Bull. Aust. Math. Soc. **93** (2016), 211–222
doi:10.1017/S0004972715000994

MORE CONSTRUCTIONS OF APPROXIMATELY MUTUALLY UNBIASED BASES

XIWANG CAO✉ and WUN-SENG CHOU

(Received 7 May 2015; accepted 9 May 2015; first published online 17 August 2015)

Abstract

Let m be a positive integer and p a prime number. We prove the orthogonality of some character sums over the finite field $\mathbb{F}_{p^m}$ or over a subset of a finite field and use this to construct some new approximately mutually unbiased bases of dimension p^m over the complex number field $\mathbb{C}$, especially with $p = 2$.

2010 *Mathematics subject classification*: primary 11T71; secondary 81P70.

Keywords and phrases: finite field, character sum, approximately mutually unbiased bases, quantum information theory.

1. Introduction

A basis $B = \{b_1, b_2, \ldots, b_n\}$ of the n-dimensional complex vector space $\mathbb{C}^n$ is orthonormal if

$$\langle b_i \mid b_j \rangle = \begin{cases} 1 & \text{for } 1 \le i = j \le n, \\ 0 & \text{for } 1 \le i \ne j \le n, \end{cases}$$

where $\langle u \mid v \rangle = \sum_{i=1}^{n} u_i \bar{v}_i$ is the Hermite inner product of the vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$. Two orthonormal bases B and B' are called mutually unbiased bases (MUBs) if and only if

$$|\langle b \mid b' \rangle|^2 = 1/n \quad \text{for all } b \in B \text{ and } b' \in B'. \tag{1.1}$$

The notion of MUBs was initially proposed by Schwinger [20] in 1960. He noticed that the corresponding (quantum) states of these MUBs are maximally incompatible. Using such a basis to obtain optimal outcomes leads to maximally random results compared to other bases. Therefore, MUBs constitute a basic ingredient in many applications of quantum information processing: quantum tomography, quantum key distribution in cryptography, discrete Wigner function, quantum teleportation, and quantum error correction codes (see [7, 9, 18, 19] and the references therein).

The work of X. Cao was supported by the NNSF of China (11371011). The work of W. Chou was supported by the MST of Taiwan under grant number 103-2115-M-001-006.

MUBs are also closely related to spherical 2-designs [4, 10], semifields [4], complex Hadamard matrices [3], orthogonal Latin squares [5], finite geometry [5], frames [3], planar functions [5] and character sums over finite fields [9, 17].

If $\mathcal{B} = \{B_1, \ldots, B_N\}$ is a collection of pairwise mutually unbiased bases of $\mathbb{C}^n$, then it can be shown that $N \le n + 1$ (see [1, 9]). An extremal set attaining this bound is called a *complete MUB*. Let $f(n)$ denote the maximum cardinality of any set containing pairwise mutually unbiased bases of $\mathbb{C}^n$. It is known that $f(n) = n + 1$ when n is a prime power and it is conjectured that complete MUBs only exist for such n (see [1, 5]). Little is known about $f(n)$ for other n, even for $f(6)$, but it is conjectured that $f(6) = 3$ (see [5]). The following results are shown in [5]:

(1) $f(n_1 n_2) \ge \min\{f(n_1), f(n_2)\}$ for all positive integer n_1, n_2;
(2) $f(n) \ne n$, in other words, $f(n) = n + 1$ or $f(n) \le n - 1$;
(3) $f(n^2) \ge L(n) + 2$, where $L(n)$ is the maximal number of mutually orthogonal Latin squares.

When the characteristic of the finite field $\mathbb{F}_q$ is odd, Klappenecker and Rötteler obtained the following two results.

Lemma 1.1 [9]. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \ge 5$. Define sets of vectors*

$$B_\alpha = \{b_{\lambda,\alpha} \mid \lambda \in \mathbb{F}_q\} \quad \text{where } b_{\lambda,\alpha} = \frac{1}{\sqrt{q}}(\omega_p^{\mathrm{tr}((k+\alpha)^3+\lambda(k+\alpha))})_{k\in\mathbb{F}_q},$$

in which ω_p is a pth root of unity in $\mathbb{C}$ and $\mathrm{tr}(\cdot)$ is the absolute trace. Let $B_\infty = \{e_1, \ldots, e_q\}$ denote the standard basis, where e_i has 1 in its ith component and 0 elsewhere. The standard basis B_∞ and the sets B_α, with $\alpha \in \mathbb{F}_q$, form a complete MUB of $\mathbb{C}^q$,

Lemma 1.2 [9]. *Let $\mathbb{F}_q$ be a finite field of odd characteristic p. Define*

$$B_a = \{v_{a,b} \mid b \in \mathbb{F}_q\} \quad \text{where } v_{a,b} = \frac{1}{\sqrt{q}}(\omega_p^{\mathrm{tr}(ax^2+bx)})_{x\in\mathbb{F}_q}.$$

Then the standard basis B_∞ and the sets B_a, with $a \in \mathbb{F}_q$, form a complete MUB of $\mathbb{C}^q$.

