$$

Let $c = \mathrm{Tr}_e^{m-1}(\frac{a}{a+b})$. We have

$$\begin{cases} \mathrm{Tr}_e^{m-1}(\frac{b}{a+b}) = 1 + c, \\ \mathrm{Tr}_e^{m-1}(\frac{a^2}{a^2+b^2}) = c^2, \\ \mathrm{Tr}_e^{m-1}(\frac{b^2}{a^2+b^2}) = 1 + c^2, \\ \mathrm{Tr}_e^{m-1}(\frac{ab}{a^2+b^2}) = c + c^2. \end{cases} \tag{16}$$

Note that $u = \mathrm{Tr}_e^{m-1}(ax_1)$ and $v = \mathrm{Tr}_e^{m-1}(bx_1)$. It then follows from (15) and the identities in (16) that

$$\begin{cases} \gamma^2(u+v)c^2 + (\gamma^2 v + \mathrm{Tr}_1^e(u) + x_2)c = (1+\gamma^2)u, \\ \gamma^2(u+v)c^2 + (\gamma^2 u + \mathrm{Tr}_1^e(u) + x_2)c = v + \mathrm{Tr}_1^e(u) + x_2. \end{cases} \tag{17}$$

If $c = 0$, it is clear that $u = 0$, $v + x_2 = 0$, and thus $v \in \mathrm{GF}(2)$. Recall that $\mathrm{Tr}_1^e(u) = \mathrm{Tr}_1^e(v)$ and e is odd, we have $v = \mathrm{Tr}_1^e(v) = \mathrm{Tr}_1^e(u) = 0$ and $x_2 = 0$. If $c \neq 0$, adding the two equations in (17), we have

$$\gamma^2(u+v) = \frac{(1+\gamma^2)u + v + \mathrm{Tr}_1^e(u) + x_2}{c}. \tag{18}$$

Using the right hand of this equation to substitute $\gamma^2(u+v)$ in the first equation of (17), we arrive at

$$\begin{aligned} &((1+\gamma^2)u + v + \mathrm{Tr}_1^e(u) + x_2)c + (\gamma^2 v + \mathrm{Tr}_1^e(u) + x_2)c \\ &\quad = (1+\gamma^2)u \end{aligned}$$

which leads to

$$(1+\gamma^2)uc + (1+\gamma^2)vc = (1+\gamma^2)u. \tag{19}$$

Recall that $\gamma \neq 1$, thus $1 + \gamma^2 \neq 0$. It then follows from (19) that

$$(c+1)u + vc = 0.$$

Similarly, using the right hand of (18) to substitute $\gamma^2(u+v)$ in the second equation of (17), one has

$$cu + (c+1)v = \epsilon$$

where $\epsilon = \mathrm{Tr}_1^e(u) + x_2 \in \mathrm{GF}(2)$. Therefore we obtain the following system of equations:

$$\begin{cases} (c+1)u + cv = 0, \\ cu + (c+1)v = \epsilon. \end{cases}$$

If $c = 1$, we immediately have $v = 0, u = \epsilon = x_2$. Thus $x_2 = u = \mathrm{Tr}_1^e(u) = \mathrm{Tr}_1^e(v) = 0$. On the other hand, for $c \neq 1$, we have

$$\begin{cases} u = \epsilon c, \\ v = \epsilon(c+1). \end{cases}$$

Thus $v = u+\epsilon$. It follows again from the fact $\mathrm{Tr}_1^e(u) = \mathrm{Tr}_1^e(v)$ that $\epsilon = 0$ since $\epsilon \in \mathrm{GF}(2)$. This means that $u = v = 0$ and $x_2 = 0$.

It can be seen from the analysis above that $u = v = 0$ and $x_2 = 0$ for any c (i.e., for any $a \neq b$). By (15), we have $x_1 = 0$. Thus Equation (12) has only one solution $x = (x_1, x_2) = 0$ in $\mathrm{GF}(2^m)$. This means that $f_a - f_b$ is bent and finishes the proof of this lemma. ■

Applying Lemmas 6 and 7, and Theorem 2, we immediately get the conclusion in Theorem 3.

Example 1: Let $m = 10$, $e = 3$, $\ell = 3$, $k = 1$. *Then* $P(x_1)$ *in (7) and* $Q(x_1)$ *in (8) are respectively given by* $P(x_1) = \mathrm{Tr}_1^9(x_1^3 + x_1^5 + x_1^9 + x_1^{17})$ *and* $Q(x_1) = \mathrm{Tr}_1^9(x_1^9)$. *By Theorem 3, for any given element* γ *in* $\mathrm{GF}(2^3)$ *with* $\gamma \neq 1$, $\mathcal{C}_{\mathcal{F}}$ *is an optimal* $(2^{19} + 2^{10}, 2^{10})$ *codebook with* $I_{\max}(\mathcal{C}_{\mathcal{F}}) = \frac{1}{2^5}$. *This example is also verified by a computer program.*

B. The Second Family of Optimal Codebooks

The second family of codebooks is complex-valued and is based on the Helleseth-Gong function [13]. Before introducing this family of codebooks, we first recall the definition of the Helleseth-Gong function.

