Certain codebooks and the generalized Erdős-Falconer distance problem (extended abstract)

Shohei Satake*

Faculty of Advanced Science and Technology
Kumamoto University
Kumamoto, Japan

shohei-satake@kumamoto-u.ac.jp

Abstract

The main purpose of this extended abstract is to establish a connection between minimizing the maximal cross-correlation amplitude of certain codebooks and the generalized Erdős-Falconer distance problem in vector spaces over finite fields studied in number theory and additive combinatorics. Our results also contain some constructions of asymptotically optimal codebooks.

1 Introduction

An (N, K)-*codebook* $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_N\} \subseteq \mathbb{C}^K$ consists of N complex vectors of length K such that $\|\mathbf{c}_i\|_2 = 1$ for all $1 \leq i \leq N$, which is also termed as a *signal set* or a *frame*. Define the *maximum cross-correlation amplitude* $I_{max}(\mathcal{C})$ of an (N, K)-codebook $\mathcal{C}$ as

$$I_{max}(\mathcal{C}) = \max_{1 \leq i < j \leq N} |\langle \mathbf{c}_i, \mathbf{c}_j \rangle| \tag{1}$$

where $\langle \mathbf{c}_i, \mathbf{c}_j \rangle$ denotes the standard inner product of the complex vectors $\mathbf{c}_i$ and $\mathbf{c}_j$. For a given K, it is desirable to construct an (N, K)-codebook $\mathcal{C}$ with as large N and small $I_{max}(\mathcal{C})$ as possible due to the practical applications in a variety of areas such as code-division multiple-access communication systems [15, 26]; combinatorial designs [6]; compressed sensing [1, 4, 10, 22]; coding theory [3]; and more. In the literature, a lower bound on $I_{max}(\mathcal{C})$ with respect to N and K was proved in [37], which is known as the *Welch bound*.

*S. Satake has been supported by Grant-in-Aid for JSPS Fellows 20J00469 of the Japan Society for the Promotion of Science.

Theorem 1 (Welch bound). *For any (N, K)-codebook $\mathcal{C}$ with $N \geq K$, we have*

$$I_{max}(\mathcal{C}) \geq I_{wel}(N, K) := \sqrt{\frac{N-K}{(N-1)K}} \tag{2}$$

where the equality holds if and only if $\left|\langle \mathbf{c}_i, \mathbf{c}_j \rangle\right| = \sqrt{\frac{N-K}{(N-1)K}}$ for all $1 \leq i \neq j \leq N$.

A codebook achieving the Welch bound is usually called a *maximum-Welch-bound-equality (MWBE) codebook* [39]. It is also known as the *equiangular tight frame* [5] in frame theory and equivalent to line packing in Grassmannian spaces [6]. In the literature, certain families of MWBE codebooks were deterministically constructed via discrete Fourier transform matrices [31, 39]; extended codes from any ideal two-level auto-correlation sequences [15, 39, 40]; conference matrices [6, 34]; difference sets in groups [8, 17, 39]; Steiner systems [13], and so on.

As pointed out by Sarwate in [31], it is very hard to construct an MWBE codebook in general. Hence there have been a number of attempts to construct codebooks nearly meeting the Welch bound as well, that is, the maximum cross-correlation amplitude $I_{max}(\mathcal{C})$ is slightly higher than the corresponding Welch bound, but asymptotically achieves it for large enough N. In this paper, we say an infinite family of (N, K_N)-codebooks $\{\mathcal{C}_N\}_{N\geq 1}$ is *asymptotically optimal* with respect to the Welch bound if $\lim_{N\to\infty} I_{max}(\mathcal{C}_N)/I_{wel}(N, K_N) = 1$. In the literature, asymptotically optimal codebooks have been constructed by using codes and codebooks [31]; almost difference sets [8]; relative difference sets [42]; binary sequences [40]; character sums [16, 24, 25]; Cayley sum graphs [32], and so forth.

On the other hand, it is known that an (N, K)-codebook $\mathcal{C}$ cannot meet the Welch bound if $\mathcal{C}$ is a real codebook with $N > K(K+1)/2$ or a complex codebook with $N > K^2$. In these cases, the following lower bound, called the *Levenshtein bound*, is known ([21]).

Theorem 2 (Levenshtein bound). *For a real (N, K)-codebook $\mathcal{C}$ with $N > K(K+1)/2$,*

$$I_{max}(\mathcal{C}) \geq I_{lev}^{(\mathbb{R})}(N, K) := \sqrt{\frac{3N - K^2 - 2K}{(N-K)(K+2)}}. \tag{3}$$

For a complex (N, K)-codebook $\mathcal{C}$ with $N > K^2$,

$$I_{max}(\mathcal{C}) \geq I_{lev}^{(\mathbb{C})}(N, K) := \sqrt{\frac{2N - K^2 - K}{(N-K)(K+1)}}. \tag{4}$$

Many publications have studied constructions of codebooks meeting the Levenshtein bound by using codes [3]; quadratic Gauss sums [38]; non-linear planar functions [9]; bent functions [41]; generalized bent $\mathbb{Z}_4$-valued quadratic forms [30], and so on.

The generalized Erdős-Falconer distance problem in vector spaces over finite fields is a finite field analogue of the Erdős and Falconer distance problems [11, 12] over $\mathbb{R}^d$ in discrete geometry, and has been extensively studied in number theory and additive combinatorics; see [20, 35, 36], for example. In this extended abstract, we shall investigate

certain families of codebooks obtained from polynomials over finite fields. These families provide many new asymptotically optimal codebooks and also contain optimal codebooks constructed in Wootters-Fields [38] and Ding-Yin [9]. Then we establish a connection between minimizing the maximum cross-correlation amplitude of these codebooks and the generalized Erdős-Falconer distance problem.

