Des. Codes Cryptogr. (2012) 63:209–224
DOI 10.1007/s10623-011-9549-2

Construction of cyclotomic codebooks nearly meeting the Welch bound

Aixian Zhang · Keqin Feng

Received: 31 March 2011 / Revised: 6 July 2011 / Accepted: 12 July 2011 /
Published online: 10 August 2011

Abstract Ding and Feng (IEEE Trans Inform Theory 52(9):4229–4235, 2006, IEEE Trans Inform Theory 53(11):4245–4250, 2007) constructed series of (N, K) codebooks which meet or nearly meet the Welch bound $\sqrt{\frac{N-K}{(N-1)K}}$ by using difference set (DS) or almost difference set (ADS) in certain finite abelian group respectively. In this paper, we generalize the cyclotomic constructions considered in (IEEE Trans Inform Theory 52(9):4229–4235, 2006, IEEE Trans Inform Theory 53(11):4245–4250, 2007) and (IEEE Trans Inform Theory 52(5), 2052–2061, 2006) to present more series of codebooks which nearly meet the Welch bound under looser conditions than ones required by DS and ADS.

Keywords Codebook · Welch bound · Cyclotomic class · Cyclotomic number · Gauss sum · Gauss period · Difference set · Almost difference set

Mathematics Subject Classification (2000) 94A05 · 05B10

1 Introduction

An (N, K) codebook $\mathcal{C}$ is a set $\{c_1, \ldots, c_N\}$ of N unit norm complex vectors c_i $(1 \le i \le N)$ in $\mathbb{C}^K$. Let

$$I_{\max}(\mathcal{C}) = \max_{1 \le i \ne j \le N} |c_i c_j^H|,$$

where c_j^H denotes the Hermite transpose of vector c_j. We have the following Welch lower bound:

Communicated by T. Helleseth.

A. Zhang (✉)
School of Mathematical Science, Capital Normal University, Beijing 100048, China
e-mail: zhangaixian1008@126.com

K. Feng
Department of Mathematical Science, Tsinghua University, Beijing 100084, China
e-mail: kfeng@math.tsinghua.edu.cn

Lemma 1.1 (Welch [6]) *For any (N, K) codebook $\mathcal{C}$ with $N > K$, we have*

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

Codebooks with low value $I_{\max}(\mathcal{C})$ are used in direct spread CDMA systems, quantum information processing, packing and coding theory (see [5] and the references therein). A codebook $\mathcal{C}$ is called optimal if it meets the Welch bound (1). One of the important methods to construct optimal codebooks comes from difference sets in finite abelian groups as indicated and developed by Ding and Feng [3,4] where they also constructed several series of codebooks which nearly meet the Welch bound by using almost difference sets.

Let G be an (additive) abelian group of order v, D be a k-element subset of G. We define the multiset

$$\Delta(D) = \{d - d' : d, d' \in D,\ d \neq d'\}.$$

D is called a (v, k, λ) difference set of G if the number of x in $\Delta(D)$ is exactly λ for each non-zero element $x \in G$. More generally, D is called a (v, k, λ) almost difference set of G if there exists a partition $G\backslash\{0\} = A \bigcup B$ such that the number of x in $\Delta(D)$ is exactly λ and $\lambda + 1$ for each $x \in A$ and $x \in B$ respectively.

Let $\widehat{G}$ be the character group of G. For any k-element subset $D = \{d_1, \ldots, d_k\}$ of G, we define the following $(N, K) = (v, k)$ codebook

$$\mathcal{C}(D) = \{c_\chi : \chi \in \widehat{G}\},$$

where

$$c_\chi = \frac{1}{\sqrt{k}}(\chi(d_1), \ldots, \chi(d_k)).$$

For $\chi, \chi' \in \widehat{G}$, we have

$$c_\chi c_{\chi'}^H = \frac{1}{k}\sum_{d\in D} \chi\bar{\chi}'(d) = \frac{1}{k}\sum_{d\in D} \psi(d)\ \ (\psi = \chi\bar{\chi}' \in \widehat{G}).$$

Therefore

$$I_{\max}(\mathcal{C}(D))^2 = \frac{1}{k^2}\max\left\{\left|\sum_{d\in D}\psi(d)\right|^2 : 1 \neq \psi \in \widehat{G}\right\},$$

and

$$\begin{aligned}\left|\sum_{d\in D}\psi(d)\right|^2 &= \sum_{d,d'\in D}\psi(d)\bar{\psi}(d') = \sum_{d,d'\in D}\psi(d-d')\\ &= k + \sum_{\substack{d,d'\in D\\ d\neq d'}}\psi(d-d').\end{aligned} \tag{2}$$

From (2) it is derived directly in [4] and [5] that if D is a difference set of G then $\mathcal{C}(D)$ is an optimal codebook. On the other hand, Ding and Feng [3,4] consider the codebooks $\mathcal{C}(D)$ from almost difference sets D.

Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, $q-1 = ef,\ e \geq 2,\ \alpha$ be a primitive element of $\mathbb{F}_q$ such that $\mathbb{F}_q^{\times} =< \alpha >$. The cyclotomic classes of order e are defined by

$$D_\lambda = D_\lambda^{(e,q)} = \alpha^\lambda < \alpha^e > \quad (0 \leq \lambda \leq e-1).$$

In this paper, we are concerned with the following cyclotomic difference sets and almost difference sets.

Lemma 1.2 ([3], Corollary 4)

(A) *If* $q = 4t^2 + 1$ *and* t *is an odd integer, then* $D_0^{(4,q)}$ *is a* $(v,k) = (q, (q-1)/4)$ *DS in* $\mathbb{F}_q$.

(B) *If* $q = 8t^2 + 1 = 64u^2 + 9$ *and both* t *and* u *are odd integers, then* $D_0^{(8,q)}$ *is a* $(v,k) = (q, (q-1)/8)$ *DS in* $\mathbb{F}_q$.

(C) *If* $q = 4t^2 + 27, t$ *is an odd integer and* $(3,t) = 1$, *then* $D_0^{(6,q)} \bigcup D_1^{(6,q)} \bigcup D_3^{(6,q)}$ *is a* $(v,k) = (q, (q-1)/2)$ *DS in* $\mathbb{F}_q$.

Lemma 1.3 ([1])

(I) *If* $q = s^2 + 4t^2,\ s = 5$ *or* -3 *and* $\frac{q-1}{4}$ *is odd, then* $D_0^{(4,q)}$ *is an ADS in* $\mathbb{F}_q$ *with* $(v,k,\lambda) = (q, \frac{q-1}{4}, \frac{q-13}{16})$.

(II) *If* $q = s^2 + 4t^2,\ t = \pm 1$ *and* $\frac{q-1}{4}$ *is odd, then* $D_0^{(4,q)} \bigcup D_1^{(4,q)}$ *is an ADS in* $\mathbb{F}_q$ *with* $(v,k,\lambda) = (q, \frac{q-1}{2}, \frac{q-5}{4})$.