When the characteristic of the finite field is even, Klappenecker and Rötteler use Galois rings to construct some complete MUBs.

Since the restriction (1.1) is very strict, Shparlinski and Winterhof [22] propose the following definition:

Definition 1.3. The orthonormal bases in the set $\mathcal{B} = \{B_1, \ldots, B_N\}$ are called *approximately mutually unbiased bases* (AMUBs) if for all $u \in B_i, v \in B_j, 1 \le i \ne j \le N$,

$$|\langle u \mid v\rangle| \le \frac{1 + o(1)}{\sqrt{n}} \quad \text{or} \quad O\Big(\frac{1}{\sqrt{n}}\Big) \quad \text{or} \quad O\Big(\frac{\log(n)}{\sqrt{n}}\Big).$$

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

After the concept of AMUB was introduced by Shparlinski and Winterhof [22], AMUBs were constructed by using character sums over finite fields [11, 23, 24]. These AMUBs are closely related to spherical 2-designs, finite geometry and compressed sensing matrices.

In this paper, inspired by Lemmas 1.1 and 1.2, we present more constructions of AMUBs by using the orthogonality of some character sums over finite fields. Section 2 introduces properties of the character sums. We find that the character sums form an orthonormal basis of a certain complex function space. That is, every complex-valued function over a finite field can be decomposed as a linear combination of character sums. Then, in Section 3, we show how to use these character sums to construct more AMUBs.

2. Orthogonality of some character sums

In this section we fix a prime number p, a positive odd integer m and a positive integer k. Throughout, χ denotes the canonical additive character of $\mathbb{F}_{p^m}$. For $a, b \in \mathbf{F}_{p^m}$, the *Kloosterman sum* $K_m(a, b)$ is defined by

$$K_m(a,b) = \sum_{x \in \mathbf{F}_{p^m}}{}' \chi(ax + bx^{-1}).$$

For properties of $K_m(a, b)$, see, for example, [14, Ch. 5]. It is easy to check that $K_m(a, b) = K_m(1, ab) = K_m(ab, 1)$ for $ab \neq 0$, thus for convenience, we denote $K_m(1, a)$ by $K_m(a)$. The Kloosterman sums over $\mathbb{F}_{2^m}$ are determined by Lachaud and Wolfmann.

Lemma 2.1 [12]. *The set* $\{K_m(\lambda) \mid \lambda \in \mathbb{F}_{2^m}\}$ *is the set of all integers* $s \equiv -1 \pmod 4$ *in the range*

$$[-2^{m/2+1} + 1, 2^{m/2+1} + 1].$$

For $a, b \in \mathbf{F}_{2^m}$, define the character sums:

$$C_m^{(k)}(a,b) = \sum_{x \in \mathbf{F}_{2^m}} \chi(ax^{2^k+1} + bx),$$
$$G_m^{(k)}(a,b) = \sum_{x \in \mathbf{F}_{2^m}} \chi(ax^{2^k+1} + bx^{-1}).$$

Many interesting applications of these character sums have been found in coding theory and combinatorial applications of finite fields (see, for example, [2, 6, 8, 15]).

Lahtonen, McGuire and Ward gave the following evaluation.

Lemma 2.2 [13]. *If* m *is odd and* $\gcd(k, m) = 1$, *then*

$$C_m^{(k)}(1,1) = \left(\frac{2}{m}\right) 2^{(m+1)/2} = \begin{cases} 2^{(m+1)/2} & \text{if } m \equiv \pm 1 \pmod 8, \\ -2^{(m+1)/2} & \text{if } m \equiv \pm 3 \pmod 8, \end{cases}$$

where $(2/m)$ *is the Jacobi symbol.*

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

Define the trace map $\mathrm{Tr}_1^m(a) = \sum_{j=0}^{m-1} a^{2^j}$. From Lemma 2.2, follows:

LEMMA 2.3 [2]. *If m is odd and $\gcd(k, m) = 1$, then:*

(1) $C_m^{(k)}(a, b) = C_m^{(k)}(1, b/a^{1/(2^k+1)})$;

(2) $C_m^{(k)}(1, a) = C_m^{(k)}(1, a^2)$ *for all* $a \in \mathbb{F}_{2^m}$;

(3) $C_m^{(k)}(1, a) = 0$ *if and only if* $\mathrm{Tr}_1^m(a) = 0$;

(4) *if* $\mathrm{Tr}_1^m(a) = 1$, *there is an* $h \in \mathbb{F}_{2^m}$ *such that* $a = h^{2^k} + h^{2^{m-k}} + 1$ *and*

$$C_m^{(k)}(1, a) = \chi(h^{2^k+1} + h) C_m^{(k)}(1, 1) = \chi(h^{2^k+1} + h)\left(\frac{2}{m}\right) 2^{(m+1)/2}.$$