Let p be an odd prime. The Helleseth-Gong (HG) function $H(x)$ from $\mathrm{GF}(p^m)$ to $\mathrm{GF}(p)$ is defined by

$$H(x) = \mathrm{Tr}_1^m\left(\sum_{i=0}^{\ell} u_i x^{(p^{2ki}+1)/2}\right) \tag{20}$$

where $m = (2\ell + 1)k$, $1 \leq s \leq 2\ell$ is an integer such that $\gcd(s, 2\ell + 1) = 1$, $b_0 = 1$, $b_{is} = (-1)^i$ and $b_i = b_{2\ell+1-i}$ for $i = 1, 2, \ldots, \ell$, $u_0 = b_0/2 = (p + 1)/2$, and $u_i = b_{2i}$ for $i = 1, 2, \ldots, \ell$. Herein, all the indexes of b's are taken mod $(2\ell + 1)$. From the HG function $H(x)$, we can get a set of bent functions with desirable properties. The following result was proved by Jang *et al.* [16, p. 1842].

Lemma 8: Let $H(x)$ *be the HG function defined by (20). Then for any* $a \in \mathrm{GF}(p^m)^*$, $H(ax^2)$ *is a bent function. Furthermore, for any* $a \neq b \in \mathrm{GF}(p^m)^*$, $H(ax^2) - H(bx^2)$ *is also a bent function.*

Theorem 4: Let $\mathcal{F}$ *be a set of functions from* $\mathrm{GF}(p^m)$ *to* $\mathrm{GF}(p)$ *defined by*

$$\mathcal{F} = \{H(ax^2) | a \in \mathrm{GF}(p^m)^*\}$$

where $H(x)$ *is the HG function in (20). Then* $\mathcal{C}_{\mathcal{F}}$ *is an optimal complex-valued* $(p^{2m} + p^m, p^m)$ *codebook with alphabet size* $p + 2$.

Proof: The conclusion follows directly from Lemma 8 and Theorem 1. ■

Example 2: Let $p = 3$ *and* $m = 5$, *and the HG function in (20) be given by* $H(x) = 2\mathrm{Tr}_1^5(x) + 2\mathrm{Tr}_1^5(x^5) + \mathrm{Tr}_1^5(x^{41})$. *By Theorem 4,* $\mathcal{C}_{\mathcal{F}}$ *is an optimal* $(3^{10} + 3^5, 3^5)$ *codebook with* $I_{\max}(\mathcal{C}_{\mathcal{F}}) = \frac{1}{\sqrt{3^5}}$. *This example is also verified by a computer program.*

Example 3: Let $p = 5$ *and* $m = 3$, *and the HG function in (20) be given by* $H(x) = 3\mathrm{Tr}_1^3(x) + 4\mathrm{Tr}_1^3(x^{13})$. *By Theorem 4,* $\mathcal{C}_{\mathcal{F}}$ *is an optimal* $(5^6 + 5^3, 5^3)$ *codebook with* $I_{\max}(\mathcal{C}_{\mathcal{F}}) = \frac{1}{\sqrt{5^3}}$. *This example is also verified by a Magma program.*

V. Concluding Remarks

In this paper, we proposed a construction of codebooks with sets of bent functions satisfying certain conditions. The codebooks generated by the construction can meet the Levenstein bound provided that the underlying sets of bent functions have appropriate family size. By introducing two classes of such sets of bent functions, we obtained two new families of optimal codebooks. It would be possible to search for more sets of bent functions leading to more optimal codebooks. The reader is invited to join the adventure.

Finally, we would mention an application of codebooks achieving the Levenstein bound in compressed sensing. Compressed sensing is a novel sampling theory, which provides a fundamentally new approach to data acquisition. A central problem in compressed sensing is the construction of the sensing matrix. For more information on the theory of compressed sensing, the reader is referred to Donoho [11] and Candès and Tao [3]. Very recently, Li and Ge [22] found that codebooks achieving the Levenstein bound can be used to construct deterministic sensing matrices with smallest coherence. The numerical experiments conducted in [22] showed that the sensing matrices from some known codebooks meeting the Levenstein bound have a good performance. It would be interesting to investigate the application of the new families of codebooks meeting the Levenstein bound presented in this paper using the framework developed in [22].