(III) *If* $q \equiv 5(mod8)$ *is a prime,* $q = s^2 + 4t^2,\ s \equiv \pm 1(mod4)$, *then*

$$D_{(i,j,l)} = [\{0\} \times (D_i^{(4,q)} \bigcup D_j^{(4,q)})] \bigcup [\{1\} \times (D_l^{(4,q)} \bigcup D_j^{(4,q)})]$$

is an ADS in $\mathbb{F}_2 \times \mathbb{F}_q$ *with* $(v,k,\lambda) = (2q, q-1, \frac{q-3}{2})$ *provided*

(1) $t = 1$ *and* $(i,j,l) = (0,1,3)$ *or* $(0,2,1)$; *or*

(2) $s = 1$ *and* $(i,j,l) = (1,0,3)$ *or* $(0,1,2)$.

For all series D of ADS in Lemma 1.3 (and several other series of ADS), the values of $I_{\max}(\mathcal{C}(D))^2$ have been determined in [4] as shown in the Table 1. All codebooks $\mathcal{C}(D)$ in the table *nearly meeting* the Welch bound in the following meaning.

A series of (N_n, K_n) codebooks $\mathcal{C}_n$ $(n = 1, 2, \ldots)$ are called to nearly meeting the Welch bound if the following two conditions are satisfied when $n \to \infty$:

Table 1

D	Parameters (N,K) of $\mathcal{C}$	$\frac{N-K}{(N-1)K}$	$I_{\max}(\mathcal{C})^2$
(I)	$\left(q, \frac{q-1}{4}\right)$	$\frac{3q+1}{(q-1)^2}$	$\frac{3q+1+8\sqrt{q}}{(q-1)^2}$
(II)	$\left(q, \frac{q-1}{2}\right)$	$\frac{q+1}{(q-1)^2}$	$\frac{1}{(\sqrt{q}-1)^2}$
(III)			
(i,j,l) $= (0,1,3)$ or $(0,1,2)$	$(2q, q-1)$	$\frac{2(q^2+q+1)}{(2q-1)^2(q-1)}$	$\frac{2q+2\sqrt{q}}{4(q-1)^2}$

(1) There exists a constant $a,\ 0 < a < 1$ such that $N_n, K_n \to \infty$ and

$$K_n = aN_n + O(\sqrt{N_n}),$$

such that the Welch bound

$$\sqrt{\frac{N_n - K_n}{(N_n - 1)K_n}} \approx \sqrt{\frac{1-a}{a}}\frac{1}{\sqrt{N_n}}.$$

(2) There exists a positive constant c such that

$$I_{\max}(\mathcal{C}_n) - \sqrt{\frac{N_n - K_n}{(N_n - 1)K_n}} \le \frac{c}{N_n}.$$

We can check that all series of codebooks $\mathcal{C}(D)$ in the Table 1 nearly meeting the Welch bound by using following lemma.

Lemma 1.4 *A series (N_n, K_n) codebooks $\mathcal{C}_n$ $(n = 1, 2, \ldots)$ nearly meeting the Welch bound if $N_n, K_n \to \infty$ when $n \to \infty$ and for all $n \ge 1$ the following two conditions are satisfied*

(1) *there exist constants a and $b,\ 0 < a < 1,\ b > 0$ such that $|N_n - aK_n| \le b\sqrt{K_n}$;*
(2) *there exists a constant $d > 0$ such that*

$$K_n^2 I_{\max}(\mathcal{C}_n)^2 \le \frac{a-1}{a}K_n + d\sqrt{K_n}.$$

Proof Let $E_n = I_{\max}(\mathcal{C}_n) - \sqrt{\frac{N_n - K_n}{(N_n-1)K_n}}$. From now on, we omit the subscript n in $\mathcal{C}_n,\ E_n,\ N_n$ and K_n. Then $E \ge 0$ since $\sqrt{\frac{N-K}{(N-1)K}}$ is the lower bound of $I_{\max}(\mathcal{C})$. We have

$$\begin{aligned}
E\left(I_{\max}(\mathcal{C}) + \sqrt{\frac{N-K}{(N-1)K}}\right) &= I_{\max}(\mathcal{C})^2 - \frac{N-K}{(N-1)K} \\
&\le \frac{1}{K^2}\left(\frac{a-1}{a}K + d\sqrt{K}\right) - \frac{N-K}{(N-1)K} \quad (\text{ by condition } (2)) \\
&= \frac{(a-1)(N-1)K + ad(N-1)\sqrt{K} - aK(N-K)}{a(N-1)K^2} \\
&= \frac{K(aK-N) - (a-1)K + ad(N-1)\sqrt{K}}{a(N-1)K^2} \\
&\le \frac{b\sqrt{K}K - (a-1)K + ad(N-1)\sqrt{K}}{a(N-1)K^2} \quad (\text{ by condition } (1)) \\
&\le \frac{c'}{N^{3/2}} \quad (\text{ for some } c' > 0),
\end{aligned}$$

and

$$I_{\max}(\mathcal{C}) + \sqrt{\frac{N-K}{(N-1)K}} \ge 2\sqrt{\frac{N-K}{(N-1)K}} \ge \frac{c''}{N^{1/2}} \quad (\text{ for some } c'' > 0).$$

Therefore $E \le c/N$ for $c = c'/c'' > 0$. This completes the proof of Lemma 1.4.

In this paper we present several general constructions of codebooks which nearly meet the Welch bound by using cyclotomic classes in finite fields. All constructions can be viewed as generalizations of the codebooks derived from the DS in Lemma 1.2, ADS in Lemma 1.3 and one construction (Theorem 4.1) derived from a series of ADS given in Theorem 2.2 [7]. Our main aim is to show that such series of codebooks $\mathcal{C}(D)$ are as good as ones constructed by ADS under rather looser conditions than ones required by D being DS or ADS. We give these cyclotomic constructions of codebooks in Sects. 3–4 and introduce several preliminaries on Gauss sums, Gauss periods and cyclotomic numbers in Sect. 2.

2 Preliminaries

In this section we introduce some basic facts on Gauss sums, Gauss periods and cyclotomic numbers we need in Sects. 3 and 4. For the detail we refer to books [2,5] and papers [1,3,4].

2.1 Gauss sums

Let $q = p^s$ where $s \geq 1$ and p be a prime, $T : \mathbb{F}_q \to \mathbb{F}_p$ be the trace mapping. For a multiplicative character χ of $\mathbb{F}_q$ (we assume $\chi(0) = 0$), the Gauss sum over $\mathbb{F}_q$ is defined by

$$G(\chi) = \sum_{x \in \mathbb{F}_q^{\times}} \chi(x)\zeta_p^{T(x)} \quad \left(\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}\right).$$

In this paper we need the following basic properties and particular values of Gauss sums.

Theorem 2.1 (1) *For $\chi = 1$ (the trivial character), $G(\chi) = -1$. For $\chi \neq 1$,*

$$|G(\chi)| = \sqrt{q}, \ \overline{G(\chi)} = \chi(-1)G(\bar{\chi}),$$

where $\bar{\chi} = \chi^{-1}$ is the conjugate of χ.

