IEICE TRANS. FUNDAMENTALS, VOL.E107–A, NO.8 AUGUST 2024

LETTER

New Constructions of Approximately Mutually Unbiased Bases by Character Sums over Galois Rings*

You GAO[†,††a)], **Ming-Yue XIE**[†b)], **Gang WANG**[†c)], ***Nonmembers***, ***and*** **Lin-Zhi SHEN**[†d)], ***Member***

SUMMARY Mutually unbiased bases (MUBs) are widely used in quantum information processing and play an important role in quantum cryptography, quantum state tomography and communications. It's difficult to construct MUBs and remains unknown whether complete MUBs exist for any non prime power. Therefore, researchers have proposed the solution to construct approximately mutually unbiased bases (AMUBs) by weakening the inner product conditions. This paper constructs q AMUBs of $\mathbb{C}^q$, $(q+1)$ AMUBs of $\mathbb{C}^{q-1}$ and q AMUBs of $\mathbb{C}^{q-1}$ by using character sums over Galois rings and finite fields, where q is a power of a prime. The first construction of q AMUBs of $\mathbb{C}^q$ is new which illustrates K AMUBs of $\mathbb{C}^K$ can be achieved. The second and third constructions in this paper include the partial results about AMUBs constructed by W. Wang et al. in [9].

key words: *quantum information process, AMUBs, Gauss sums, Jacobi sums, Galois rings, finite fields*

1. Introduction

Mutually unbiased bases (MUBs) are widely used in quantum information processing and play an important role in quantum cryptography, quantum state tomography and communications. In [1], by using the unbiased measurements, the errors can be reduced in the study of quantum state tomography. W. Wootters et al. [2] show that the complete MUBs can provide the optimal set of measurements. The security of password transmission can be enhanced through applying the unbiased measurements into quantum systems [3]. In order to prove the SPR conjecture put forward by M. Saniga, M. Planat and H. Rosu, mutually orthogonal Latin squares (MOLS) can be constructed by using some functions and algebraic structure of MUBs [3]. At the same time, the approximately symmetric informationally complete positive operator valued measures (ASIC-POVMs) can be obtained by constructing MUBs [4].

For any two vectors u and v of the K-dimensional complex inner product space $\mathbb{C}^K$, the Hermite inner product of vectors $u = (u^1, u^2, \ldots, u^K)^t$ and $v = (v^1, v^2, \ldots, v^K)^t$ is defined as $\langle u|v\rangle = \sum_{i=1}^{K} \overline{u^i} v^i \in \mathbb{C}$, where $\overline{u^i}$ is the complex conjugate of u^i.

The set $B = \{v_1, v_2, \ldots, v_K\}$ is called an orthonormal basis of $\mathbb{C}^K$, if $\langle v_i|v_j\rangle = \begin{cases} 1, & \text{for } 1 \le i = j \le K, \\ 0, & \text{for } 1 \le i \ne j \le K. \end{cases}$

Definition 1 ([5]) Let $\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$ be a set of orthonormal bases of $\mathbb{C}^K$ and $m \ge 2$. $\mathcal{B}$ is called mutually unbiased bases (MUBs) if for any $v_i \in B_i$ and $v_j \in B_j$ $(1 \le i \ne j \le m)$, $\left|\langle v_i|v_j\rangle\right|^2 = \frac{1}{K}$.

$\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$ on $\mathbb{C}^K$ with size $|\mathcal{B}| = m$. If $f(K)$ is the maximal value of m, then $f(K) \le K+1$. A maximum of $(K+1)$ MUBs on $\mathbb{C}^K$ is called complete MUBs, where K is a prime power. The complete MUBs can be obtained by planar functions construction, WF construction, Alltop construction, Pauli matrix construction and Galois ring construction [1], [6]. There are at least $(L(K)+2)$ MUBs on $\mathbb{C}^{K^2}$ ([7], [8]), where $L(K)$ is the maximum number of orthogonal latin squares of order $K \ge 2$.

The condition that K is a prime power is still somewhat too strict for quantum computation. It is unknown if the maximum number of MUBs is attained for any non prime power. At the same time, the researchers suppose there is no complete MUBs on $\mathbb{C}^K$ for K not being a power of prime. It is necessary to study the approximately mutually unbiased bases (AMUBs) by considering the vector systems which is approximately mutually unbiased ([4], [9]) such as $|\langle v_i|v_j\rangle| = O(\frac{1}{\sqrt[4]{K}}), |\langle v_i|v_j\rangle| \le \frac{1}{\sqrt{K}}(2+o(1)), |\langle v_i|v_j\rangle| \le \frac{1}{\sqrt{K}}(1+o(1)), |\langle v_i|v_j\rangle| = O(\frac{1}{\sqrt{K}}), |\langle v_i|v_j\rangle| = O(\frac{1}{\sqrt{K}}\log K)$, where $1 \le i \ne j \le m$.