The remainder of this extended abstract is organized as follows. In Section 2, we present preliminary notations and results on finite fields. In Section 3, we briefly review the generalized Erdős-Falconer distance problem. In Section 4, we first define families of codebooks and then establish a relationship between minimizing the maximum cross-correlation amplitude of these codebooks and the generalized Erdős-Falconer distance problem. Also we provide families of asymptotically optimal codebooks, together with some extensions of results due to Koh-Shen [20]. In Section 5, some concluding remarks are made.

2 Preliminaries

Let G be a finite abelian group where the operation is expressed by addition here. A *character* μ on G is a group homomorphism from G to the multiplicative group of the complex field $\mathbb{C}$, that is, for any $a, b \in G$, we have $\mu(a+b) = \mu(a)\mu(b)$ and $|\mu(a)| = 1$. Moreover we have $\mu(-a) = \overline{\mu(a)}$ for every character μ. If a character μ such that for any $a \in G$, $\mu(a) = 1$, then μ is called the *principal character* of G. The set of all characters of G forms an abelian group which is referred to as the *character group* of G and denoted by $\widehat{G}$. Here the operation is the multiplication of characters, that is, for $\mu_1, \mu_2 \in \widehat{G}$, we have $(\mu_1 \cdot \mu_2)(a) := \mu_1(a)\mu_2(a)$ for all $a \in G$. It is known that $\widehat{G}$ is isomorphic to G.

Let $q = p^t$ where p is a prime number and $t \geq 1$ is an integer. In this extended abstract, $\mathbb{F}_q$ denotes a finite field of order q. Also $\mathbb{F}_q^+$ and $\mathbb{F}_q^*$ mean the additive and multiplicative group of $\mathbb{F}_q$, respectively. Note that $\mathbb{F}_q^+$ is isomorphic to the direct product $(\mathbb{Z}/p\mathbb{Z})^t$ and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The following is the definition of additive characters of $\mathbb{F}_q$.

Definition 3. An *additive character* χ of $\mathbb{F}_q$ is a character on the additive group $\mathbb{F}_q^+$.

For $t \geq 1$, $\mathbb{F}_q$ is the extension field of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of degree t, which has the same structure as a linear space over $\mathbb{F}_p$ of dimension t. Let $\mathrm{Tr}_{q/p}$ be the *trace* function from $\mathbb{F}_q$ to $\mathbb{F}_p$ defined as

$$\mathrm{Tr}_{q/p}(x) := x + x^p + \cdots + x^{p^{t-1}}$$

for any $x \in \mathbb{F}_q$. This is a linear mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$, that is, for any $x, y \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_p$, we have $\mathrm{Tr}_{q/p}(x) \in \mathbb{F}_p$, $\mathrm{Tr}_{q/p}(x+y) = \mathrm{Tr}_{q/p}(x) + \mathrm{Tr}_{q/p}(y)$ and $\mathrm{Tr}_{q/p}(\alpha x) = \alpha \mathrm{Tr}_{q/p}(x)$. Notice that $\mathrm{Tr}_{q/p}$ is surjective.

Note that additive characters of $\mathbb{F}_q$ are expressed by $\mathrm{Tr}_{q/p}$. For $\alpha \in \mathbb{F}_q$, let $\chi_\alpha(x) = \exp(\frac{2\pi i}{p} \cdot \mathrm{Tr}_{q/p}(\alpha x))$ for all $x \in \mathbb{F}_q^+$. Then it holds that $\widehat{\mathbb{F}_q^+} = \{\chi_\alpha \mid \alpha \in \mathbb{F}_q\}$. In particular, χ_α is principal if and only if $\alpha = 0$, and $\chi_1(x) = \exp(\frac{2\pi i}{p} \cdot \mathrm{Tr}_{q/p}(x))$ is said to be *canonical*.

The following proposition shows the *orthogonal relation* of additive characters.

Proposition 4.

$$\sum_{x\in\mathbb{F}_q}\chi_\alpha(x)=\begin{cases}q & \alpha=0;\\ 0 & \alpha\in\mathbb{F}_q^*.\end{cases} \tag{5}$$

Throughout this extended abstract, we use the following asymptotic notations. Let $f(q)>0$, $g(q)>0$ be functions of q. Then (1) $f=O(g)$ if $\limsup_{q\to\infty} f(q)/g(q)<\infty$; (2) $f=\Omega(g)$ if $\liminf_{q\to\infty} f(q)/g(q)>0$; (3) $f=\Theta(g)$ if $f=O(g)$ and $f=\Omega(g)$; (4) $f\approx g$ if $\lim_{q\to\infty} f(q)/g(q)=1$.

3 The generalized Erdős-Falconer distance problem

This section briefly reviews the generalized Erdős-Falconer distance problem. The original Erdős and Falconer distance problems consider the size or Lebesgue measure of the set of Euclidean distances between points in a given large set of points in $\mathbb{R}^d$ with $d\geq 2$, which are well-studied in discrete geometry; for details, see e.g. [11, 12, 14, 27].