(2) *Let $q = p^s$ and $p \geq 3$, χ be the quadratic character of $\mathbb{F}_q$. Then*

$$G(\chi) = \begin{cases} (-1)^{s-1}\sqrt{q}, & if \ p \equiv 1 (mod 4) \\ (-1)^{s-1} i^s \sqrt{q}, & if \ p \equiv 3 (mod 4). \end{cases}$$

(3) *Let $p \equiv 1 (mod 4)$, $q = p^m = A^2 + B^2$ where A and B be integers, $(p, A) = 1$ and $A \equiv 1 (mod 2)$. For a character χ of $\mathbb{F}_q$ with order 4, $\left\{G(\chi)^2, G(\bar{\chi})^2\right\} = \left\{\sqrt{q}(A + iB), \sqrt{q}(A - iB)\right\}$.*

2.2 Gauss periods

Let α be a primitive element of $\mathbb{F}_q$ such that $\mathbb{F}_q^{\times} =< \alpha >$. Let $q = p^s$, $q - 1 = ef$ $(e \geq 2)$ and $T : \mathbb{F}_q \to \mathbb{F}_p$ be the trace mapping. For the cyclotomic classes of order e in $\mathbb{F}_q$

$$D_\lambda = D_\lambda^{(e,q)} = \alpha^\lambda < \alpha^e > \quad (0 \leq \lambda \leq e - 1), \tag{3}$$

we define the Gauss periods of order e on $\mathbb{F}_q$ by

$$\eta_\lambda = \sum_{x \in D_\lambda} \zeta_p^{T(x)} \quad (0 \leq \lambda \leq e - 1).$$

Let χ be the character of $\mathbb{F}_q$ with order e defined by $\chi(\alpha) = \zeta_e$. Then

$$\eta_\lambda = \frac{1}{e}\sum_{x\in\mathbb{F}_q^\times}\zeta_p^{T(x)}\sum_{i=0}^{e-1}\chi^i\left(x\alpha^{-\lambda}\right) = \frac{1}{e}\sum_{i=0}^{e-1}\bar{\zeta}_e^{i\lambda}G\left(\chi^i\right). \tag{4}$$

Therefore η_λ can be computed if we know the values of Gauss sums $G(\chi^i)$ $(0 \le i \le e-1)$.

2.3 Cyclotomic numbers

For the cyclotomic classes D_λ defined by (3), the cyclotomic numbers of order e on $\mathbb{F}_q$ are defined by

$$(i, j) = (i, j)_e^{(q)} = \sharp\{x \in D_i : x + 1 \in D_j\} \quad (0 \le i, j \le e-1).$$

In Sects. 3 and 4, we need the following values of cyclotomic numbers listed in [5].

Lemma 2.2 (1) *Let $p \equiv 5(mod 8)$, $q = p^{2m+1} = a^2+4b^2$, $a \equiv 1(mod 4)$ and $(a, p) = 1$. Then $(i, j) = (i, j)_4^{(q)}$ $(0 \le i, j \le 3)$ are given explicitly by Table 2 and the relations*

$$16A = q - 7 + 2a, \quad 16B = q + 1 + 2a - 8b, \quad 16C = q + 1 - 6a,$$
$$16D = q + 1 + 2a + 8b, \quad 16E = q - 3 - 2a.$$

(2) *Let $p \equiv 7(mod 12)$, $q = p^{2m+1}$, $q = a^2 + 27b^2$ where $a,\ b \in \mathbb{Z}$ and $(a, p) = 1$. Then $(i, j) = (i, j)_6^{(q)}$ $(0 \le i, j \le 5)$ are given explicitly by Table 3 and the relations*

$$36A = q - 11 - 8a, \quad 36B = 36C = q + 1 - 2a + 12b,$$
$$36D = q + 1 + 16a, \quad 36E = 36F = q + 1 - 2a - 12b,$$
$$36G = q - 5 + 4a + 6b, \quad 36H = q - 5 + 4a - 6b, \quad 36I = 36J = q + 1 - 2a.$$

(3) *Let $p \equiv 9(mod 16)$, $q = p^{2m+1} = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \equiv 1(mod 4)$ and $4|y$. Then the $(i, j) = (i, j)_8^{(q)}$ $(0 \le i, j \le 7)$ are given explicitly by Table 4 and the relations*

$$64A = q - 15 - 2x, \quad 64B = 64F = q + 1 + 2x - 4a + 16y,$$
$$64E = q + 1 - 18x, \quad 64D = 64H = q + 1 + 2x - 4a - 16y,$$
$$64C = q + 1 + 6x + 8a - 16y, \quad 64I = 64J = q - 7 + 2x + 4a,$$
$$64G = q + 1 + 6x + 8a + 16y, \quad 64L = 64O = q + 1 + 2x - 4a,$$
$$64K = q + 1 - 6x + 4a + 16b, \quad 64N = q - 7 - 2x - 8a,$$
$$64M = q + 1 - 6x + 4a - 16b.$$

Remark The Table 3 listed in [2] is under the condition that 2 is a cubic in $\mathbb{F}_q^\times$. But by Theorem 7.1.1 in [2], P.213, it can be seen that this condition is equivalent to $q = a^2 + 27b^2$ for $a,\ b \in \mathbb{Z}$ and $(a, p) = 1$.

Table 2

i \ j	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

Table 3

j i	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	E	C	I
2	H	J	G	F	I	B
3	A	G	H	A	G	H
4	G	F	I	B	H	J
5	H	I	E	C	I	G

Table 4

j i	0	1	2	3	4	5	6	7
0	A	B	C	D	E	F	G	H
1	I	J	K	L	F	D	L	M
2	N	O	N	M	G	L	C	K
3	J	O	O	I	H	M	K	B
4	A	I	N	J	A	I	N	J
5	I	H	M	K	B	J	O	O
6	N	M	G	L	C	K	N	O
7	J	K	L	F	D	L	M	I

3 First construction

In this section, we present first construction of codebooks $\mathcal{C}(D)$ which nearly meet the Welch bound. We take $\mathbb{F}_q$ as underlying additive group G and subset D as a cyclotomic class or a union of cyclotomic classes of order $e = 4,\ 6$ and 8 in $\mathbb{F}_q$.

Let $q = p^m,\ q-1 = ef\ (e \geq 2),\ \mathbb{F}_q^\times =<\alpha>$ and $D_\lambda = D_\lambda^{(e,q)} = \alpha^\lambda <\alpha^e>\quad (0 \leq \lambda \leq e-1)$ be the cyclotomic classes of order e in $\mathbb{F}_q$. For $1 \leq l \leq e-1$, let

$$\begin{aligned} D &= \bigcup_{s=1}^{l} D_{\lambda_s} \ \ (0 \leq \lambda_1 < \cdots < \lambda_l \leq e-1) \\ &= \{x_1, \ldots, x_K\} \ \ (K = lf = l(q-1)/e) \end{aligned}$$

be a union of l distinct cyclotomic classes. Consider the following $(N, K) = (q, l(q-1)/e)$ codebook

$$\mathcal{C}(D) = \left\{ c_b = \frac{1}{\sqrt{K}}(\varphi_b(x_1), \ldots, \varphi_b(x_K)) : b \in \mathbb{F}_q \right\}, \tag{5}$$

where $\{\varphi_b : b \in \mathbb{F}_q\}$ is the group of additive characters of $\mathbb{F}_q$ and φ_b is defined by $\varphi_b(x) = \zeta_p^{T(bx)}\ (x \in \mathbb{F}_q)$.