We choose the definition as follows.

Definition 2 ([4]) The set $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$, where for $1 \le i \le m$, B_i is an orthonormal basis of $\mathbb{C}^K$, is called approximately mutually unbiased bases (AMUBs) if $\left|\langle v_i|v_j\rangle\right|^2 \le \frac{1}{K}(1+o(1))$ holds for all $v_i \in B_i$, $v_j \in B_j$ and $1 \le i \ne j \le m$.

We know AMUBs exist on $\mathbb{C}^K$ for a prime power K. Moreover, if we are slightly more liberal about the constraints, AMUBs exist in any dimension [4]. A. Klappenecker et al. [4] constructed $(K+1)$ AMUBs on $\mathbb{C}^K$, where

Manuscript received September 11, 2023.
Manuscript revised December 14, 2023.
Manuscript publicized February 7, 2024.

[†]School of Sciences, Civil Aviation University of China, Tianjin, 300300, China.
[††]Tianjin Key Laboratory of Advanced Signal Processing, Civil Aviation University of China, Tianjin, 300300, China.

*This research is supported by the National Natural Science Foundation of China (Grant No. 12301670), the Scientific Research Project of Tianjin Education Commission (Grant No. 2022KJ075), the Fundamental Research Funds for the Central Universities of China (No. 3122023QD25) and the Open Foundation of Tianjin Key Laboratory of Advanced Signal Processing (Grant No. 230122011003).

a) E-mail: gao_you@263.net
b) E-mail: xmy199896@163.com
c) E-mail: gwang06080923@mail.nankai.edu.cn (Corresponding author)
d) E-mail: linzhishen@mail.nankai.edu.cn

DOI: 10.1587/transfun.2023EAL2083

$K = p-1$ and p is a prime. I. E. Shparlinski et al. [10] constructed $(K+1)$ AMUBs on $\mathbb{C}^K$. W. Wang et al. [9] constructed K AMUBs on $\mathbb{C}^{K-1}$, $(K+1)$ AMUBs on $\mathbb{C}^{K-1}$ and K AMUBs on $\mathbb{C}^{K+1}$ for a prime power K. J. Li et al. [11] constructed $(K+1)$ AMUBs on $\mathbb{C}^{K(K-1)}$, where K is a prime power. G. Wang et al. [12] constructed K AMUBs on $\mathbb{C}^{K-1}$ and $(K+1)$ AMUBs on $\mathbb{C}^{K-1}$ for a prime power K.

In [13], the performance of AMUBs sequences is similar to that of MUBs. At the same time, explicit descriptions on the Gauss sums and Jacobi sums over Galois ring $GR(p^2, r)$ were expressed in [14]. By using character sums over Galois rings in [14], we construct q AMUBs of $\mathbb{C}^q$, $(q+1)$ AMUBs of $\mathbb{C}^{q-1}$ and q AMUBs of $\mathbb{C}^{q-1}$, where q is a prime power. The first construction of q AMUBs of $\mathbb{C}^q$ is new which illustrates K AMUBs of $\mathbb{C}^K$ can be achieved. In the second construction, different $(K+2)$ AMUBs of $\mathbb{C}^K$ are gained for different values of i and t'. Moreover, Theorem 2 in [9] are obtained when $i = t' = 0$ in Theorem 2. Therefore, our construction is more general compared with [9]. In the third construction, different $(K+1)$ AMUBs of $\mathbb{C}^K$ are gained for different elements of $1+M$. Moreover, if selecting the special element 1 from $1+M$, Theorem 1 in [9] are obtained. Therefore, our construction indeed generalized the results in [9].

2. Preliminaries

In this section, some basic results about character sums over Galois ring $GR(p^2, r)$ are provided [14]–[17].

Let p be a prime, $\mathbb{F}_p$ be the finite field with p elements, $\mathbb{Z}_{p^2} = \mathbb{Z}/p^2\mathbb{Z}$, r be a positive integer and $q = p^r$. Let $h(x)$ be a basic primitive polynomial of degree r in $\mathbb{Z}_{p^2}[x]$, which means that, under the reduction modulo p:

$$\mathbb{Z}_{p^2}[x] \to \mathbb{F}_p[x] = \mathbb{Z}_p[x], \quad h(x) = \sum_{i=0}^{r} c_i x^i \mapsto \overline{h(x)} = \sum_{i=0}^{r} \overline{c_i} x^i,$$

where $\overline{c_i} \equiv c_i \pmod p$ and $\overline{h(x)}$ is a primitive polynomial in $\mathbb{F}_p[x]$ with degree r.