Let $d\geq 2$ be an integer and q denote a prime power. For each $\mathbf{x}=(x_1,\ldots,x_d)\in\mathbb{F}_q^d$, let $||\mathbf{x}||=\mathbf{x}\cdot\mathbf{x}=x_1^2+\cdots+x_d^2$ where "$\cdot$" denotes the dot product. For subsets $\mathcal{E},\mathcal{F}\subset\mathbb{F}_q^d$, the *distance set* of $\mathcal{E}$ and $\mathcal{F}$, denoted by $\Delta(\mathcal{E},\mathcal{F})$, is defined as

$$\Delta(\mathcal{E},\mathcal{F}):=\{||\mathbf{x}-\mathbf{y}||\in\mathbb{F}_q\mid \mathbf{x}\in\mathcal{E},\mathbf{y}\in\mathcal{F}\}. \tag{6}$$

Clearly, $1=|\{0\}|\leq|\Delta(\mathcal{E},\mathcal{F})|\leq|\mathbb{F}_q|=q$. The *Erdős-Falconer distance problem* in the d-dimensional vector space $\mathbb{F}_q^d$ concerns the cardinality of $\Delta(\mathcal{E},\mathcal{F})$ for sufficiently large q, which was firstly studied by Bourgain-Katz-Tao [2] in the context of sum-product estimates over finite fields in additive combinatorics; see also [14]. Bourgain-Katz-Tao [2] proved that if $d=2$, q is a prime with $q\equiv 3 \pmod 4$ and $|\mathcal{E}|=\Theta(q^\delta)$ for some $0<\delta<2$, then there exists $\varepsilon>0$ depending on δ such that $\Delta(\mathcal{E},\mathcal{E})=\Omega(|\mathcal{E}|^{\frac{1}{2}+\varepsilon})$. After this work, Iosevich-Rudnev [18] proved that for each $d\geq 2$ and sufficiently large odd prime powers q,

$$|\Delta(\mathcal{E},\mathcal{E})|=\Omega\Big(\min\Big\{q,\frac{|\mathcal{E}|}{q^{\frac{d-1}{2}}}\Big\}\Big)$$

when $|\mathcal{E}|=\Omega(q^{\frac{d}{2}})$. In particular, Iosevich-Rudnev [18] observed that $|\Delta(\mathcal{E},\mathcal{E})|=\Theta(q)$ if $|\mathcal{E}|=\Omega(q^{\frac{d+1}{2}})$, which can be regarded as a finite field analogue of the result due to Falconer [12] that the distance set determined by a subset of $\mathbb{R}^d$ with $d\geq 2$ of Hausdorff dimension greater than $(d+1)/2$ has positive Lebesgue measure ([18, p.6130]).

After these works, many publications have also developed the study of the *generalized Erdős-Faloconer distance problem* which concerns distance sets determined by more general polynomials; see e.g. [20, 35, 36]. Let $P\in\mathbb{F}_q[X_1,\ldots,X_d]$ where $\mathbb{F}_q[X_1,\ldots,X_d]$ denotes the set of polynomials with coefficients over $\mathbb{F}_q$ with d variables $X_1,\ldots,X_d$. Let $\mathcal{E},\mathcal{F}\subset\mathbb{F}_q^d$. The *distance set* of $\mathcal{E}$ and $\mathcal{F}$ *with respect to* P, denoted by $\Delta_P(\mathcal{E},\mathcal{F})$, is defined as

$$\Delta_P(\mathcal{E},\mathcal{F}):=\{P(\mathbf{x}-\mathbf{y})\in\mathbb{F}_q\mid \mathbf{x}\in\mathcal{E},\mathbf{y}\in\mathcal{F}\}. \tag{7}$$

As in the case of $\Delta(\mathcal{E},\mathcal{F})$, it holds that $1 \le |\Delta_P(\mathcal{E},\mathcal{F})| \le q$. Clearly when $P(X_1,\ldots,X_d) = X_1^2+\cdots+X_d^2$, then $\Delta_P(\mathcal{E},\mathcal{F}) = \Delta(\mathcal{E},\mathcal{F})$. The following theorem was proved by Koh-Shen [20] which is a generalized version of the analogous result by Iosevich-Rudnev [18] of the Falconer's result mentioned in the previous paragraph.

Theorem 5 ([20])**.** *Let $d \ge 2$ be an arbitrarily fixed integer and q denote a prime power. Recall that χ_1 denotes the canonical additive character of $\mathbb{F}_q$. Let $P \in \mathbb{F}_q[X_1,\ldots,X_d]$. Suppose that the following condition $(*)$ holds for sufficiently large q.*

$(*)$ *For every $\mathbf{c} \in \mathbb{F}_q^d$ and $c \in \mathbb{F}_q^*$, it holds that*

$$\left|\sum_{\mathbf{x}\in\mathbb{F}_q^d} \chi_1(cP(\mathbf{x}) + \mathbf{c}\cdot\mathbf{x})\right| = O\Big(\sqrt{q^d}\Big). \tag{8}$$

Then for any $\mathcal{E},\mathcal{F} \subset \mathbb{F}_q^d$, it holds when $|\mathcal{E}||\mathcal{F}| = \Omega(q^{d+1})$ that $|\Delta_P(\mathcal{E},\mathcal{F})| = \Theta(q)$. In particular, if $\mathcal{E} = \mathcal{F}$, then it holds when $|\mathcal{E}| = \Omega(q^{\frac{d+1}{2}})$ that $|\Delta_P(\mathcal{E},\mathcal{E})| = \Theta(q)$.

The proof of Theorem 5 (and Theorem 4.4) in [20] implies the following theorem showing the implied constants in asymptotic notations in Theorem 5 under a stronger condition.