Theorem 3.1 *For fixed $e,\ l\ (1 \leq l \leq e-1)$, and $q \to \infty$ the series of codebooks $\mathcal{C}(D)$ defined by (5) nearly meet the Welch bound if*

$$\sum_{i=0}^{e-1} \eta_{j+i} \sum_{s,t=1}^{l} ((\lambda_s - i, \lambda_t - i)) = O(\sqrt{q}) \ \ (0 \leq j \leq e-1), \tag{6}$$

where $\eta_j = \sum_{x \in D_j} \zeta_p^{T(x)}$ $(0 \leq j \leq e-1)$ are the Gauss periods, and

$$((i, j)) = (i, j)_e^{(q)} - \frac{q-1}{e^2} \ \ (0 \leq i, j \leq e-1).$$

Proof Since $K = lf$ and $N = q = 1 + ef = \frac{e}{l}K + 1$, from Lemma 1.4 we know that the codebook $\mathcal{C}(D)$ nearly meets the Welch bound if, by taking $a = e/l$,

$$K^2 \left| c_{b_1} c_{b_2}^H \right|^2 \le \frac{a-1}{a} K + O\left(\sqrt{K}\right) = \frac{e-l}{e} K + O\left(\sqrt{K}\right) \tag{7}$$

for all distinct b_1 and b_2 in $\mathbb{F}_q$. But

$$K\left(c_{b_1} c_{b_2}^H\right) = \sum_{x \in D} \varphi_{b_1}(x) \bar{\varphi}_{b_2}(x) = \sum_{x \in D} \varphi_b(x),$$

where $b = b_1 - b_2 \neq 0$. Therefore

$$\begin{aligned} K^2 \left| c_{b_1} c_{b_2}^H \right|^2 &= \sum_{x,y \in D} \varphi_b(x) \bar{\varphi}_b(y) = \sum_{x,y \in D} \varphi_b(x-y) \\ &= K + \sum_{\substack{x,y \in D \\ x \neq y}} \varphi_b(x-y). \end{aligned}$$

Thus the condition (7) is equivalent to

$$\sum_{\substack{x,y \in D \\ x \neq y}} \varphi_b(x-y) = -\frac{l}{e} K + O\left(\sqrt{K}\right) \ \left(for\ all\ b \in \mathbb{F}_q^\times \right). \tag{8}$$

By the definition of D we have

$$\begin{aligned} \sum_{\substack{x,y \in D \\ x \neq y}} \varphi_b(x-y) &= \sum_{z \in \mathbb{F}_q^\times} \varphi_b(z) \sum_{\substack{y \in D \\ y+z \in D}} 1 = \sum_{i=0}^{e-1} \sum_{z \in C_i} \zeta_p^{T(bz)} \sum_{s,t=1}^{l} \sum_{\substack{y \in C_{\lambda_s} \\ y+z \in C_{\lambda_t}}} 1 \\ &= \sum_{i=0}^{e-1} \sum_{z \in C_i} \zeta_p^{T(bz)} \sum_{s,t=1}^{l} (\lambda_s - i, \lambda_t - i)_e^{(q)} \\ &= \sum_{i=0}^{e-1} \sum_{z \in C_i} \zeta_p^{T(bz)} \sum_{s,t=1}^{l} \left(\frac{q-1}{e^2} + ((\lambda_s - i, \lambda_t - i)) \right) \\ &= \frac{(q-1)l^2}{e^2} \sum_{z \in \mathbb{F}_q^\times} \zeta_p^{T(bz)} + \sum_{i=0}^{e-1} \eta_{i+j} \sum_{s,t=1}^{l} ((\lambda_s - i, \lambda_t - i)), \end{aligned}$$

where j is determined by $b \in D_j$. Since

$$\frac{(q-1)l^2}{e^2} \sum_{z \in \mathbb{F}_q^\times} \zeta_p^{T(bz)} = -\frac{(q-1)l^2}{e^2} = -\frac{l}{e} K,$$

the condition (8) is equivalent to (6). This completes the proof of Theorem 3.1.

Now we show some applications of Theorem 3.1 in case $e = 4$, 6 and 8.

Corollary 3.2 *Let* $p \equiv 5 (mod 8)$, $q = p^{2m+1} = a^2 + 4b^2$, $a \equiv 1 (mod 4)$, a, $b > 0$, *and* $(a, p) = 1$. *Let* $D_\lambda = D_\lambda^{(4,q)}$ $(0 \le \lambda \le 3)$ *be the cyclotomic classes of order 4 in* $\mathbb{F}_q$.

(1) For $D = D_\lambda$ $(0 \le \lambda \le 3)$, the series of $(N, K) = (q, (q-1)/4)$ codebooks $\mathcal{C}(D)$ defined by (5) nearly meet the Welch bound $\sqrt{\frac{N-K}{(N-1)K}} = \frac{\sqrt{3q+1}}{q-1}$ if a is bound. More exactly, we have

$$I_{\max}(\mathcal{C}(D)) - \frac{\sqrt{3q+1}}{q-1} \le \frac{a+1}{\sqrt{3}(q-1)}.$$

(2) For $D = D_\lambda \bigcup D_{\lambda+1}$ $(0 \le \lambda \le 3)$, the series of $(N, K) = (q, (q-1)/2)$ codebooks $\mathcal{C}(D)$ nearly meet the Welch bound $\sqrt{\frac{N-K}{(N-1)K}} = \frac{\sqrt{q+1}}{q-1}$, if b is bounded. More exactly, we have

$$I_{\max}(\mathcal{C}(D)) - \frac{\sqrt{q+1}}{q-1} \le \frac{b}{q-1}.$$

Proof (1) For $D = D_\lambda$, the left-hand side of (6) becomes

$$\begin{aligned}\sum_{i=0}^{3} \eta_{i+j}((\lambda - i, \lambda - i)) &= \sum_{i=0}^{3} \eta_{i+j}((i-\lambda, 0))\ (0 \le j \le 3)\\ &= \sum_{i=0}^{3} \eta_{k+i}((i, 0))\ \ (0 \le k \le 3,\ k = j + \lambda),\end{aligned}$$

since $(i, j) = (-i, j - i)$ so that $((i, j)) = ((-i, j - i))$. By Lemma 2.2 (1) we have

$$((0,0)) = ((2,0)) = \frac{-3+a}{8},\quad ((1,0)) = ((3,0)) = \frac{-1-a}{8}. \tag{9}$$