Suppose that ξ is a root of $h(x)$ in some extension ring of $\mathbb{Z}_{p^2}$, then $\overline{\xi}(= \xi \pmod p)$ is a root of $\overline{h(x)}$ in the algebraic closure of $\mathbb{F}_p$, and the order of both ξ and $\overline{\xi}$ are $q-1$. Let $T^* = \langle \xi \rangle$ be the cyclic group. Set $T = T^* \cup \{0\}$.

Fact 1 ([14]) The Galois ring $R = GR(p^2, r)$ is the extension ring of $\mathbb{Z}_{p^2}$, which is defined by

$$R = GR(p^2, r) = \mathbb{Z}_{p^2}[x]/h(x) = \mathbb{Z}_{p^2}[\xi].$$

Each element α in R can be uniquely expressed by $\alpha = a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1}$, $a_i \in \mathbb{Z}_{p^2}$, or $\alpha = a + bp$, $a, b \in T$. Moreover, α is a unit if and only if $a_0 \neq 0$ or $a \neq 0$.

Fact 2 ([14]) The Galois group $Gal(R/\mathbb{Z}_{p^2}) = \langle \sigma \rangle$ is a cyclic group of order r generated by σ, where r is a integer and σ is defined by $\sigma(a + bp) = a^p + pb^p$, $a, b \in T$. Then, the trace mappings are denoted:

$$\mathrm{Tr}_{R/\mathbb{Z}_{p^2}} : R \longrightarrow \mathbb{Z}_{p^2}, \ \mathrm{Tr}(\alpha) = \sum_{i=0}^{r-1} \sigma^i(\alpha), \ \alpha \in R.$$

Fact 3 ([14]) The kernel $M = (p) = pR = \{pb : b \in T\}$. The group of additive characters of $(R, +)$ is $\widehat{R} = \{\lambda_b : b \in R\}$, where $\lambda_b : R \to \langle \zeta_{p^2} \rangle$ is defined by $\lambda_b(x) = \zeta_{p^2}^{\mathrm{Tr}(bx)}$ and $\zeta_m = e^{\frac{2\pi\sqrt{-1}}{m}}$ for any positive integer m.

The group of multiplicative characters of R is denoted by $\widehat{R^*}$. $1 + M \cong \mathbb{F}_p = \overline{T}$ by φ given as follows:

$$\varphi : (1+M, \cdot) \simeq (\mathbb{F}_q, +), \ 1 + pb \mapsto \varphi(b) = \overline{b}, \ b \in T.$$

Remark that $\overline{T} = \mathbb{F}_q$. $\widehat{R^*} = \widehat{T^*} \times (\widehat{1+M})$, so each multiplicative character of R can be written uniquely as $\chi = \omega^i \varphi_b$, where $\omega^i \in \widehat{T^*}$ $(0 \le i \le q-2)$ and $\varphi_b \in (\widehat{1+M})$ $(b \in T)$ are defined by

$$\omega^i(1+M) = 1, \ \omega^i(\xi) = \zeta_{q-1}^i,$$

$$\varphi_b(T^*) = 1, \ \varphi_b(1+px) = \overline{\varphi}_{\overline{b}}(\overline{x}) = \zeta_p^{\overline{\mathrm{Tr}(\overline{b}\overline{x})}} \ (x \in T).$$

Remark that $\overline{\varphi}_{\overline{b}}$ is an additive character of $\mathbb{F}_q$.

Fact 4 ([14]) Let $M = \{pb : b \in T\}$ be the unique maximal ideal of R, then the unit group of R is $R^* = R \backslash M$.

Fact 5 ([16]) We have the quotient group $R^*/(1+M)$. Let $\widehat{R^*}$ be the multiplicative characters group of R^*. The annihilator of $1+M$ in $\widehat{R^*}$ is denoted by A, then the order of A is $|R^*/(1+M)| = q-1$.

A is a subgroup of $\widehat{R^*}$, that is, $A = \left\{\omega^0, \ldots, \omega^{q-2}\right\} = \widehat{T^*}$. The multiplicative characters group of $R^*/(1+M)$ is denoted by $\widehat{R^*/(1+M)}$, therefore $\chi(s(1+M)) = \mu(s)$, $s \in T^*$ for any $\chi \in \widehat{R^*/(1+M)}$ and $\mu \in A$.

Let χ and λ be a multiplicative character and an additive character of R, respectively. The Gauss sum for χ and λ over R is defined by $G(\chi, \lambda) = \sum_{x \in R^*} \chi(x)\lambda(x) \in \mathbb{Z}\left[\zeta_{(q-1)p^2}\right]$.