Theorem 6. *Let $d \ge 2$ be an arbitrarily fixed integer and q denote a prime power. Let $P \in \mathbb{F}_q[X_1,\ldots,X_d]$. Suppose that the following condition $(**)$, which is stronger than $(*)$ in Theorem 5, holds for sufficiently large q.*

$(**)$ *There exists a function $f_P(q)$ of q such that for every $\mathbf{c} \in \mathbb{F}_q^d$ and $c \in \mathbb{F}_q^*$,*

$$\left|\sum_{\mathbf{x}\in\mathbb{F}_q^d} \chi_1(cP(\mathbf{x}) + \mathbf{c}\cdot\mathbf{x})\right| \le f_P(q) \tag{9}$$

and

$$f_P(q) \approx \sqrt{q^d}. \tag{10}$$

Then for any $0 < \varepsilon < 1$ and $\mathcal{E},\mathcal{F} \subset \mathbb{F}_q^d$, it holds that $|\Delta_P(\mathcal{E},\mathcal{F})| \ge \varepsilon q$ if $|\mathcal{E}||\mathcal{F}| \ge \delta q f_P^2(q) \approx \delta q^{d+1}$ where $\delta = \varepsilon/(1-\varepsilon)$. In particular, if $\mathcal{E} = \mathcal{F}$, then it holds that $|\Delta_P(\mathcal{E},\mathcal{E})| \ge \varepsilon q$ if $|\mathcal{E}| \ge \sqrt{\delta}\cdot\sqrt{q} f_P(q) \approx \sqrt{\delta}\cdot q^{\frac{d+1}{2}}$.

Remark 7. If one replaces the condition (10) by a weaker condition that $f_P(q) \le C\sqrt{q^d}$ with $C > 1$, then the discussion in [20] implies a weaker claim that $|\Delta_P(\mathcal{E},\mathcal{F})| \ge \varepsilon q$ when $|\mathcal{E}||\mathcal{F}| \ge C^2\cdot\delta q f_P^2(q)$, which is much greater than δq^{d+1} for sufficiently large q. As will be shown in Theorem 11 and Remark 14, the condition (10) is optimal, and thus under the discussion in [20], the condition (10) optimizes the lower bound of $|\mathcal{E}||\mathcal{F}|$ so that $|\Delta_P(\mathcal{E},\mathcal{F})| \ge \varepsilon q$.

It will turn out in the next section that the condition $(*)$ or $(**)$ holds if and only if codebooks defined in the next section have the maximal cross-correlation amplitude with the optimal order of magnitude.

4 Codebooks from polynomials over finite fields

This section first defines families of codebooks from polynomials over finite fields. Then the main result in this extended abstract is shown, together with some constructions of asymptotically optimal codebooks with respect to the Welch bound. Constructions here also generate codebooks meeting the Levenshtein bound provided in Wootters-Fields [38] and Ding-Yin [9].

Definition 8. Let $d \geq 1$ be an integer and q a prime power. Let $V := \mathbb{F}_q \times \mathbb{F}_q^d$. For a polynomial $P \in \mathbb{F}_q[X_1, \ldots, X_d]$, define $D_P := \{(x, \mathbf{x}) \in V \mid x + P(\mathbf{x}) = 0\}$. Note that V forms an abelian group of order q^{d+1} and $|D_P| = q^d$. For each character ψ of V, define a vector $c_\psi \in \mathbb{C}^{q^d}$ as follows:

$$c_\psi := \frac{1}{\sqrt{q^d}}(\psi(\mathbf{d}))_{\mathbf{d} \in D_P}. \tag{11}$$

Let $\mathbf{e}_i := (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C}^{q^d}$ denote a unit-norm vector such that the ith coordinate of $\mathbf{e}_i$ is 1 and all other coordinates are 0. Denote $\mathcal{E}_{q^d} := \{\mathbf{e}_i : 1 \leq i \leq q^d\}$. Then

$$\mathcal{C}_P := \{c_\psi \mid \psi \text{ is a character of } V\} \cup \mathcal{E}_{q^d} \tag{12}$$

is a $(q^{d+1} + q^d, q^d)$-codebook.

Note that each character ψ of V can be expressed using the canonical additive character χ_1 of $\mathbb{F}_q$ as the following form:

$$\psi((x, \mathbf{x})) = \chi_1\big((x, \mathbf{x}) \cdot (a, \mathbf{a})\big) \quad (\forall (x, \mathbf{x}) \in V) \tag{13}$$

for $(a, \mathbf{a}) \in V$ uniquely determined by ψ. Also ψ is principal if and only if $(a, \mathbf{a}) = (0, \ldots, 0)$. Thus,

$$\mathcal{C}_P = \{c_{(a,\mathbf{a})} \mid (a, \mathbf{a}) \in V\} \cup \mathcal{E}_{q^d}, \tag{14}$$

where for each $(a, \mathbf{a}) \in V$, the vector $c_{(a,\mathbf{a})}$ is defined as

$$c_{(a,\mathbf{a})} := \frac{1}{\sqrt{q^d}}\Big(\chi_1\big((x, \mathbf{x}) \cdot (a, \mathbf{a})\big)\Big)_{(x,\mathbf{x}) \in D_P}. \tag{15}$$

Remark 9. Suppose $d = 1$. Then the $(q^2 + q, q)$-codebook $\mathcal{C}_P$ is a generalization of the codebook with the same parameters studied by Wootters-Fields [38] and Ding-Yin [9].

Remark 10. By the definition of the canonical additive character of $\mathbb{F}_q$ in Section 2, $\mathcal{C}_P$ is a real codebook if and only if q is a power of 2. Otherwise, $\mathcal{C}_P$ is a complex codebook.

The following is the main theorem in this extended abstract.