Thus

$$\sum_{i=0}^{3} \eta_{k+i}((i,0)) = \frac{1}{8}\left[(\eta_k + \eta_{k+2})(-3+a) + (\eta_{k+1} + \eta_{k+3})(-1-a)\right]. \tag{10}$$

By (4) we know that $\eta_k = O(\sqrt{q})$ $(0 \le k \le 3)$ so that $\sum_{i=0}^{3} \eta_{k+i}((i,0)) = O(\sqrt{q})$, thus the codebook $\mathcal{C}(D)$ nearly meets the Welch bound if a is bounded. More exactly, it is known that

$$\eta_0 + \eta_2 = \sum_{x \in D_0^{(2,q)}} \zeta_p^{T(x)} = \frac{1}{2}(-1 + \sqrt{q}),$$

$$\eta_1 + \eta_3 = \sum_{x \in D_1^{(2,q)}} \zeta_p^{T(x)} = \frac{1}{2}(-1 - \sqrt{q}).$$

By (10) we get $\sum_{i=0}^{3} \eta_{k+i}((i,0)) = \frac{1}{8}\left(2 \pm (a-1)\sqrt{q}\right)$. Therefore

$$\begin{aligned}I_{\max}(\mathcal{C}(D)) &\le \frac{1}{K}\left(\frac{3K}{4} + \frac{1}{8}(2 + (a+1)\sqrt{q})\right)^{\frac{1}{2}}\\ &= \frac{1}{q-1}\sqrt{3q + 2(a+1)\sqrt{q} + 1}.\end{aligned}$$

Therefore

$$I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} \leq \frac{1}{q-1}\left(\sqrt{3q+2(a+1)\sqrt{q}+1} - \sqrt{3q+1}\right)$$
$$\leq \frac{a+1}{\sqrt{3}(q-1)}.$$

(2) For $D = D_\lambda \bigcup D_{\lambda+1}$, the left-hand side of (6) becomes

$$\sum_{i=0}^{3} \eta_{k+i}\left[((-i,-i)) + ((-i,1-i)) + ((1-i,-i)) + ((1-i,1-i))\right]$$
$$= \sum_{i=0}^{3} \eta_{k+i}\left[((i,0)) + ((i,1)) + ((i-1,3)) + ((i-1,0))\right] \ (0 \leq k \leq 3). \quad (11)$$

By Lemma 2.2 (1), we have (9) and

$$((0,1)) = ((1,3)) = (1+a-4b)/8,$$
$$((0,3)) = ((3,1)) = (1+a+4b)/8,$$
$$((1,1)) = ((2,1)) = ((2,3)) = ((3,3)) = (-1-a)/8.$$

It can be computed that the right-hand side of (11) is

$$\frac{1}{2}(\eta_k + \eta_{k+2})(-1-b) + \frac{1}{2}(\eta_{k+1} + \eta_{k+3})(-1+b)$$
$$= \frac{1}{4}\left(-1 \pm \sqrt{q}\right)(-1-b) + \frac{1}{4}\left(-1 \mp \sqrt{q}\right)(-1+b)$$
$$= \frac{1}{2}\left(1 \pm b\sqrt{q}\right).$$

Therefore

$$I_{\max}(\mathcal{C}(D)) = \frac{1}{K}\left(\frac{K}{2} + \frac{1}{2}\left(1 + b\sqrt{q}\right)\right)^{1/2} = \frac{1}{q-1}\sqrt{q+1+2b\sqrt{q}},$$

and

$$I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} = \frac{1}{q-1}\left(\sqrt{q+1+2b\sqrt{q}} - \sqrt{q+1}\right) \leq \frac{b}{q-1},$$

which means that the codebook $\mathcal{C}(D)$ nearly meets the Welch bound if b is bounded. This completes the proof of Corollary 3.2.

Corollary 3.3 (1) *Let $p \equiv 7(mod 12)$, $q = p^{2m+1}, q = a^2 + 27b^2$, a, $b > 0$ and $(a, p) = 1$. Then for*

$$D = D_k^{(6,q)} \bigcup D_{k+1}^{(6,q)} \bigcup D_{k+3}^{(6,q)} \ (0 \leq k \leq 5),$$

the series of $(N, K) = \left(q, \frac{q-1}{2}\right)$ codebooks $\mathcal{C}(D)$ nearly meet the Welch bound provided b is bounded.

(2) *Let $p \equiv 9(mod 16)$, $q = p^{2m+1} = x^2+4y^2 = a^2+2b^2, 4q = a^2+3b^2\, x$, $a > 0$, $4|y$ and $(p, x) = (a, x) = 1$. Then for $D = D_\lambda^{(8,q)}$, the series of $(N, K) = \left(q, \frac{q-1}{8}\right)$ codebooks $\mathcal{C}(D)$ nearly meet the Welch bound provided both x and a are both bounded.*

Proof (1) In this case the left-hand side of (6) becomes $\sum_{i=0}^{5} \eta_{j+i} M_i$ $(0 \le j \le 5)$, where

$$M_i = \sum_{\lambda,\mu \in \{0,1,3\}} ((\lambda - i, \mu - i)) \quad (0 \le i \le 5).$$

By $((i,j)) = (i,j)_6^{(q)} - \frac{q-1}{36}$ and $(i,j)_6^{(q)}$ $(0 \le i, j \le 6)$ are listed in Lemma 2.2 (2), we get

$$\begin{aligned} M_0 &= ((0,0)) + ((0,1)) + ((0,3)) + ((1,0)) \\ &\quad + ((1,1)) + ((1,3)) + ((3,0)) + ((3,1)) + ((3,3)) \\ &= A + B + D + G + H + E + A + G + A - \frac{q-1}{4} = \frac{-6+b}{6}. \end{aligned}$$

Similarly we can get $M_3 = M_0$, $M_1 = M_4 = -\frac{1}{2}$, $M_2 = M_5 = -\frac{b}{6}$. Thus

$$\begin{aligned} \sum_{i=0}^{5} \eta_{j+i} M_i &= \frac{1}{6}\big[(\eta_j + \eta_{j+3})(-6+b) + (\eta_{j+1} + \eta_{j+4})(-3) \\ &\quad + (\eta_{j+2} + \eta_{j+5})(-b)\big], \end{aligned}$$

so that $\sum_{i=0}^{5} \eta_{j+i} M_i = O(\sqrt{q})$ and $\mathcal{C}(D)$ nearly meets the Welch bound if b is bounded.