Lemma 1 ([16], [17]) If $p\mu \in M$ and $\chi = \omega^i\varphi_0$, where $\mu \in T$, $\omega^i \in \widehat{T^*}$ $(0 \le i \le q-2)$ and φ_0 is the trivial character of $1+M$, then $G(\omega^i\varphi_0, \lambda_{p\mu})$ is the Gauss sum $G(\omega^i, \lambda_\mu)$ over $\mathbb{F}_q$. The Gauss sum $G(\omega^i\varphi_0, \lambda_{p\mu})$ satisfies

$$G(\omega^i\varphi_0, \lambda_{p\mu}) = \begin{cases} q-1, & \text{if } \lambda_{p\mu} = 1 \text{ and } \omega^i\varphi_0 = 1, \\ 0, & \text{if } \lambda_{p\mu} = 1 \text{ and } \omega^i\varphi_0 \neq 1, \\ -1, & \text{if } \lambda_{p\mu} \neq 1 \text{ and } \omega^i\varphi_0 = 1. \end{cases}$$

If $\lambda_{p\mu} \neq 1$ and $\omega^i\varphi_0 \neq 1$, then $|G(\omega^i\varphi_0, \lambda_{p\mu})| = \sqrt{q}$.

Let $\chi_1 = \omega_1\varphi_{b_1}$ and $\chi_2 = \omega_2\varphi_{b_2}$ be multiplicative characters of R, then the Jacobi sum for χ_1 and χ_2 over R is defined by $J(\chi_1, \chi_2; \alpha) = \sum_{\substack{x,y \in R^* \\ x+y=\alpha}} \chi_1(x)\chi_2(y)$, $\alpha \in R \backslash \{0\}$.

Lemma 2 ([16], [17]) If $\chi_1 = \omega_1\varphi_0$ and $\chi_2 = \omega_2\varphi_0$, where $\omega_1, \omega_2 \in T^*$ and φ_0 is the trivial character of $1+M$, then $J(\omega_1\varphi_0, \omega_2\varphi_0)$ is the Jacobi sum $J(\omega_1, \omega_2)$ on $\mathbb{F}_q$. The Jacobi sum $J(\omega_1\varphi_0, \omega_2\varphi_0)$ satisfies

$$J(\omega_1\varphi_0, \omega_2\varphi_0) = \begin{cases} q-2, & \text{if } \omega_1\varphi_0 = 1 \text{ and } \omega_2\varphi_0 = 1, \\ 0, & \text{if } \omega_1\varphi_0 \neq 1, \omega_2\varphi_0 = 1 \text{ or } \\ & \omega_1\varphi_0 = 1, \omega_2\varphi_0 \neq 1, \\ -\omega_1(-1), & \text{if } \omega_1\varphi_0 \neq 1 \text{and} \omega_1\varphi_0 = \overline{\omega_2\varphi_0}. \end{cases}$$

If $\omega_1\varphi_0 \neq 1$, $\omega_2\varphi_0 \neq 1$ and $\omega_1\varphi_0\omega_2\varphi_0 \neq 1$, then $|J(\omega_1\varphi_0, \omega_2\varphi_0)| = \sqrt{q}$.

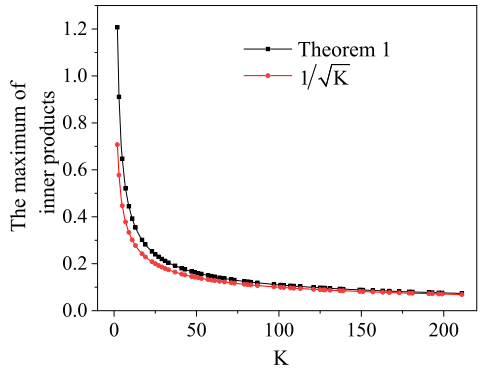

Fig. 1 The maximum of inner product of theorem 1 approaches closely to $\frac{1}{\sqrt{K}}$.

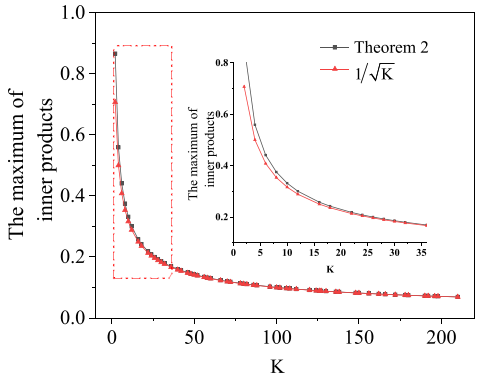

Fig. 2 The maximum of inner product of theorem 1 approaches closely to $\frac{1}{\sqrt{K}}$.