Theorem 11. *Let $d \geq 1$ be an arbitrarily fixed integer and q denote a sufficiently large prime power. Then the condition $(*)$ in Theorem 5 holds if and only if*

$$I_{max}(\mathcal{C}_P) = O\left(\frac{1}{\sqrt{q^d}}\right). \tag{16}$$

Moreover, the condition (**) in Theorem 6 holds if and only if there exists a function $f_P(q)$ of q such that

$$I_{max}(\mathcal{C}_P) \leq \frac{f_P(q)}{q^d} \approx \frac{1}{\sqrt{q^d}}. \tag{17}$$

Remark 12. Suppose that the equation (17) holds. Then for each $d \geq 2$, $\mathcal{C}_P$ asymptotically meets the Welch bound. In fact, for each $d \geq 2$, $\mathcal{C}_P$ is a $(q^{d+1}+q^d, q^d)$-codebook and

$$I_{wel}(q^{d+1}+q^d, q^d) = \sqrt{\frac{(q^{d+1}+q^d)-q^d}{(q^{d+1}+q^d-1)\cdot q^d}} = \sqrt{\frac{q}{q^{d+1}+q^d-1}} \approx \frac{1}{\sqrt{q^d}}.$$

Thus,

$$\lim_{N\to\infty} \frac{I_{max}(\mathcal{C}_P)}{I_{wel}(N,K)} = \lim_{q\to\infty} \frac{I_{max}(\mathcal{C}_P)}{I_{wel}(q^{d+1}+q^d, q^d)} = 1.$$

Remark 13. Suppose that the equation (17) holds. Then, if $d = 1$ and q is odd, $\mathcal{C}_P$ asymptotically meets the Levenshtein bound. In fact, since q is odd, $\mathcal{C}_P$ is a complex (q^2+q, q)-codebook by Remark 10. In this case,

$$I_{lev}^{(\mathbb{C})}(q^2+q, q) = \sqrt{\frac{2(q^2+q)-q^2-q}{(q+1)(q^2+q-q)}} = \frac{1}{\sqrt{q}}.$$

Thus,

$$\lim_{N\to\infty} \frac{I_{max}(\mathcal{C}_P)}{I_{lev}^{(\mathbb{C})}(N,K)} = \lim_{q\to\infty} \frac{I_{max}(\mathcal{C}_P)}{I_{lev}^{(\mathbb{C})}(q^2+q, q)} = 1.$$

If $d = 1$ and q is even, then $\mathcal{C}_P$ is a real (q^2+q, q)-codebook by Remark 10. Thus the equation (17) cannot hold by the Levenshtein bound for real codebooks. In this case, the right hand side of (17) should be $\sqrt{2/q}$. Also, the right hand side of (10) should be $\sqrt{2q}$.

Remark 14. Theorem 11 and the Welch bound imply that for each $d \geq 2$, the condition (10) is optimal in the sense that if the condition (9) holds for $f_P(q)$, then $f_P(q)$ cannot be smaller than $C\sqrt{q^d}$ with $0 < C < 1$ for any sufficiently large q.

Theorems 5, 6 and 11 directly give the following corollary which shows an interesting connection between the Erdős-Falconer distance problem and minimizing $I_{max}(\mathcal{C}_P)$ of the $(q^{d+1}+q^d, q^d)$-codebook $\mathcal{C}_P$ with $d \geq 2$.

Corollary 15. *Let $d \geq 2$ be an arbitrarily fixed integer and q a sufficiently large prime power. Suppose that the equation (16) in Theorem 11 holds. Then, if $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_q^d$ with $|\mathcal{E}||\mathcal{F}| = \Omega(q^{d+1})$, then $|\Delta_P(\mathcal{E}, \mathcal{F})| = \Theta(q)$. In particular, if $\mathcal{E} = \mathcal{F}$, then it holds when $|\mathcal{E}| = \Omega(q^{\frac{d+1}{2}})$ that $|\Delta_P(\mathcal{E}, \mathcal{E})| = \Theta(q)$.*

Moreover if the equation (17) holds, then for any $0 < \varepsilon < 1$ and $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_q^d$, it holds that $|\Delta_P(\mathcal{E}, \mathcal{F})| \geq \varepsilon q$ if $|\mathcal{E}||\mathcal{F}| \geq \delta q f_P^2(q) \approx \delta q^{d+1}$ where $\delta = \varepsilon/(1-\varepsilon)$. In particular, if $\mathcal{E} = \mathcal{F}$, then it holds that $|\Delta_P(\mathcal{E}, \mathcal{E})| \geq \varepsilon q$ if $|\mathcal{E}| \geq \sqrt{\delta} \cdot \sqrt{q} f_P(q) \approx \sqrt{\delta} \cdot q^{\frac{d+1}{2}}$.

Now we give a proof of Theorem 11.

Proof of Theorem 11. We give only a proof of the first claim since the second claim follows from the proof of the first one.

Let $\mathcal{C}'_P = \mathcal{C}_P \setminus \mathcal{E}_{q^d}$. Note that $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0$ for $1 \le i \ne j \le q^d$, and $|\langle \mathbf{e}_i, \mathbf{c} \rangle| = 1/\sqrt{q^d}$ for every pair of $1 \le i \le q^d$ and $\mathbf{c} \in \mathcal{C}'_P$. Thus to prove the first claim, it suffices to show the following claim: for each pair of $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}'_P$ with $\mathbf{c}_1 \ne \mathbf{c}_2$, it holds that

$$|\langle \mathbf{c}_1, \mathbf{c}_2 \rangle| = O\left(\frac{1}{\sqrt{q^d}}\right) \tag{18}$$

if and only if the condition $(*)$ in Theorem 5 holds.