As a consequence, one has the following bound:

LEMMA 2.4. *Suppose that $q = 2^m$, m is odd and $\gcd(k, m) = 1$. For all $a, b \in \mathbb{F}_q$,*

$$|C_m^{(k)}(a, b)| \le \sqrt{2q}.$$

Let $V = \mathbb{C}^{\mathbb{F}_q}$ be the set of complex-valued functions from $\mathbb{F}_q$ to $\mathbb{C}$. For any pair of functions $f, g \in V$, define

$$(f, g) = \sum_{c \in \mathbb{F}_q} f(c)\overline{g(c)},$$

where the bar denotes the complex conjugate. It is easy to check that $(\cdot, \cdot)$ is an inner product and V forms a unitary space with this inner product. For every $a \in \mathbb{F}_q$, let f_a denote the function

$$f_a : \mathbb{F}_q \to \mathbb{C}; \quad f_a(a) = 1, \quad f_a(b) = 0 \quad \text{for all } b \ne a.$$

It is obvious that $\{f_a \mid a \in \mathbb{F}_q\}$ forms a basis of V. Thus, $\dim_{\mathbb{C}}(V) = q$.

Now consider the set of all normalised additive characters of $\mathbb{F}_q$ (here we use 'normalised' to denote divided by $\sqrt{q}$). By the orthogonal relation of characters, we know that this set forms an orthonormal basis of V. Thus every function in V is a $\mathbb{C}$-linear combination of the additive characters.

Similarly, if one takes $W = \mathbb{C}^{\mathbb{F}_q^*}$, then W is a $(q-1)$-dimensional vector space. In this case, the set of all normalised multiplicative characters of $\mathbb{F}_q$ forms an orthonormal basis of W.

In this section, we will show that some of the character sums considered here also contribute to orthogonal bases of V.

PROPOSITION 2.5. *For every element $h_1, h_2 \in L = \mathbb{F}_q$ with $q = p^m$,*

$$\sum_{x \in L} K_m(1, h_1 x) K_m(1, h_2 x) = \begin{cases} q^2 & \text{if } h_1 = h_2 \ne 0, \\ 0 & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

PROOF. If $h_1h_2 = 0$, the result is obvious. For $h_1h_2 \neq 0$, we compute

$$\begin{aligned}\sum_{x\in L} K_m(1,h_1x)K_m(1,h_2x) &= \sum_{x,y,z\in L} \chi(h_1xy + h_2xz + y^{-1} + z^{-1}) \\ &= \sum_{y,z\in L} \chi(y^{-1}+z^{-1}) \sum_{x\in L} \chi(x(h_1y + h_2z)) \\ &= q\sum_{z\in L} \chi(z^{-1}(1+(h_2/h_1)^{-1})) \\ &= \begin{cases} q^2 & \text{if } h_1 = h_2, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

□

The Kloosterman sum is a bridge linking $C_m^{(k)}(1,a)$ and $G_m^{(k)}(1,a)$.

PROPOSITION 2.6. *Set $L = \mathbb{F}_q$ with $q = 2^m$. For any positive integer k,*

$$G_m^{(k)}(1,a) = \frac{1}{q}\sum_{x\in L} K_m(x)C_m^{(k)}(1,xa^{-1}) \quad \textit{for all } a \in L^*, \tag{2.1}$$

$$C_m^{(k)}(1,a) = \frac{1}{q}\sum_{x\in L} K_m(x)G_m^{(k)}(1,xa^{-1}) \quad \textit{for all } a \in L^*. \tag{2.2}$$

PROOF. Observe that

$$\begin{aligned}\sum_{x\in L} K_m(x)C_m^{(k)}(1,xa^{-1}) &= \sum_{x\in L}\sum_{y\in L} \chi(y+xy^{-1}) \sum_{z\in L} \chi(z^{2^k+1} + a^{-1}xz) \\ &= \sum_{y\in L}\sum_{z\in L} \chi(z^{2^k+1}+y) \sum_{x\in L} \chi(x(y^{-1}+a^{-1}z)) \\ &= q\sum_{z\in L} \chi(z^{2^k+1} + az^{-1}) = qG_m^{(k)}(1,a).\end{aligned}$$

This proves (2.1), and (2.2) follows from the orthogonality relations. □

In the sequel, we tacitly assume that the elements of $\mathbb{F}_q$ are listed in some fixed order and this order will be used whenever an object indexed by elements of $\mathbb{F}_q$ appears. For every $a \neq 0$, denote the vector $q^{-1}(K_m(ax))_{x\in\mathbb{F}_q}$ by $\vec{K}_a$. Denote the vector $q^{-1/2}(1,1,\dots,1)$ by $\vec{\mathbb{I}}$. Proposition 2.5 shows that $\{\vec{K}_a |\ a \in \mathbb{F}_{p^m}^*\} \cup \{\vec{\mathbb{I}}\}$ contributes to an orthonormal basis of V. So, when $q = 2^m$, we have

$$G_m^{(k)}(1,a) = \sum_{x\in L} (G_m^{(k)}(1,a), q^{-1}K_m(ax))q^{-1}K_m(ax) = \frac{1}{q^2}\sum_{x\in L} (G_m^{(k)}(1,a), K_m(x))K_m(x).$$