(2) In this case the left-hand side of (6) becomes $\sum_{i=0}^{7} \eta_{k+i}((i,0))$ $(0 \le k \le 7)$. By the table of values $(i,0)_8^{(q)} = \frac{q-1}{64} + ((i,0))$ given in Lemma 2.2 (3), we get

$$\begin{aligned} ((0,0)) = ((4,0)) &= \frac{1}{32}(-7 - x), \\ ((2,0)) = ((6,0)) &= \frac{1}{32}(-3 - x - 4a), \\ ((1,0)) = ((3,0)) = ((5,0)) = ((7,0)) &= \frac{1}{32}(-3 + x + 2a). \end{aligned}$$

Therefore $\sum_{i=0}^{7} \eta_{k+i}((i,0)) = O(\sqrt{q})$ $(0 \le k \le 7)$ and the codebook $\mathcal{C}(D)$ nearly meets the Welch bound if both x and a are bounded. This completes the proof of Corollary 3.3.

Remark (1) The upper bound of $I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}}$ can be estimated by using (4) and the values of Gauss sums $G(\chi)$ for characters χ of order 3 and 4. The results are too complicate to be written.

(2) The constructions in Corollary 3.2 and 3.3 can be viewed as generalizations of the constructions from difference sets given in Lemma 1.2 (A), (B) and (C) and almost difference sets given in Lemma 1.3 (I) and (II).

4 Second construction

In this section we consider the underlying group to be $\mathbb{Z}_4 \times \mathbb{F}_q$ or $\mathbb{F}_2 \times \mathbb{F}_q$. Firstly, we assume that $q = p^m$ and $p \ge 3$. Let $D_\lambda = D_\lambda^{(2,q)}$ $(\lambda = 0,\ 1)$ and consider the following subset of the additive group $\mathbb{Z}_4 \times \mathbb{F}_q$,

$$\begin{aligned} D &= [\{0\} \times D_0] \bigcup [\{1,2,3\} \times D_1] \\ &= \{x_1, x_2, \ldots, x_K\} \;\; K = |D| = 2(q-1). \end{aligned} \tag{12}$$

We construct the following $(N, K) = (4q, 2(q-1))$ codebook

$$\mathcal{C}(D) = \left\{ c_\chi = \frac{1}{\sqrt{K}} (\chi(x_1), \chi(x_2), \ldots, \chi(x_K)) : \chi \in (\mathbb{Z}_4 \times \mathbb{F}_q)^\wedge \right\}, \tag{13}$$

where $(\mathbb{Z}_4 \times \mathbb{F}_q)^\wedge$ is the character group of additive group $\mathbb{Z}_4 \times \mathbb{F}_q$. Each character χ can be uniquely expressed by $\chi_\alpha = \lambda_a \lambda_b$ where $\alpha = (a, b),\ a \in \mathbb{Z}_4,\ b \in \mathbb{F}_q$ and for $x = (x_1, x_2) \in \mathbb{Z}_4 \times \mathbb{F}_q$,

$$\chi_\alpha(x) = \lambda_a(x_1)\lambda_b(x_2) = \zeta_4^{ax_1} \zeta_p^{T(bx_2)}$$

and the $T : \mathbb{F}_q \to \mathbb{F}_p$ be the trace mapping.

Theorem 4.1 *For the* $(N, K) = (4q, 2(q-1))$ *codebook defined by* (12) *and* (13)*, we have*

$$I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} \le \begin{cases} \frac{1}{q-1}, & if\ q \equiv 1(mod 4) \\ \frac{15}{8(q-1)\sqrt{4q-1}}, & if\ q \equiv 3(mod 4). \end{cases}$$

Particularly, the series of $\mathcal{C}(D)$ *nearly meet the Welch bound.*

Proof For distinct elements c and c' in the codebook $\mathcal{C}(D)$,

$$\begin{aligned} K(c'c^H) &= \sum_{x \in D} \chi_\alpha(x) \quad \left(\text{for some } \chi_\alpha,\ 1 \ne \chi_\alpha = \lambda_a\lambda_b \in \widehat{\mathbb{Z}_4} \times \widehat{\mathbb{F}_q}\right) \\ &= \sum_{y \in D_0} \lambda_b(y) + (\lambda_a(1) + \lambda_a(2) + \lambda_a(3)) \sum_{y \in D_1} \lambda_b(y) \\ &\quad (a \in \mathbb{Z}_4, b \in \mathbb{F}_q, (a, b) \ne (0, 0)). \end{aligned}$$

If $b = 0$ and $a \ne 0$, then $K\left(c'c^H\right) = \frac{q-1}{2} - \frac{q-1}{2} = 0$.
If $b \ne 0$, and $a = 0$, then

$$\begin{aligned} K(c'c^H) &= \sum_{y \in D_0} \lambda_b(y) + 3 \sum_{y \in D_1} \lambda_b(y) = -1 + 2 \sum_{y \in D_1} \lambda_b(y) \\ &= -1 + \sum_{y \in \mathbb{F}_q^\times} \lambda_b(y)(1 - \eta(y)) \left(\eta \text{ is the quadratic character of } \mathbb{F}_q^\times\right) \\ &= -2 - \eta_b G(\eta) = -2 \pm G(\eta). \end{aligned}$$

If $b \ne 0$ and $a \ne 0$, then

$$K(c'c^H) = \sum_{y \in D_0} \lambda_b(y) - \sum_{y \in D_1} \lambda_b(y) = \eta_b G(\eta) = \pm G(\eta).$$

Since $G(\eta) = \pm\sqrt{q}$ for $q \equiv 1(\text{mod}4)$ and $G(\eta) = \pm\sqrt{q}\zeta_4$ for $q \equiv 3(\text{mod}4)$. We get that for $q \equiv 1(\text{mod}4)$,

$$I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} \le \frac{\sqrt{q}+2}{2(q-1)} - \sqrt{\frac{q+1}{(4q-1)(q-1)}} \le \frac{1}{q-1}.$$

For $q \equiv 3(\mathrm{mod}4)$

$$|c'c^H| \leq \frac{1}{K}|2 \pm \sqrt{q}\zeta_4| = \frac{\sqrt{q+4}}{2(q-1)},$$

and

$$\begin{aligned} I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} &\leq \frac{\sqrt{q+4}}{2(q-1)} - \sqrt{\frac{q+1}{(4q-1)(q-1)}} \\ &= \frac{15q}{2(q-1)\sqrt{4q-1}(\sqrt{4q^2+15q-4} - \sqrt{4q^2-4})} \\ &\leq \frac{15}{8(q-1)\sqrt{4q-1}}. \end{aligned}$$

Remark For the case $q \equiv 3(\mathrm{mod}4)$, the set D' defined by (12) plus three elements $(0,0), (1,0), (3,0)$ is an almost difference set of $\mathbb{Z}_4 \times \mathbb{F}_q$ in Theorem 2.2 [7]. We can also show that $\mathcal{C}(D')$ nearly meets the Welch bound. Moreover, for case $q \equiv 3(\mathrm{mod}4)$ the difference between $I_{\max}(\mathcal{C}(D))$ and the Welch bound is $O(N^{3/2})$ which is better than required value $O(\frac{1}{N})$.

There are other series of ADS on underlying group in $\mathbb{F}_q \times \mathbb{F}_{q'}$ in [7]. We will deal with the related codebooks in successive paper.