3. The Constructions of Approximately Mutually Unbiased Bases

In this section, three new constructions of approximately mutually unbiased bases are given.

Let $K = q$. $x_1, x_2, \ldots, x_{K-1}$ denote all of the elements of T^*, and B_* denotes the set formed by the K-dimensional vector $|e_i\rangle$ whose i-th component is 1, 0 in the other components and $1 \le i \le K$. For any multiplication character $\chi = \omega^i\varphi_c$ ($0 \le i \le K-2$, $c \in T$, c is fixed) and any addition character λ_b ($b \in M$), the vector of length K by

$$c_{\chi,b} = \frac{1}{\sqrt{K}}(\chi(x_1)\lambda_b(x_1), \cdots, \chi(x_{K-1})\lambda_b(x_{K-1}), 1). \quad (1)$$

Theorem 1 For any $\chi = \omega^i\varphi_c \in \widehat{R^*}$ ($0 \le i \le K-2$, $c \in T$, c is fixed), denote $B_\chi = \left\{c_{\chi,b} : b \in M\right\}$, where $c_{\chi,b}$ is defined by (1). Therefore,

$$\mathcal{B} = \left\{B_\chi : \chi = \omega^i\varphi_c, 0 \le i \le K-2, c \in T, c \text{ is fixed}\right\} \cup \{B_*\}$$

is an AMUBs of $\mathbb{C}^K$ and $|\mathcal{B}| = K$.

Proof For any $b' \in M$,

$$\left\langle c_{\chi,b'} | c_{\chi,b'} \right\rangle = \frac{1}{K}\left(\sum_{x\in T^*} \bar{\chi}(x)\bar{\lambda}_{b'}(x)\chi(x)\lambda_{b'}(x) + 1\right) = 1.$$

For any $b_1 \ne b_2 \in M$,

$$\left\langle c_{\chi,b_1} | c_{\chi,b_2} \right\rangle = \frac{1}{K}\left(\sum_{x\in T^*} \bar{\chi}(x)\bar{\lambda}_{b_1}(x)\chi(x)\lambda_{b_2}(x) + 1\right) = 0.$$

Therefore, B_χ is an orthonormal basis of $\mathbb{C}^K$.

For any $c_{\chi,b} \in B_\chi$, $e_i \in B_*$, $|\left\langle c_{\chi,b} | e_i \right\rangle| = \frac{1}{\sqrt{K}} \le \frac{1}{\sqrt{K}}(1 + o(1))$.

For any $c_{\chi,b} \in B_\chi$ and $c_{\chi',b'} \in B_{\chi'}$, denote $\chi = \omega^i\varphi_c$, $\chi' = \omega^j\varphi_c$ and $\bar{\lambda}_b\lambda_{b'} = \lambda_{b'-b} = \lambda_d$, by Lemma 1,

$$\begin{aligned}\left\langle c_{\chi,b} | c_{\chi',b'} \right\rangle &= \frac{1}{K}\left(\sum_{x\in T^*} \bar{\chi}(x)\bar{\lambda}_b(x)\chi'(x)\lambda_{b'}(x) + 1\right) \\ &= \frac{1}{K}\left(G\left(\omega^{j-i}, \lambda_u\right) + 1\right)\end{aligned}$$

and

$$|\left\langle c_{\chi,b} | c_{\chi',b'} \right\rangle| = \begin{cases} \frac{1}{K} \le \frac{1}{\sqrt{K}}(1 + o(1)), & \text{if } \lambda_u = 1, \\ \le \frac{\sqrt{K}+1}{K} \le \frac{1}{\sqrt{K}}(1 + o(1)), & \text{if } \lambda_u \ne 1. \end{cases}$$

Thus, $\mathcal{B}$ is an AMUBs of $\mathbb{C}^K$.

Remark 1 Let $f(K)$ be the maximal value of m such that there exist an MUB $\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$ on $\mathbb{C}^K$ with size $|\mathcal{B}| = m$. Then $f(K) = K+1$ or $f(K) \le K-1$ for all $K \ge 2$ (see [9]). Thus Theorem 1 illustrates K AMUBs of $\mathbb{C}^K$ can be achieved. Moreover, the maximum of inner product of Theorem 1 approaches closely to $\frac{1}{\sqrt{K}}$ is shown in Fig. 1.