Thus Proposition 2.6 may be rewritten as

$$C_m^{(k)}(1,xa^{-1}) = (G_m^{(k)}(1,a), q^{-1}K_m(x)), \quad G_m^{(k)}(1,xa^{-1}) = (C_m^{(k)}(1,a), q^{-1}K_m(x)).$$

Note that here one uses

$$(K_m(1,a), \vec{\mathbb{I}}) = (C_m^{(k)}(1,a), \vec{\mathbb{I}}) = (G_m^{(k)}(1,a), \vec{\mathbb{I}}) = 0.$$

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

PROPOSITION 2.7. *Let k be an integer and m an odd integer with* $\gcd(k,m)=1$. *For* $h_1, h_2 \in \mathbb{F}_{2^m}$,

$$\sum_{x\in L} C_m^{(k)}(1,h_1x)C_m^{(k)}(1,h_2x) = \begin{cases} q^2 & \text{if } h_1 = h_2, \\ 0 & \text{otherwise}, \end{cases}$$

$$\sum_{x\in L} G_m^{(k)}(1,h_1x)G_m^{(k)}(1,h_2x) = \begin{cases} q^2 & \text{if } h_1 = h_2, \\ 0 & \text{otherwise}. \end{cases}$$

The proof of this proposition is similar to that of Proposition 2.6.

For $a \neq 0$, denote by $\vec{G}_a$ and $\vec{C}_a$ the vectors $q^{-1}(G_m^{(k)}(ax))_{x\in\mathbb{F}_q}$ and $q^{-1}(C_m^{(k)}(ax))_{x\in\mathbb{F}_q}$, respectively. By Proposition 2.7, $\{\vec{G}_a \mid a \in \mathbb{F}_{2^m}\} \cup \{\vec{\mathbb{I}}\}$ and $\{\vec{C}_a \mid a \in \mathbb{F}_{2^m}\} \cup \{\vec{\mathbb{I}}\}$ are orthogonal bases of V. Using these orthogonal relations, we have the following proposition whose proof is similar to that of propositions above.

PROPOSITION 2.8. *For k an integer, m an odd integer with* $\gcd(k,m)=1$ *and* $a \in \mathbb{F}_{2^m}^*$,

$$C_m^{(k)}(1,a) = \frac{1}{q}\sum_{x\in\mathbb{F}_{2^m}} G_m^{(k)}(1,a^{-1}x)K_m(x),$$

$$K_m(a) = \frac{1}{q}\sum_{x\in\mathbb{F}_{2^m}} G_m^{(k)}(1,x)C_m^{(k)}(a,x).$$

3. The constructions

In this section let $\mathbb{F}_q$ be a finite field of order $q = p^m$ and characteristic p. We give several constructions of AMUBs of $\mathbb{C}^q$. The first construction is over any finite field.

THEOREM 3.1 (Construction A). *Suppose that n is a positive integer with* $\gcd(n,p)=1$ *and $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of degree n over $\mathbb{F}_q$. Denote by $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q\}$ the set of vectors given by*

$$v_{a,b} = \frac{\theta(a)}{\sqrt{q}}(\chi(ax+bf(x)))_{x\in\mathbb{F}_q},$$

where θ is a map from $\mathbb{F}_q$ to $\mathbb{C}$ such that $|\theta(a)|=1$ for all $a \in \mathbb{F}_q$. Then the standard basis and the sets B_a, with $a \in \mathbb{F}_q$, form an AMUB of $\mathbb{C}^q$.

REMARK 3.2. The polynomial f is a permutation polynomial if $f : a \longmapsto f(a)$ for $a \in \mathbb{F}_q$ is a permutation. An example is the Dickson polynomial

$$D_n(x) = \sum_{k=0}^{\lfloor n/2\rfloor} \frac{n}{n-k}\binom{n-k}{k}x^{n-2k}$$

with $\gcd(n, q^2-1)=1$ (see [14]).