If $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}'_P$ with $\mathbf{c}_1 \ne \mathbf{c}_2$, then $\mathbf{c}_1 = \mathbf{c}_{(a,\mathbf{a})}$ and $\mathbf{c}_2 = \mathbf{c}_{(b,\mathbf{b})}$ for some $(a, \mathbf{a}), (b, \mathbf{b}) \in V$ with $(a, \mathbf{a}) \ne (b, \mathbf{b})$. Let $(c, \mathbf{c}) = (a - b, \mathbf{a} - \mathbf{b}) \in V \setminus \{(0, \dots, 0)\}$. Then, using the discussion in Vinh [35],

$$\begin{aligned}
|\langle \mathbf{c}_1, \mathbf{c}_2 \rangle| &= \frac{1}{q^d} \sum_{(x,\mathbf{x}) \in D_P} \chi_1\big((x, \mathbf{x}) \cdot (c, \mathbf{c})\big) \\
&= \frac{1}{q^d} \sum_{\substack{(x,\mathbf{x}) \in \mathbb{F}_q \times \mathbb{F}_q^d \\ x + P(\mathbf{x}) = 0}} \chi_1\big(xc + \mathbf{x} \cdot \mathbf{c}\big) \\
&= \frac{1}{q^d} \cdot \frac{1}{q} \sum_{(x,\mathbf{x}) \in \mathbb{F}_q \times \mathbb{F}_q^d} \sum_{s \in \mathbb{F}_q} \chi_1(s(x + P(\mathbf{x}))) \chi_1\big(xc + \mathbf{x} \cdot \mathbf{c}\big) \qquad (19) \\
&= \frac{1}{q^d} \cdot \frac{1}{q} \sum_{s,x \in \mathbb{F}_q} \chi_1\big((s + c)x\big) \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi_1(sP(\mathbf{x}) + \mathbf{x} \cdot \mathbf{c}) \\
&= \frac{1}{q^d} \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi_1(-cP(\mathbf{x}) + \mathbf{x} \cdot \mathbf{c}),
\end{aligned}$$

where the third and last equalities in (19) follow from Proposition 4.

If $c = 0$ and $\mathbf{c} = (c_1, \dots, c_d) \ne (0, \dots, 0)$, then it holds by Proposition 4 that

$$\sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi_1(-cP(\mathbf{x}) + \mathbf{x} \cdot \mathbf{c}) = \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi_1(\mathbf{x} \cdot \mathbf{c}) = \prod_{i=1}^{d} \left(\sum_{x \in \mathbb{F}_q} \chi_1(c_i x) \right)^d = 0. \tag{20}$$

Thus by (19) and (20), the equation (18) holds if and only if the condition $(*)$ in Theorem 5 holds. □

The rest of this section is to construct polynomials P from non-linear planar functions which $\mathcal{C}_P$ asymptotically meeting the Welch or Levenshtein bounds.

Definition 16. Let f be a function from $\mathbb{F}_q^+$ to $\mathbb{F}_q^+$. Then f is called a *non-linear planar function* over $\mathbb{F}_q^+$ if f is not a group homomorphism from $\mathbb{F}_q^+$ to itself and the function $f(X + a) - f(X)$ is a permutation of $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$.

Note that if q is even, there does not exist non-linear planar functions over $\mathbb{F}_q^+$, while there always exists a non-linear planar function over $\mathbb{F}_q^+$, which is a polynomial in $\mathbb{F}_q[X]$, if q is odd.

Lemma 17 (e.g. Lemma 3 in [9])**.** *Let f be a non-linear planar function over $\mathbb{F}_q^+$. Then it holds that*

$$\Big|\sum_{x\in\mathbb{F}_q}\chi_1(f(x))\Big| = \sqrt{q}. \tag{21}$$

Theorem 18. *Let $d \geq 2$ be an arbitrarily fixed integer. Suppose that q is an odd prime power. For each $1 \leq i \leq d$, let $f_i(X_i)$ be a non-linear planar function over $\mathbb{F}_q^+$. If $P(X_1,\ldots,X_d) = \sum_{i=1}^d f_i(X_i)$, then $\mathcal{C}_P$ is a $(q^{d+1}+q^d, q^d)$-codebook with*

$$I_{max}(\mathcal{C}_P) = \frac{1}{\sqrt{q^d}}. \tag{22}$$

Proof. By the proof of Theorem 11, it suffices to show that for each $c \in \mathbb{F}_q^*$ and $\mathbf{c} = (c_1,\ldots,c_d) \in \mathbb{F}_q^d$,

$$\Big|\sum_{\mathbf{x}\in\mathbb{F}_q^d}\chi_1(-cP(\mathbf{x})+\mathbf{x}\cdot\mathbf{c})\Big| = \sqrt{q^d}. \tag{23}$$

By the assumption of P, it holds for each $\mathbf{x} = (x_1,\ldots,x_d) \in \mathbb{F}_q^d$ that

$$-cP(\mathbf{x})+\mathbf{x}\cdot\mathbf{c} = \sum_{i=1}^d(-cf_i(x_i)+c_ix_i),$$

and thus

$$\sum_{\mathbf{x}\in\mathbb{F}_q^d}\chi_1(-cP(\mathbf{x})+\mathbf{x}\cdot\mathbf{c}) = \prod_{i=1}^d\Big\{\sum_{x_i\in\mathbb{F}_q}\chi_1(-cf_i(x_i)+c_ix_i)\Big\}. \tag{24}$$

By the definition of f_i, the function $g_i(X_i) := -cf_i(X_i)+c_iX_i$ is also a non-linear planar function over $\mathbb{F}_q^+$ for every $1 \leq i \leq d$. In fact, since $c \in \mathbb{F}_q^*$, $g_i(X_i+a)-g_i(X_i) = -c\{f_i(X_i+a)-f_i(X_i)\}+c_ia$ is a permutation of $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$. Thus it follows from (24) and Lemma 17 that

$$\Big|\sum_{\mathbf{x}\in\mathbb{F}_q^d}\chi_1(-cP(\mathbf{x})+\mathbf{x}\cdot\mathbf{c})\Big| = (\sqrt{q})^d = \sqrt{q^d}. \tag{25}$$

□

Remark 19. When $d = 1$, the (q^2+q, q)-codebook $\mathcal{C}_P$ in Theorem 18 exactly meets the Levenshtein bound. We remark that this codebook was obtained by Ding-Yin [9]. In particular, it is known that $P(X) = X^2$ is a non-linear planar function over $\mathbb{F}_q^+$ and the codebook $\mathcal{C}_P$ in this case is exactly one constructed by Wootters-Fields [38].