Let $K = q - 1$. $x_1, x_2, \ldots, x_K$ denote all of the elements of T^*, and B_* denotes the set formed by the K-dimensional vector $|e_i\rangle$ whose ith component is 1, 0 in the other components and $1 \le i \le K$. For any multiplication character $\chi = \omega^i\varphi_t$ and $\chi' = \omega^j\varphi_{t'}$, where $t, t' \in T$, $0 \le i, j \le K-1$ and i, t' are fixed, define the vector of length K by

$$c_{\chi,\chi'} = \frac{1}{\sqrt{K}}(\chi(p - x_1)\chi'(x_1), \cdots, \chi(p - x_K)\chi'(x_K)). \quad (2)$$

Theorem 2 For any $\chi = \omega^i\varphi_t \in \widehat{R^*}$ ($t \in T$, $0 \le i \le K-1$, i is fixed), denote

$$B_\chi = \left\{c_{\chi,\chi'} : \chi' = \omega^j\varphi_{t'}, 0 \le j \le K-1, t' \in T, t' \text{ is fixed}\right\},$$

where $c_{\chi,\chi'}$ is defined by (2). Therefore,

$$\mathcal{B} = \left\{B_\chi : \chi = \omega^i\varphi_t, t \in T, 0 \le i \le K-1, i \text{ is fixed}\right\} \cup \{B_*\}$$

is an AMUBs of $\mathbb{C}^K$ and $|\mathcal{B}| = K + 2$.

Proof For any $\chi' = \omega^j\varphi_{t'} \in \widehat{R^*}$ ($0 \le j \le K-1$, $t' \in T$, t' is fixed),

$$\left\langle c_{\chi,\chi'} | c_{\chi,\chi'} \right\rangle = \frac{1}{K}\left(\sum_{x\in T^*} \bar{\chi}(p - x)\bar{\chi}'(x)\chi(p - x)\chi'(x)\right) = 1.$$

For any $\chi_1 = \omega^j\varphi_{t'} \in \widehat{R^*}$ and $\chi_2 = \omega^k\varphi_{t'} \in \widehat{R^*}$, where $0 \le j \ne k \le K-1$, $t' \in T$ and t' is fixed,

$$\left\langle c_{\chi,\chi_1} | c_{\chi,\chi_2} \right\rangle = \frac{1}{K}\left(\sum_{x\in T^*} \bar{\chi}(p-x)\bar{\chi}_1(x)\chi(p-x)\chi_2(x)\right) = 0.$$

Therefore, B_χ is an orthonormal basis of $\mathbb{C}^K$.

For any $c_{\chi,\chi_1}\in B_\chi$, $e_l\in B_*$, $|\left\langle c_{\chi,\chi_1}|e_l\right\rangle|=\frac{1}{\sqrt{K}}\le\frac{1}{\sqrt{K}}(1+o(1))$.

For any $c_{\chi,\chi_1}\in B_\chi$ and $c_{\chi',\chi_2}\in B_{\chi'}$, denote $\chi=\omega^i\varphi_{t_i}$, $\chi'=\omega^i\varphi_{t_j}$, $\chi_1=\omega^j\varphi_{t'}$ and $\chi_2=\omega^k\varphi_{t'}$, by Lemma 1,

$$\begin{aligned}\left\langle c_{\chi,\chi_1}|c_{\chi',\chi_2}\right\rangle &= \frac{1}{K}\left(\sum_{x\in T^*}\bar{\chi}\chi'(p-x)\bar{\chi}_1\chi_2(x)\right)\\ &= \frac{1}{K}\left(\varphi_{t_j-t_i}(-1)\,G\left(\overline{\omega^{k-j}},\lambda_{t_i-t_j}\right)\right)\end{aligned}$$

and

$$\left|\left\langle c_{\chi,\chi_1}|c_{\chi',\chi_2}\right\rangle\right|=\begin{cases}\frac{1}{K}\le\frac{1}{\sqrt{K}}(1+o(1)), & \text{if } j=k,\\ \frac{\sqrt{K}+1}{K}\le\frac{1}{\sqrt{K}}(1+o(1)), & \text{if } j\neq k.\end{cases}$$

Thus, $\mathcal{B}$ is an AMUBs of $\mathbb{C}^K$.

Remark 2 Different $(K+2)$ AMUBs of $\mathbb{C}^K$ are gained for different values of i and t'. Moreover, Theorem 2 in [9] are obtained when $i=t'=0$ in Theorem 2. Therefore, our construction is more general compared with [9]. According to the known results, the size of any set containing pairwise MUBs of $\mathbb{C}^K$ cannot exceed $K+1$, where $K\ge 2$ [9]. Thus Theorem 2 illustrates $(K+2)$ AMUBs of $\mathbb{C}^K$ can be achieved. The maximum of inner product of Theorem 2 approaches closely to $\frac{1}{\sqrt{K}}$ is shown in Fig. 2. Moreover the maximum of inner product of Theorem 2 in [9], Theorem 3.5 in [12] and Theorem 2 approach to $\frac{1}{\sqrt{K}}$ as the same extent.