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

Proof. By definition, for $a, a', b, b' \in \mathbb{F}_q$,

$$\langle v_{a,b} \mid v_{a',b'} \rangle = \frac{\theta(a)\overline{\theta(a')}}{q} \sum_{x \in \mathbb{F}_q} \chi((a-a')x + (b-b')f(x)).$$

If $a = a'$, then $\langle v_{a,b} \mid v_{a',b'} \rangle = \delta_{b,b'}$. Here δ is the delta function: $\delta_{b,b'} = 1$ if $b = b'$ and 0 otherwise. Thus B_a is an orthonormal basis for each $a \in \mathbb{F}_q$. For every vector e_c in the standard basis,

$$|\langle v_{a,b} \mid e_c \rangle| = \frac{1}{\sqrt{q}} |\chi(ac + bf(c))| = \frac{1}{\sqrt{q}}.$$

Finally, if $a \neq a'$, by Weil's bound [14, Theorem 5.38],

$$|\langle v_{a,b} \mid v_{a',b'} \rangle| = \frac{1}{q} \left| \sum_{x \in \mathbb{F}_q} \chi((a-a')x + (b-b')f(x)) \right| \leq \frac{n-1}{\sqrt{q}}. \qquad \square$$

In this construction, n is fixed and independent of q. In the case of the Dickson polynomial $D_n(x)$, the coefficients also do not depend on q. On the other hand, consider $f(x) = x^{q-2}$ which is trivially a permutation polynomial over $\mathbb{F}_q$. Applying Weil's bound in the last step in the proof gives a bound of $(q-3)/\sqrt{q}$. However, if we write $f(x) = x^{-1}$, with the convention $0^{-1} = 0$, then

$$v_{a,b} = \frac{\theta(a)}{\sqrt{q}} (\chi(ax + bx^{-1}))_{x \in \mathbb{F}_q},$$

where $|\theta(a)| = 1$ for all $a \in \mathbb{F}_q$. The standard basis and the sets $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q\}$, with $a \in \mathbb{F}_q$, form an AMUB of $\mathbb{C}^q$. Indeed, by Proposition 2.5, when $a \neq a'$,

$$|\langle v_{a,b} \mid v_{a',b'} \rangle| = \frac{1}{q} \left| \sum_{x \in \mathbb{F}_q} \chi((a+a')x + (b+b')x^{-1}) \right| = \frac{1}{q} |K_m((a+a')(b+b'))| \leq \frac{2}{\sqrt{q}}.$$

In the following constructions, we consider $p = 2$ and $q = 2^m$.

Theorem 3.3 (Construction B). *Suppose that $q = 2^m$ where m is an odd positive integer and k is a positive integer relatively prime to m. Set $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q\}$, where*

$$v_{a,b} = \frac{1}{\sqrt{q}} (\chi(ax + bx^{2^k+1}))_{x \in \mathbb{F}_q}.$$

Then the standard basis and the sets B_a, with $a \in \mathbb{F}_q$, form an AMUB of $\mathbb{C}^q$.

Proof. By definition, for $a, a', b, b' \in \mathbb{F}_q$,

$$\langle v_{a,b} \mid v_{a',b'} \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi((a-a')x) \chi((b-b')x^{2^k+1}).$$

Suppose that $a = a'$. Since $\gcd(2^k+1, 2^m-1) = 1$, we have $\langle v_{a,b} \mid v_{a',b'} \rangle = \delta_{b,b'}$. Thus B_a is an orthogonal basis for each $a \in \mathbb{F}_q$. Moreover,

$$\langle v_{a,b} \mid e_c \rangle = \frac{1}{\sqrt{q}} |\chi(ac + bc^{2^k+1})| = \frac{1}{\sqrt{q}}.$$

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

On the other hand, if $a \neq a'$,

$$\langle v_{a,b} \mid v_{a',b'} \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi((a-a')x)\chi((b-b')x^{2^k+1}) = \frac{1}{q} C_m^{(k)}(a-a', b-b').$$

By Lemma 2.4, $|C_m^{(k)}(a,b)| \leq \sqrt{2q}$ for all $a, b \in \mathbb{F}_q$ and the desired result follows. □

THEOREM 3.4 (Construction C). *Suppose that $q = 2^m$ where $m > 1$ is an integer. Set $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q^*\} \cup \{\lambda_a\}$, where $v_{a,b}$ and λ_a are given by*

$$v_{a,b} = \frac{1}{q}(\chi(ax)K_m(1,bx))_{x \in \mathbb{F}_q}, \quad \lambda_a = \frac{1}{\sqrt{q}}(\chi(ax))_{x \in \mathbb{F}_q}.$$

Then the standard basis and the sets B_a, with $a \in \mathbb{F}_q$, form an AMUB of $\mathbb{C}^q$.

PROOF. For $a, a' \in \mathbb{F}_q, b, b' \in \mathbb{F}_q^*$,

$$\langle v_{a,b} \mid v_{a',b'} \rangle = \frac{1}{q^2} \sum_{x \in \mathbb{F}_q} \chi((a-a')x)K_m(1,bx)K_m(1,b'x).$$

Suppose first that $a = a'$. By Proposition 2.5, we have $\langle v_{a,b} \mid v_{a',b'} \rangle = \delta_{b,b'}$. Moreover,

$$\langle v_{a,b} \mid \lambda_a \rangle = \frac{1}{q^{3/2}} \sum_{x \in \mathbb{F}_q} K_m(1,bx) = 0 \quad \text{and} \quad \langle \lambda_a \mid \lambda_a \rangle = 1.$$