Remark 20. Known examples of non-linear planar functions over $\mathbb{F}_q^+$ are expressed by a monomial of higher degree; see e.g. [9, 29] and references therein. We remark that by Theorem 18 and Corollary 15, one can extend Corollary 4.2 in Koh-Shen [20]. Let $d \geq 2$ be an arbitrarily fixed integer and q a sufficiently large prime power. Corollary 4.2 in Koh-Shen [20] states that if $P(X_1, \ldots, X_d) = \sum_{i=1}^d p_i X_i^{k_j}$ with $p_i \in \mathbb{F}_q^*$ and $k_i \geq 2$ is a fixed integer with $(k_i, q) = 1$ for every $1 \leq i \leq d$, then it holds when $|\mathcal{E}||\mathcal{F}| = \Omega(q^{d+1})$ that $|\Delta_P(\mathcal{E}, \mathcal{F})| = \Theta(q)$. This was obtained as a corollary of Theorem 5, where the condition $(*)$ was confirmed by the Weil's theorem (see e.g. Theorem 5.38 in [23]). However, for the case that some k_i is an unbounded function of q, the Weil's theorem does not necessarily imply the condition $(*)$ in general.

Now suppose that $q = p^t$ where p is an odd prime and fixed $t \geq 1$, and thus $q \to \infty$ if and only if $p \to \infty$. It was proved in [7] that X^{p^k+1} is a non-linear planar function over $\mathbb{F}_q^+$ if $k \geq 1$ is an integer such that $t/(t, k)$ is odd. For the simplicity, we consider the case that $k = 1$ and $t > k$ is odd, which directly implies that $t/(t, k) = t$ is odd; however the discussion below also works for general cases as well. Suppose that $P(X_1, \ldots, X_d) = \sum_{i=1}^d p_i X_i^{p+1} = \sum_{i=1}^d p_i X_i^{q^{(1/t)}+1}$ with $p_i \in \mathbb{F}_q^*$ for $1 \leq i \leq d$. Notice that $(p + 1, q) = 1$. Then the Weil's theorem implies that for $c \in \mathbb{F}_q^*$ and $\mathbf{c} \in \mathbb{F}_q^d$,

$$\left| \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi_1(-cP(\mathbf{x}) + \mathbf{x} \cdot \mathbf{c}) \right| = \prod_{i=1}^d \left| \sum_{x_i \in \mathbb{F}_q} \chi_1(-cp_i x_i^{q^{(1/t)}+1} + c_i x_i) \right| \leq q^{(\frac{1}{2}+\frac{1}{t})d},$$

which is much weaker than the condition $(*)$. On the other hand, Theorem 18 and Lemma 17 directly imply the condition $(*)$, and thus the statement in Corollary 4.2 in Koh-Shen [20] holds for the polynomial P defined above. By Theorem 18, one can also extend to the case of more general polynomials satisfying the conditions in Theorem 18 from other known non-linear planar functions over $\mathbb{F}_q^+$.

5 Concluding remarks

First, Section 4 gives some polynomials P such that the codebook $\mathcal{C}_P$ is asymptotically optimal. However, these are for the case that q is odd. For the case that q is even, as in Ding-Yin [9], one can use polynomials of the form of $P(X_1, \ldots, X_d) = \sum_{i=1}^d f_i(X_i)$ where each f_i is an almost bent function. Then for each $d \geq 2$, $I_{max}(\mathcal{C}_P)$ has the optimal order of the magnitude. Also, if $d = 1$, it meets the Levenshtein bound as proved by Ding-Yin [9]. The details of these results will be shown in the full paper of this extended abstract.

Next, in Section 4, asymptotically optimal $(q^{d+1}+q^d, q^d)$-codebooks $\mathcal{C}_P$ are constructed for each $d \geq 1$ and some polynomials $P \in \mathbb{F}_q[X_1, \ldots, X_d]$. These are based on the abelian group $\mathbb{F}_q \times \mathbb{F}_q^d$ and polynomials P, and thus, for each d and prime power q, to generate examples of codebooks, it would be enough to apply the operations of $\mathbb{F}_q$ to get the set D_P defining the codebook $\mathcal{C}_P$. On the other hand, as constructed in [38, 9], there exist optimal $(q^{2d} + q^d, q^d)$-codebooks, which have more vectors (see Remark 19). The constructions in [38, 9] are based on the abelian group $\mathbb{F}_{q^d} \times \mathbb{F}_{q^d}$ and non-linear planar functions over $\mathbb{F}_{q^d}^+$. Note that in these constructions, to generate examples of codebooks for each d and q, one

might need to construct the extended field $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$ of degree d, and then might apply multiplications of elements in not only $\mathbb{F}_q$ but also $\mathbb{F}_{q^d}$. To our best knowledge, these seem to take certain computational costs for each q if d is large (e.g. [28, Chapter 11]).

Acknowledgements

The author would like to thank three anonymous referees for their many constructive comments and suggestions on the results and presentation of this extended abstract.

References

[1] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova. Explicit constructions of RIP matrices and related problems. *Duke Math. J.*, 159(1): 145–185, 2011.

[2] J. Bourgain, N. Katz, T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1), 27–57, 2004.

[3] A. R. Calderbank, P. J. Cameron, W. M. Kantor, J. J. Seidel. $\mathbb{Z}_4$-kerdock codes, orthogonal spreads, and extremal Euclidean linesets. *Proc. London Math. Soc.*, 75(3): 436–480, 1997.

[4] E. Candès, T. Tao. Decoding by linear programming. *IEEE Trans. Inf. Theory*, 51(12): 4203–4215, 2005.