Let $K=q-1$. $x_1,x_2,\ldots,x_K$ denote all of the elements of the group $D\backslash\{1\}$, where $D=R^*/(1+M)$, and B_* denote the set formed by $|e_i\rangle$ whose i-th component is 1, 0 in the other components and $1\le i\le K$. The multiplicative characters group of $R^*/(1+M)$ is $\widehat{R^*/(1+M)}$. Denote A as the annihilator of $1+M$ in $\widehat{R^*}$, and by Fact 2.5, $\chi(t(1+M))=\mu(t)$, where $\chi\in\widehat{R^*/(1+M)}$, $\mu\in A$ and $t\in T^*$.

For any $\chi'\in\widehat{R^*/(1+M)}$, define the vector of length K by

$$c_{\chi,\chi'}=\frac{1}{\sqrt{K}}(\chi(1-x_1)\chi'(x_1),\cdots,\chi(1-x_{K-1})\chi'(x_{K-1}),1). \quad (3)$$

Theorem 3 For any $\chi\in\widehat{R^*/(1+M)}$, denote $B_\chi=\left\{c_{\chi,\chi'}:\chi'\in\widehat{R^*/(1+M)}\right\}$, where $c_{\chi,\chi'}$ is defined by (3). Therefore, $\mathcal{B}=\left\{B_\chi:\chi\in\widehat{R^*/(1+M)}\right\}\cup\{B_*\}$ is an AMUBs of $\mathbb{C}^K$ and $|\mathcal{B}|=K+1$.

Proof For any $\chi'\in\widehat{R^*/(1+M)}$,

$$\left\langle c_{\chi,\chi'}|c_{\chi,\chi'}\right\rangle=\frac{1}{K}\left(\sum_{x\in D\backslash\{1\}}\bar{\chi}(1-x)\bar{\chi}'(x)\chi(1-x)\chi'(x)+1\right)=1.$$

For any $\chi_1\neq\chi_2\in\widehat{R^*/(1+M)}$,

$$\left\langle c_{\chi,\chi_1}|c_{\chi,\chi_2}\right\rangle=\frac{1}{K}\left(\sum_{x\in D\backslash\{1\}}\bar{\chi}(1-x)\bar{\chi}_1(x)\chi(1-x)\chi_2(x)+1\right)=0.$$

Therefore, B_χ is an orthonormal basis of $\mathbb{C}^K$.

For any $c_{\chi,\chi'}\in B_\chi$ $e_i\in B_*$, $|\left\langle c_{\chi,\chi'}|e_i\right\rangle|=\frac{1}{\sqrt{K}}\le\frac{1}{\sqrt{K}}(1+o(1))$.

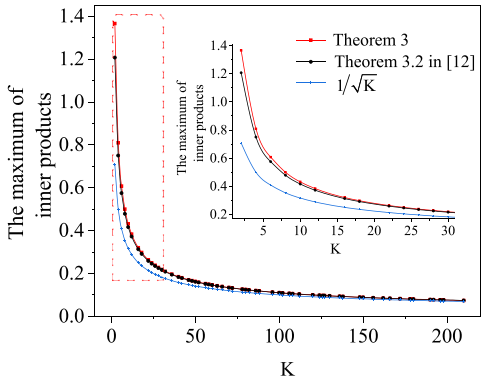

Fig. 3 The maximum of inner product of Theorem 3.2 in [12] and Theorem 3 approaches closely to $\frac{1}{\sqrt{K}}$.

For any $c_{\chi,\chi_1}\in B_\chi$, $c_{\chi',\chi_2}\in B_{\chi'}$, denote $\bar{\chi}\chi'((1-s)(1+M))=\bar{\mu}\mu'(1-s)$, $\bar{\chi}_1\chi_2((s)(1+M))=\bar{\mu}_1\mu_2(s)$, by Lemma 2,

$$\begin{aligned}\left\langle c_{\chi,\chi_1}|c_{\chi',\chi_2}\right\rangle &= \frac{1}{K}\left(\sum_{x\in D\backslash\{1\}}\bar{\chi}(1-x)\bar{\chi}_1(x)\chi'(1-x)\chi_2(x)+1\right)\\ &= \frac{1}{K}(J(\bar{\mu}\mu',\bar{\mu}_1\mu_2)+1)\end{aligned}$$

and

$$|\left\langle c_{\chi,\chi_1}|c_{\chi',\chi_2}\right\rangle|=\begin{cases}0\le\frac{1}{\sqrt{K}}(1+o(1)), & \text{if } \bar{\mu}\mu'\neq 1 \text{ and } \bar{\mu}_1\mu_2=1,\\ \frac{|-\bar{\mu}\mu'(-1)+1|}{K}\le\frac{1}{\sqrt{K}}(1+o(1)), & \text{if } \bar{\mu}\mu'\neq 1 \text{ and } \bar{\mu}\mu'=\overline{\bar{\mu}_1\mu_2},\\ \le\frac{\sqrt{K+1}+1}{K}\le\frac{1}{\sqrt{K}}(1+o(1)), & \text{if } \bar{\mu}\mu'\neq 1, \bar{\mu}_1\mu_2\neq 1 \text{ and } \bar{\mu}\mu'\neq\overline{\bar{\mu}_1\mu_2}.\end{cases}$$