Thus B_a is an orthonormal basis for each $a \in \mathbb{F}_q$. On the other hand, if $a \neq a'$, then

$$\langle \lambda_a \mid \lambda_a' \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \chi((a-a')x) = 0,$$

and

$$\begin{aligned}\langle v_{a,b} \mid v_{a',b'} \rangle &= \frac{1}{q^2} \sum_{x \in \mathbb{F}_q} \chi((a-a')x)K_m(1,bx)K_m(1,b'x) \\ &= \frac{1}{q^2} \sum_{y,z \in \mathbb{F}_q} \chi(y^{-1}+z^{-1}) \sum_{x \in \mathbb{F}_q} \chi(((a-a')+by+b'z)x) \\ &= \frac{1}{q} \sum_{y \in \mathbb{F}_q} \chi\left(\frac{a_1+b_1y}{y^2+a_1y}\right),\end{aligned}$$

where $a_1 = (a-a')/b, b_1 = (b-b')/b$. By [16, Theorem 2],

$$\left| \sum_{y \in \mathbb{F}_q} \chi\left(\frac{a_1+b_1y}{y^2+a_1y}\right) \right| \leq 4\sqrt{q}.$$

Thus we have $|\langle v_{a,b} \mid v_{a',b'} \rangle| \leq 4/\sqrt{q}$. Further,

$$\langle v_{a,b} \mid \lambda_{a'} \rangle = \frac{1}{q^{3/2}} \sum_{y \in \mathbb{F}_q} \chi(y^{-1}) \sum_{x \in \mathbb{F}_q} \chi((by+a-a')x) = \frac{1}{\sqrt{q}} \chi(b/(a-a')),$$

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

and it follows that $|\langle v_{a,b} \mid \lambda_{a'}\rangle| = 1/\sqrt{q}$. Finally, it is obvious that

$$|\langle v_{a,b} \mid e_c\rangle| = \frac{1}{q}|K_m(1,bc)| \le \frac{2}{\sqrt{q}} \quad \text{and} \quad |\langle \lambda_a \mid e_c\rangle| = \frac{1}{\sqrt{q}}.$$

The desired result now follows. □

Using the same method, we can also obtain the following Construction D.

THEOREM 3.5 (Construction D). *Suppose that $q = 2^m$ where m is an odd positive integer and k is an integer satisfying $\gcd(m,k) = 1$. Set $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q^*\} \cup \lambda_a$, where*

$$v_{a,b} = \frac{1}{q}(\chi(ax)C_m^{(k)}(1,bx))_{x\in\mathbb{F}_q}.$$

Then the standard basis and the sets B_a, with $a \in \mathbb{F}_q$, form an AMUB of $\mathbb{C}^q$.

A bound for the character sum $G_m^{(k)}(a,b)$ is given in [21]:

$$|G_m^{(k)}(a,b)| \le (2^k + 2)\sqrt{q},$$

If $\gcd(m,k) = 1$, Johansen *et al.* [8] conjectured that

$$|G_m^{(k)}(a,b)| \le 4\sqrt{q}. \tag{3.1}$$

Thus if k is relatively small or (3.1) is true, we also have the following construction.

THEOREM 3.6 (Construction E). *Suppose that $q = 2^m$ where m is an odd positive integer and k is an integer satisfying $\gcd(m,k) = 1$. Set $B_a = \{v_{a,b} \mid b \in \mathbb{F}_q^*\} \cup \lambda_a$, where*

$$v_{a,b} = \frac{1}{q}(\chi(ax)G_m^{(k)}(1,bx))_{x\in\mathbb{F}_q}.$$

Then the standard basis and the sets B_a, with $a \in \mathbb{F}_q$, form an AMUB of $\mathbb{C}^q$.

Our last construction is based on Gaussian sums. We show that some character sums are orthogonal over a subset of a finite field, and then we use this orthogonality to construct AMUBs.

THEOREM 3.7 (Construction F). *Let $q = 2^m$. For $a \in \mathbb{F}_{q^2}^*$, denote*

$$E_a = \{\alpha \in \mathbb{F}_{q^2} : \mathrm{Tr}_m^{2m}(\alpha) = a\}.$$

Let I be a subset of $\mathbb{F}_q^*$ with cardinality $|I| = s \ge 1$ and define the set $D = \bigcup_{a\in I} E_a$ (so that $|D| = qs$). Write $D = \{x_1,\dots,x_{qs}\}$ and for $\chi \in (\mathbb{F}_{q^2}^*)^\wedge$, the group of multiplicative characters of $\mathbb{F}_{q^2}$, define the complex vectors of dimension n:

$$u_\chi = \frac{1}{\sqrt{\ell}}(\chi(x_1),\dots,\chi(x_{qs}),w) \in \mathbb{C}^n, \tag{3.2}$$

where $n = qs+1$, $\ell = qs+s$ and $w \in \mathbb{C}$ satisfies $|w|^2 = s$. Let ψ be a generator of $(\mathbb{F}_{q^2}^*)^\wedge$, let $u_{i,l}$ be the vector corresponding to the character $\psi^{i+l(q-1)}$ in (3.2), for $0 \le i \le q$ and $0 \le l \le q-1$, and set $B_i = \{u_{i,l} : l = 0,1,\dots,q\}$. Then $B_0,\dots,B_q$ and the standard basis form an AMUB of $\mathbb{C}^q$.