Next, let $p \equiv 1(\mathrm{mod}4), q = p^m = A^2 + B^2,\ A,\ B \geq 1, 2|B$ and $(A, p) = 1$. Let $D_\lambda = D_\lambda^{(4,q)}$ $(0 \leq \lambda \leq 3)$ be the cyclotomic classes of order 4 in $\mathbb{F}_q$. We consider the following subset of the additive group $G = \mathbb{F}_2 \times \mathbb{F}_q$,

$$\begin{aligned} D &= \left[\{0\} \times \left(D_i \bigcup D_j\right)\right] \bigcup \left[\{1\} \times \left(D_k \bigcup D_j\right)\right] \\ &= \{x_1, x_2, \ldots, x_K\} \ \ K = |D| = q-1. \end{aligned} \tag{14}$$

Then we construct the following $(N, K) = (2q, q-1)$ codebook

$$\mathcal{C}(D) = \left\{\frac{1}{\sqrt{K}}(\chi(x_1), \ldots, \chi(x_K)) : \chi \in (\mathbb{F}_2 \times \mathbb{F}_q)^\wedge\right\}, \tag{15}$$

where $(\mathbb{F}_2 \times \mathbb{F}_q)^\wedge$ is the character group of additive group $\mathbb{F}_2 \times \mathbb{F}_q$. Each character χ can be uniquely expressed by $\chi = \chi_1\lambda_b$ where $\chi_1 \in (\mathbb{F}_2, +)^\wedge$, such that $\chi_1(0) = 1$ and $\chi_1(1) = \pm 1$, and λ_b $(b \in \mathbb{F}_q)$ is the additive character of $\mathbb{F}_q$ defined by $\lambda_b(x) = \zeta_p^{T(bx)}$ $(x \in \mathbb{F}_q)$.

Theorem 4.2 *Under the assumptions above, the* $(N, K) = (2q, q-1)$ *codebook* $\mathcal{C}(D)$ *is defined by* (14) *and* (15). *Then*

$$I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} \leq \begin{cases} \frac{1}{q-1}\left(1 + \frac{A+4}{2\sqrt{2}}\right), & if\ \{i,k\} = \{j+1, j+3\} \\ \frac{1}{q-1}\left(1 + \frac{B+4}{4\sqrt{2}}\right), & if\ q \equiv 5(mod8), \{i,k\} = \ \{j+2, j+1\}\ or\ \{j+2, j+3\}. \end{cases}$$

Therefore the series of codebooks $\mathcal{C}(D)$ *nearly meet the Welch bound if one of following two conditions satisfied*

(1) $\{i,k\} = \{j+1, j+3\}$ *and* A *is bounded;*

(2) *$q \equiv 5(mod 8)$, $\{i, k\} = \{j+2, j+1\}$ or $\{j+2, j+3\}$, and B is bounded.*

Proof For distinct vectors c and c' in $\mathcal{C}(D)$,

$$K(c'c^H) = \sum_{x \in D} \chi(x) = \sum_{y \in D_i \bigcup D_j} \lambda_b(y) + \chi_1(1) \sum_{y \in D_k \bigcup D_j} \lambda_b(y),$$

where $\chi = \chi_1 \lambda_b$ is a non-trivial character of $\mathbb{F}_2 \times \mathbb{F}_q$.

If $b = 0$, then $\chi_1(1) = -1$ and

$$K(c'c^H) = \sum_{y \in D_i \bigcup D_j} 1 - \sum_{y \in D_k \bigcup D_j} 1 = \frac{q-1}{2} - \frac{q-1}{2} = 0. \tag{16}$$

If $b \neq 0$, for $b \in D_\lambda$ we have

$$\begin{aligned} K(c'c^H) &= \sum_{y \in D_i \bigcup D_j} \zeta_p^{T(by)} + \chi_1(1) \sum_{y \in D_k \bigcup D_j} \zeta_p^{T(by)} \\ &= (\eta_{\lambda+i} + \eta_{\lambda+j}) + \chi_1(1)(\eta_{\lambda+k} + \eta_{\lambda+j}), \end{aligned} \tag{17}$$

where by (4) and $\zeta_4 = \sqrt{-1}$,

$$\eta_l = \sum_{y \in D_l} \zeta_p^{T(y)} = \frac{1}{4}\left(-1 + \bar{\zeta_4}^{\,l} G(\chi) + (-1)^l G(\eta) + \zeta_4^l G(\bar{\chi})\right)$$

$0 \leq l \leq 3$ and χ is the multiplicative character of $\mathbb{F}_q^\times$ determined by $\chi(\alpha) = \zeta_4$ for a primitive element α of $\mathbb{F}_q$ and $\eta = \chi^2$ be the quadratic character of $\mathbb{F}_q^\times$. Thus (17) becomes

$$K(c'c^H) = \frac{1}{4}(A_0 + A_1 G(\chi) + A_2 G(\eta) + A_3 G(\overline{\chi})), \tag{18}$$

where

$$\begin{aligned} A_0 &= -2 - 2\chi_1(1), \\ A_m &= \bar{\zeta_4}^{\lambda m} \left(\bar{\zeta_4}^{im} + \bar{\zeta_4}^{jm} + \chi_1(1)\left(\bar{\zeta_4}^{km} + \bar{\zeta_4}^{jm}\right)\right) \ (m = 1, 2, 3). \end{aligned}$$

(1) Firstly we assume that $i = j+1$ and $k = j+3$. Then

$$A_0 = \begin{cases} -4, & if\ \chi_1(1) = 1 \\ 0, & if\ \chi_1(1) = -1. \end{cases}$$

$$\begin{aligned} A_m &= \bar{\zeta_4}^{(\lambda+j)m}\left(\bar{\zeta_4}^{m} + 1 + \chi_1(1)\left(\zeta_4^m + 1\right)\right) \\ &= \begin{cases} \bar{\zeta_4}^{(\lambda+j)m}\left(2 + \bar{\zeta_4}^{m} + \zeta_4^m\right), & if\ \chi_1(1) = 1 \\ \\ \bar{\zeta_4}^{(\lambda+j)m}\left(\bar{\zeta_4}^{m} - \zeta_4^m\right), & if\ \chi_1(1) = -1. \end{cases} \end{aligned}$$

Therefore (18) becomes

$$K(c'c^H) = \begin{cases} -1 + \frac{1}{2}\left(\bar{\zeta_4}^{\lambda+j} G(\chi) + \zeta_4^{\lambda+j} G(\bar{\chi})\right), & if\ \chi_1(1) = 1 \\ \\ \frac{1}{2}\left(\bar{\zeta_4}^{\lambda+j+1} G(\chi) + \zeta_4^{\lambda+j+1} G(\bar{\chi})\right), & if\ \chi_1(1) = -1. \end{cases} \tag{19}$$