Acknowledgments

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

References

[1] S. Boztas and P. V. Kumar, “Binary sequences with Gold-like correlation but larger linear span,” *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 532–537, Mar. 1994.

[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. 3, pp. 436–480, 1997.

[3] E. J. Candès and T. Tao, “Decoding by linear programming,” *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

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

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

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

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

[8] 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.

[9] C. Ding and J. Yin, “Signal sets from functions with optimum nonlinearity,” *IEEE Trans. Commun.*, vol. 55, no. 5, pp. 936–940, May 2007.

[10] C. Ding and T. Helleseth, “Optimal ternary cyclic codes from monomials,” *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5898–5904, Sep. 2013.

[11] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[12] M. Fickus, D. G. Mixon, and J. C. Tremain, "Steiner equiangular tight frames," *Linear Algebra Appl.*, vol. 436, no. 5, pp. 1014–1027, 2012.

[13] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation," *IEEE Trans. Inf. Theory,* vol. 48, no. 11, pp. 2868–2872, Nov. 2002.

[14] S. Hong, H. Park, J. 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.

[15] 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.

[16] 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. 1839–1844, Aug. 2004.

[17] G. A. Kabatyanskii and V. I. Levenstein, "Bounds for packing on a sphere and in space," *Problems Inf. Transmiss.*, vol. 14, pp. 1–17, 1978.

[18] S. H. Kim and J. S. No, "New families of binary sequences with low cross correlation property," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 3059–3065, Nov. 2003.

[19] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combinat. Theory, Ser. A*, vol. 40, no. 1, pp. 90–107, 1985.

[20] V. I. Levenstein, "Bounds for packings of metric spaces and some of their applications," (in Russian), *Problems Cybern.*, vol. 40, pp. 43–110, 1983.

[21] N. Li, X. Tang, and T. Hellseth, "New constructions of quadratic bent functions in polynomial form," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5760–5767, Sep. 2014.

[22] S. Li and G. Ge, "Deterministic sensing matrices arising from near orthogonal systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2291–2302, Apr. 2014.

[23] R. Lidl and H. Niederreiter, *Finite Fields* (Encyclopedia of Mathematics), vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1983.

[24] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library). Amsterdam, The Netherlands: North Holland, 1977.

[25] 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.

[26] O. S. Rothaus, "On 'bent' functions," *J. Combinat. Theory, Ser. A*, vol. 20, no. 3, pp. 300–305, 1976.

[27] D. V. Sarwate, "Meeting the Welch bound with equality," in *Sequences and their Applications*. Berlin, Germany: Springer-Verlag, 1999, pp. 79–102.

[28] T. Strohmer and R. W. Heath, Jr., "Grassmannian frames with applications to coding and communication," *Appl. Comput. Harmonic Anal.*, vol. 14, no. 3, pp. 257–275, 2003.

[29] X. Tang, T. Helleseth, L. Hu, and W. Jiang "Two new families of optimal binary sequences obtained from quaternary sequences," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1833–1840, Apr. 2009.

[30] 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.

[31] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Ann. Phys.*, vol. 191, no. 2, pp. 363–381, 1989.

[32] 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.

[33] N. Y. Yu, "A construction of codebooks associated with binary sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5522–5533, Aug. 2012.

[34] 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 Cryptograph.*, vol. 71, no. 3, pp. 493–501, 2014.

[35] N. Y. Yu and G. Gong, "Constructions of quadratic bent functions in polynomial forms," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3291–3299, Jul. 2006.

[36] 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.

[37] A. Zhang and K. Feng, "Construction of cyclotomic codebooks nearly meeting the Welch bound," *Designs, Codes Cryptograph.*, vol. 63, no. 2, pp. 209–224, 2012.

Zhengchun Zhou received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Southwest Jiaotong University, Chengdu, China, in 2001, 2004, and 2010, respectively. From 2012 to 2013, he was a postdoctoral member in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. From 2013 to 2014, he was a research associate in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. Since 2001, he has been in the Department of Mathematics, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design and coding theory.

Dr. Zhou was the recipient of the National excellent Doctoral Dissertation award in 2013 (China).

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.

Nian Li received the B.S. and M.S. degrees in mathematics from Hubei University, Wuhan, China, in 2006 and 2009, respectively, and he received the Ph.D. degree at the Southwest Jiaotong University, Chengdu, China, in 2013. From Sept. 2011 to Aug. 2013, he was a visiting Ph.D. student in the Department of Informatics, University of Bergen, Norway. Currently, he is working as a postdoc in the Department of Mathematics, the Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. His research interests include sequence design and coding theory.