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

PROOF. If u_χ and $u_{\chi'}$ are both in B_i, then $\chi = \psi^{i+l(q-1)}$, $\chi' = \psi^{i+l'(q-1)}$. Thus

$$\langle u_\chi \mid u_{\chi'} \rangle = \frac{1}{\ell}\Big(|w|^2 + \sum_{x\in D} \bar{\chi}\chi'(x)\Big) = \frac{1}{\ell}\Big(s + \sum_{x\in D} \lambda(x)\Big) \tag{3.3}$$

where $\lambda = \bar{\chi}\chi' = \psi^{(l-l')(q-1)}$ which is not the principal character. For every $y \in \mathbb{F}_q^*$, one has $\lambda(y) = \psi^{l-l'}(y^{q-1}) = 1$. Now, we compute

$$\begin{aligned}
\sum_{x\in D} \lambda(x) &= \sum_{a\in I} \sum_{x\in E_a} \lambda(x) \\
&= \frac{1}{q} \sum_{a\in I} \sum_{x\in \mathbb{F}_{q^2}^*} \lambda(x) \sum_{y\in\mathbb{F}_q} (-1)^{\mathrm{Tr}_1^m(y(\mathrm{Tr}_m^{2m}(x)-a))} \\
&= \frac{1}{q} \sum_{a\in I} \sum_{x\in \mathbb{F}_{q^2}^*} \lambda(x) \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^m(y(\mathrm{Tr}_m^{2m}(x)-a))} + \frac{1}{q} \sum_{a\in I} \sum_{x\in \mathbb{F}_{q^2}^*} \lambda(x) \\
&= \frac{1}{q} \sum_{a\in I} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^m(ay)} \overline{\lambda}(y) \sum_{x\in\mathbb{F}_{q^2}^*} (-1)^{\mathrm{Tr}_1^{2m}(xy)} \lambda(xy) \\
&= \frac{1}{q} G_{q^2}(\lambda) \sum_{a\in I} \sum_{y\in\mathbb{F}_q^*} (-1)^{\mathrm{Tr}_1^m(ay)} = -\frac{1}{q} G_{q^2}(\lambda) s,
\end{aligned}$$

where $G_{q^2}(\lambda) = \sum_{x\in\mathbb{F}_{q^2}^*} (-1)^{\mathrm{Tr}_1^{2m}(x)} \lambda(x)$ is the Gaussian sum. Since the order of λ divides $q+1$, by Stickelberger's theorem (see, for example, [14, Theorem 5.16]), we know that $G_{q^2}(\lambda) = q$, and thus by (3.3), $\langle u_\chi \mid u_{\chi'} \rangle = 0$. Thus each B_i forms an orthonormal basis of $\mathbb{C}^n$. Moreover, it is easy to see that

$$|\langle u_\chi \mid e_j \rangle|^2 = \begin{cases} 1/\ell & \text{if } 1 \le j \le qs, \\ s/(q+1) & \text{if } j = qs+1. \end{cases}$$

Obviously, $|\langle u_\chi \mid e_i \rangle|^2 = O(1/n)$ as $q \to \infty$.

For $u_\chi \in B_i, u_{\chi'} \in B_{i'}, i \neq i'$,

$$\langle u_\chi \mid u_{\chi'} \rangle = \frac{1}{\ell}\Big(s + \sum_{x\in D} \lambda(x)\Big)$$

where $\lambda = \overline{\chi}\chi'$ is not the principal character. A calculation similar to that above shows that

$$\langle u_\chi \mid u_{\chi'} \rangle = \frac{1}{\ell}\Big(s - \frac{1}{q} G_{q^2}(\lambda)\overline{G_q(\lambda)}\Big),$$

where $G_q(\lambda)$ is a Gaussian sum over $\mathbb{F}_q$. By [14, Theorem 5.11],

$$|\langle u_\chi \mid u_{\chi'} \rangle|^2 \le \frac{1}{n^2}(s + \sqrt{q})^2 = O\Big(\frac{1}{n}\Big) \quad \text{as } q \to \infty.$$

Therefore, $B_0, \ldots, B_q$ and the standard basis form an AMUB. □

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press

Remark 3.8.

(1) If we take w as $(1, 1, \ldots, 1)$ of dimension s instead of the number w in Construction F, then we can similarly show that the bases $B_0, \ldots, B_q$ and the standard basis form an AMUB.

(2) If we take $s = 1$, then the above construction is just that of [23, Theorem 3].

Acknowledgement

Part of this work was done while the first author was visiting the Institute of Mathematics, Academia Sinica, in September 2014.