If $q \equiv 5(\text{mod}8)$, then $\overline{G(\chi)} = \chi(-1)G(\bar{\chi}) = -G(\bar{\chi})$, $\bar{\zeta_4}^{l}G(\chi) + \zeta_4^{l}G(\bar{\chi}) = \alpha\zeta_4$ for some real number α. Therefore, for $\chi_1(1) = 1$,

$$\begin{aligned} K^2|c'c^H|^2 &= 1 - \frac{1}{4}\left(\bar{\zeta_4}^{\lambda+j}G(\chi) - \zeta_4^{\lambda+j}\overline{G(\chi)}\right)^2 \\ &= 1 + \frac{1}{4}\left(2G(\chi)\overline{G(\chi)} + (-1)^{\lambda+j+1}G(\chi)^2 + (-1)^{\lambda+j+1}\overline{G(\chi)}^2\right). \end{aligned}$$

Since $G(\chi)^2 = \sqrt{q}(A + B\zeta_4),\ G(\chi)\overline{G(\chi)} = q$ we get

$$K^2\left|c'c^H\right|^2 = 1 + \frac{1}{2}\left(q \pm A\sqrt{q}\right). \tag{20}$$

Similarly, for $\chi_1(1) = -1$, we have

$$K^2\left|c'c^H\right|^2 = \frac{1}{2}\left(q \pm A\sqrt{q}\right). \tag{21}$$

By (16), (20) and (21) we get, for $q \equiv 5(\text{mod}8)$

$$I_{\max}(\mathcal{C}(D)) = \frac{1}{K}\sqrt{\frac{q + A\sqrt{q}}{2} + 1} = \frac{1}{q-1}\sqrt{\frac{q + A\sqrt{q}}{2} + 1},$$

and

$$\begin{aligned} I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} &\le \frac{1}{q-1}\left(1 + \sqrt{\frac{q + A\sqrt{q}}{2}} - \sqrt{\frac{q^2-1}{2q-1}}\right) \\ &\le \frac{1}{q-1}\left(1 + \frac{A}{2\sqrt{2}}\right) \le \frac{1}{q-1}\left(1 + \frac{A+4}{2\sqrt{2}}\right). \end{aligned} \tag{22}$$

If $q \equiv 1(\text{mod}8)$, then $G(\bar{\chi}) = \overline{G(\chi)}$ and the right-hand side of (19) are real numbers. Thus

$$K^2\left|c'c^H\right|^2 \le 1 + \frac{1}{2}\left(q + A\sqrt{q}\right) + 2\sqrt{q},$$

so that

$$I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} \le \frac{1}{q-1}\left(1 + \frac{A+4}{2\sqrt{2}}\right). \tag{23}$$

Put (22) and (23) together we get the result in case $i = j + 1$ and $k = j + 3$.

(2) Now we assume that $i = j + 2$ and $k = j + 3$. We still have (18) and

$$A_0 = \begin{cases} -4, & if\ \chi_1(1) = 1 \\ 0, & if\ \chi_1(1) = -1. \end{cases}$$

$$\begin{aligned} A_m &= \bar{\zeta_4}^{(\lambda+j)m}((-1)^m + 1 + \chi_1(1)(\zeta_4^m + 1)) \\ &= \begin{cases} \bar{\zeta_4}^{(\lambda+j)m}(2 + (-1)^m + \zeta_4^m), & if\ \chi_1(1) = 1 \\ \bar{\zeta_4}^{(\lambda+j)m}((-1)^m - \zeta_4^m), & if\ \chi_1(1) = -1. \end{cases} \end{aligned}$$

Therefore (18) becomes

$$K(c'c^H) = \begin{cases} -1 + \frac{1}{4}\Big[\bar{\zeta_4}^{\lambda+j}(1+\zeta_4)G(\chi) + 2(-1)^{\lambda+j}G(\chi^2) \\ \quad +\zeta_4^{\lambda+j}(1+\bar{\zeta_4})G(\bar{\chi})\Big], \quad if \quad \chi_1(1) = 1 \\ \frac{1}{4}\Big[\bar{\zeta_4}^{\lambda+j}(-1-\zeta_4)G(\chi) + 2(-1)^{\lambda+j}G(\chi^2) \\ \quad +\zeta_4^{\lambda+j}(-1-\bar{\zeta_4})G(\bar{\chi})\Big], \quad if \quad \chi_1(1) = -1. \end{cases}$$

If $q \equiv 5(\text{mod}8)$, then $\overline{G(\chi)} = -G(\bar{\chi}),\ G(\chi^2) = \sqrt{q}$ so that

$$\begin{aligned} K^2\left|c'c^H\right|^2 &\le \frac{1}{16}\left(\bar{\zeta_4}^{\lambda+j}(1+\zeta_4)G(\chi) - \zeta_4^{\lambda+j}(1+\bar{\zeta_4})\overline{G(\chi)}\right)^2 + \left(1+\frac{\sqrt{q}}{2}\right)^2 \\ &= \frac{q}{4} + \sqrt{q} + 1 + \frac{1}{16}\left(4q + 4B\sqrt{q}\right) = \frac{q}{2} + \frac{B+4}{4}\sqrt{q} + 1, \end{aligned}$$

and

$$\begin{aligned} I_{\max}(\mathcal{C}(D)) - \sqrt{\frac{N-K}{(N-1)K}} &\le \frac{1}{q-1}\left(\sqrt{\frac{q}{2} + \frac{B+4}{4}\sqrt{q} + 1} - \sqrt{\frac{q^2-1}{2q-1}}\right) \\ &\le \frac{1}{q-1}\left(1 + \frac{B+4}{4\sqrt{2}}\right). \end{aligned}$$

For the remain cases, the computations and estimations are similar as above, and to be omitted. This completes the proof of Theorem 4.2.

Remark The construction in Theorem 4.2 can be viewed as a generalization of construction from almost difference sets given in Lemma 1.3 (III).

Acknowledgments The second author is supported by grant of NSFC (No. 10990011), The Tsinghua National Lab. for Information Science and Technology, and The National Center for Theoretic Sciences in Hsinchu and Tainan of Taiwan when he visited there in June-July, 2010.

References

1. Arasu K.T., Ding C., Helleseth T., Kumar P.V., Martinsen H.: Almost difference sets and their sequences with optimal autocorrelation. IEEE Trans. Inform. Theory **47**(7), 2934–2943 (2001).
2. Berndt B.C., Evans R.J., Williams K.S.: Gauss and Jacobi Sums. Wiley-Interscience Pub, Chris (1998).
3. Ding C.: Complex codebooks from combinatorial designs. IEEE Trans. Inform. Theory **52**(9), 4229–4235 (2006).
4. Ding C., Feng T.: A generic construction of complex codebooks meeting the Welch bound. IEEE Trans. Inform. Theory **53**(11), 4245–4250 (2007).
5. Storer T.: Cyclotomy and Difference Sets. Marham, Chicago (1967).
6. Welch L.: Lower bounds on the maximum cross correlation of signals. IEEE Trans. Inform. Theory **20**(3), 397–399 (1974).
7. Zhang Y., Lei J.-g., Zhang S.-P.: A new family of almost difference sets and some necessary conditions. IEEE Trans. Inform. Theory **52**(5), 2052–2061 (2006).