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

[6] J. H. Conway, R. H. Harding, N. J. A. Sloane. Packing lines, planes, etc.: Packings in Grassmannian spaces. *Exp. Math.*, 5(2): 139–159, 1996.

[7] P. Dembowski, T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103: 239–258, 1968.

[8] C. Ding, T. Feng. A generic construction of complex codebooks meeting the Welch bound. *IEEE Trans. Inf. Theory*, 53(11): 4245–4250, 2007.

[9] C. Ding, J. Yin. Signal sets from functions with optimum nonlinearity. *IEEE Trans. Commun.*, 55(5): 936–940, 2007.

[10] D. L. Donoho, M. Elad, Optimally sparse representation in general (nonorthogonal) dictionaries via ℓ_1 minimization. *Proc. Nat. Acad. Sci. United States Amer.,* 100: 2197–2202, 2003.

[11] P. Erdős. On sets of distances of n points. *Amer. Math. Monthly*, 53(5): 248–250, 1946.

[12] K. J. Falconer. On the Hausdorff dimensions of distance sets. *Mathematika*, 32(2): 206–212, 1985.

[13] M. Fickus, D. G. Mixon, J. C. Tremain. Steiner equiangular tight frames. *Linear Algebra Appl.*, 436(5): 1014–1027, 2012.

[14] J. Garibaldi, A. Iosevich, S. Senger. *The Erdős Distance Problem*, Amer. Math. Soc., 2011.

[15] S. W. Golomb, G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar.* Cambridge Univ. Press, 2005.

[16] Z. Heng, C. Ding, Q. Yue. New constructions of asymptotically optimal codebooks with multiplicative characters. *IEEE Trans. Inf. Theory,* 64(10): 6498–6505, 2017.

[17] H. Hu, J. Wu. New constructions of codebooks nearly meeting the Welch bound with equality. *IEEE Trans. Inf. Theory,* 60(2): 1348–1355, 2014.

[18] A. Iosevich, M. Rudnev. Erdős distance problem in vector spaces over finite fields. *Trans. Amer. Math. Soc.*, 359(12): 6127–6142, 2007.

[19] A. Klappenecker, M. Rötteler, I. E. Shparlinski, A. Winterhof. On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states. *J. Math. Phys.*, 46(8): 082104, 2005.

[20] D. Koh, C.-Y. Shen. The generalized Erdős-Falconer distance problems in vector spaces over finite fields. *J. Number Theory*, 132(11): 2455–2473, 2012.

[21] V. I. Levenshtein. Bounds for packing of metric spaces and some of their applications. *Problem Cybern.*, 40: 43–110, 1983.

[22] S. Li, G. Ge. Deterministic construction of sparse sensing matrices via finite geometry. *IEEE Trans. Signal Processing,* 62(11): 2850–2859, 2014.

[23] R. Lidl, H. Niederreiter. *Finite Fields.* Cambridge Univ. Press, 1984.

[24] W. Lu, X. Wu, X. Cao, M. Chen. Six constructions of asymptotically optimal codebooks via the character sums. *Des. Codes Cryptogr.*, 88(6): 1139–1158, 2020.

[25] G. Luo, X. Cao. Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum. *IEEE Trans. Inf. Theory*, 64(10): 6498–6505, 2018.

[26] J. L. Massey, T. Mittelholzer. Welch's bound and sequence sets for code-division multiple-access systems. in *Sequences II.* Springer-Verlag, pp. 63–78, 1993.

[27] P. Mattila. *Fourier Analysis and Hausdorff Dimension.* Cambridge Univ. Press, 2015.

[28] G. L. Mullen, D. Panario. *Handbook of Finite Fields.* Taylor and Francis, 2013.

[29] A. Pott, Almost perfect and planar functions. *Des. Codes Cryptogr.*, 78(1): 141–195, 2016.

[30] Y. Qi, S. Mesnager, C. Tang. Codebooks from generalized bent $\mathbb{Z}_4$-valued quadratic forms. *Discrete Math.*, 343(3): 111736, 2020.

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

[32] S. Satake, Y. Gu. Constructions of complex codebooks asymptotically meeting the Welch bound: A graph theoretic approach. To appear in Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT2020).

[33] I. E. Shparlinski, A. Winterhof. Constructions of approximately mutually unbiased bases. *Lecture Notes in Comput. Sci.*, 3887: 793–799, 2006.

[34] T. Strohmer, R. Heath. Grassmannian frames with applications to coding and communication. *Appl. Comput. Harmon. Anal.,* 14(3): 257–275, 2003.

[35] L. A. Vinh. On the generalized Erdős-Falconer distance problems over finite fields. *J. Number Theory*, 133(9): 2939–2947, 2013.

[36] V. Vu. Sum-product estimates via directed expanders. *Math. Res. Lett.*, 15(2): 375–388, 2008.

[37] L. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Trans. Inf. Theory*, 20(3): 397–399, 1974.

[38] W. Wootters, B. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.*, 191(2): 363–381, 1989.

[39] P. Xia, S. Zhou, G. B. Giannakis. Achieving the Welch bound with difference sets. *IEEE Trans. Inf. Theory,* 51(5): 1900–1907, 2005.

[40] N. Y. Yu. A construction of codebooks associated with binary sequences. *IEEE Trans. Inf. Theory,* 58(8): 5522–5533, 2012.

[41] Z. Zhou, C. Ding, N. Li. New families of codebooks achieving the levenshtein bound. *IEEE Trans. Inf. Theory,* 60(11), 7382–7387, 2014.

[42] Z. Zhou, X. Tang. New nearly optimal codebooks from relative difference sets. *Adv. Math. Commun.,* 5(3): 521–527, 2011.