References

[1] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury and F. Vatan, 'A new proof of the existence of mutually unbiased bases', *Algorithmica* **34** (2002), 512–528.
[2] J. Dillon and H. Dobbertin, 'New cyclic difference sets with Singer parameters', *Finite Fields Appl.* **10** (2004), 342–389.
[3] T. Durt, B. G. Englert, I. Bengtsson and K. Zyczkowski, 'On mutually unbiased bases', *Int. J. Quantum Inf.* **8** (2010), 535–640.
[4] C. Godsil and A. Roy, 'Equiangular lines, mutually unbiased bases and spin models', *European J. Combin.* **30** (2009), 246–262.
[5] J. Hall, 'Mutually unbiased bases and related structures', PhD Thesis, RMIT University, Melbourne, 2011.
[6] T. Helleseth, 'Some results about the cross-correlation function between two maximal linear sequences', *Discrete Math.* **16** (1976), 209–232.
[7] I. D. Ivanovic, 'Geometrical description of quantal state determination', *J. Phys.* A **14** (1981), 3241–3245.
[8] A. Johansen, T. Helleseth and A. Kholosha, 'Further results on m-sequences with five-valued cross correlation', *IEEE Trans. Inform. Theory* **55** (2009), 5792–5802.
[9] A. Klappenecker and M. Rötteler, 'Constructions of mutually unbiased bases', $\mathbb{F}_{q^r}$ *2003*, Lecture Notes in Computer Science, 2948 (eds. G. Mullen, A. Poli and H. Stichtenoth) (Springer, Berlin, 2003), 137–144.
[10] A. Klappenecker and M. Rötteler, 'Mutually unbiased bases are complex projective 2-designs', *Proc. 2005 IEEE Intl Symp. on Information Theory,* Adelaide, Australia (2005), 1740–1744.
[11] A. Klappenecker, M. Rötteler and I. E. Shparlinski, 'On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states', *J. Math. Phys.* **46** (2005), 082104.
[12] G. Lachaud and J. Wolfmann, 'The weights of the orthogonals of the extended quadratic binary Goppa codes', *IEEE Trans. Inform. Theory* **36** (1990), 686–692.
[13] J. Lahtonen, G. McGuire and H. W. Ward, 'Gold and Kasami-Welch functions, quadratic forms and bent functions', *Adv. Math. Commun.* **1** (2007), 243–250.
[14] R. Lidl and H. Niederriter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20 (Addison-Wesley, Reading, MA, 1983).
[15] P. Lisonêk, 'On the connection between Kloosterman sums and elliptic curves', *SETA 2008*, Lecture Notes in Computer Science, 5203 (eds. S. W. Golomb *et al.*) (Springer, Berlin, 2008), 182–187.
[16] C. J. Moreno and O. Moreno, 'Exponential sums and Goppa codes: I', *Proc. Amer. Math. Soc.* **111** (1991), 523–531.
[17] M. Planat and H. Rosu, 'Mutually unbiased bases, phase uncertainties and Gauss sums', *Eur. Phys. J.* D **36** (2005), 133–139.

[18] A. Rao, D. Donovan and J. L. Hall, 'Mutually orthogonal Latin squares and mutually unbiased bases in dimensions of odd prime power', *Cryptogr. Commun.* **2** (2010), 221–231.
[19] M. Saniga and M. Planat, 'Hjelmslev geometry of mutually unbiased bases', *J. Phys.* A **39** (2006), 435–440.
[20] J. Schwinger, 'Unitary operator bases', *Proc. Natl. Acad. Sci. USA* **46** (1960), 570–579.
[21] A. G. Shanbhag, P. V. Kumar and T. Helleseth, 'An upper bound for the extended Kloosterman sums over Galois rings', *Finite Fields Appl.* **4** (1998), 218–238.
[22] I. E. Shparlinski and A. Winterhof, *Construction of Approximately Mutually Unbiased Bases*, Lecture Notes in Computer Science, 3887 (Springer, Berlin, 2006), 793–799.
[23] W. Y. Wang, A. X. Zhang and K. Q. Feng, 'Constructions of approximately mutually unbiased bases and symmetric informationally complete positive operator-valued measures by Gauss and Jacobi sums', *Sci. Sin. Math.* **42** (2012), 971–984; (in Chinese).
[24] G. Xu, 'Compressed sensing matrices from Fourier matrices', *IEEE Trans. Inform. Theory* **61** (2014), 469–478.

XIWANG CAO, Department of Mathematics,
Nanjing University of Aeronautics and Astronautics,
Nanjing 210016, PR China
and
State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, PR China
e-mail: xwcao@nuaa.edu.cn

WUN-SENG CHOU, Institute of Mathematics,
Academia Sinica, Taiwan
and
Department of Mathematical Sciences,
National Chengchi University, Taipei, Taiwan
e-mail: macws@math.sinica.edu.tw

https://doi.org/10.1017/S0004972715000994 Published online by Cambridge University Press