Thus, $\mathcal{B}$ is an AMUBs of $\mathbb{C}^K$.

Remark 3 Different $(K+1)$ AMUBs of $\mathbb{C}^K$ are gained for different elements of $1+M$. Moreover, if selecting the special element 1 from $1+M$, Theorem 1 in [9] are obtained. Therefore, our construction is more general compared with [9]. According to the known results, the complete MUBs cannot exist on $\mathbb{C}^K$ for K is not a prime power [8]. Thus Theorem 3 illustrates $(K+1)$ AMUBs of $\mathbb{C}^K$ can be achieved. The maximum of inner product of Theorem 3, Theorem 1 in [9] and Theorem 3.2 in [12] approach closely to $\frac{1}{\sqrt{K}}$ in Fig. 3.

4. Conclusion

Let q be a prime power. In this paper, by using character sums over Galois rings and finite fields, q AMUBs of $\mathbb{C}^q$, $(q+1)$ AMUBs of $\mathbb{C}^{q-1}$ and q AMUBs of $\mathbb{C}^{q-1}$ are provided. In addition, the constructions in this paper contain the results about AMUBs obtained in [9].

References

[1] J. Hall, "Mutually unbiased bases and related structures," Ph.D. thesis, RMIT University, Australia, 2011.
[2] W. Wootters and B. Fields, "Optimal state-determination by mutually unbiased measurements," Ann. Phys., vol.191, no.2, pp.363–381, 1989.
[3] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Phys. Rev. Lett., vol.88, no.12, pp.127902-1–127902-4, 2002.
[4] A. Klappenecker, M. Rötteler, I.E. Shparlinski, and A. Winterhof, "On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states," J. Math. Phys., vol.46, no.8, pp.082104-1–082104-29, 2005.
[5] T. Durt, B. Englert, I. Bengtsson, and K. Zyczkowski, "On mutually unbiased bases," Int. J. Quantum Inf., vol.8, no.4, pp.535–640, 2010.
[6] A. Klappenecker and M. Rötteler, "Constructions of mutually unbiased bases," Finite Fields and Applications, LNCS, vol.2948, pp.137–144, 2004.
[7] P. Wocjan and T. Beth, "New construction of mutually unbiased bases in square dimensions," Quantum Inf. Comput., vol.5, no.2, pp.93–101, 2005.
[8] K. Feng and L. Jin, "Several mathematical problems in quantum information theory," Sci. Sin. Math., vol.47, no.11, pp.1387–1408, 2017.
[9] W. Wang, A. Zhang, and K. Feng, "Constructions of approximately mutually unbiased bases and symmetric informationally complete positive operator-valued measures by Gauss and Jacobi sums," Sci. Sin. Math., vol.42, no.10, pp.971–984, 2012 (in Chinese).
[10] I.E. Shparlinski and A. Winterhof, "Constructions of approximately mutually unbiased bases," LATIN 2006: Theoretical Informatics, LNCS, vol.3887, pp.793–799, 2006.
[11] J. Li and K. Feng, "Constructions on approximately mutually unbiased bases by Galois rings," J. Syst. Sci. Complex., vol.28, no.6, pp.1440–1448, 2015.
[12] G. Wang, M. Niu, and F. Fu, "Two new constructions of approximately mutually unbiased bases," Int. J. Quantum Inf., vol.16, no.4, pp.1850038-1–1850038-10, 2018.
[13] Y. Chen, "Sequence design based on MUB and research on application in wireless communication," master's thesis, Hangzhou Dianzi University, China, 2021 (in Chinese).
[14] J. Li, S. Zhu, and K. Feng, "The Gauss sums and Jacobi sums over Galois ring $GR(p^2, r)$," Sci. Sin. Math., vol.56, no.7, pp.1457–1465, 2013.
[15] Z. Wan, Lecture Notes on Finite Fields and Galois Rings, World Scientific, Singapore, 2003.
[16] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, U.K., 1996.
[17] B. Berndt, R. Evans, and K. Williams, Gauss and Jacobi Sums, Wiley, NewYork, U.S., 1998.