中国科学 : 数学　2012 年　第 42 卷　第 10 期 : 971 ~ 984
www.springerlink.com　math.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

利用 Gauss 和与 Jacobi 和构造近似 MUB 和 SIC-POVM

王威扬[①*], 张爱仙[①], 冯克勤[②]
① 首都师范大学数学科学学院, 北京 100048;
② 清华大学数学科学系, 北京 100084
E-mail: wangweiyang@pku.edu.cn, zhangaixian1008@126.com, kfeng@math.tsinghua.edu.cn

收稿日期: 2012-03-06; 接受日期: 2012-06-07; * 通信作者
国家自然科学基金 (批准号: 10990011) 资助项目

摘要　MUB (mutually unbiased bases) 和 SIC-POVM (symmetric informationally complete positive operator-valued measure) 是量子信息中的两个重要研究对象. 目前关于非素数幂维的完全 MUB 是否存在还没有确定的结果, 对于 SIC-POVM 目前只有有限多种维数 K 有存在性结果或数值结果. 于是很多弱化了内积条件的近似 MUB 和 SIC-POVM 被人们所考虑. 本文使用 Klappenecker 等人给出的近似 MUB 和 SIC-POVM 的定义, 利用 Gauss 和与 Jacobi 和对于素数方幂 q 给出了一类 $q-1$ 维 q-近似 MUB (AMUB)、一类 $q-1$ 维 $(q+1)$AMUB 以及 $q+1$ 维 qAMUB, 还利用 Gauss 和给出了一类 $q-1$ 维近似 SIC-POVM (ASIC-POVM) .

关键词　MUB　SIC-POVM　Gauss 和　Jacobi 和　球面上的 t 设计
MSC (2010) 主题分类　81P15

1　引言

MUB 和 SIC-POVM 在量子信息中有重要的意义, 在量子测量 [1–4]、量子密码 [5]、quantum state tomography [6] 等方面有所应用 (文献 [7] 中有更多应用).

从组合的角度来看, MUB 和 SIC-POVM 属于一类特殊的球面 2- 设计. 它们和复球面上的 t- 设计 [3,5,8,9]、复 Hadamard 矩阵 [7,8,10]、有限几何 [2]、相对差集 [3,10] 以及完美非线性映射 [3,10] 有密切的关系.

在量子物理中, 复向量空间中 $\mathbb{C}^K$ 中一个非零向量 $v=(v_1,v_2,\ldots,v_n)$ 记为 $|v\rangle$ (又称为一个量子态). $\mathbb{C}^K$ 中两个量子态 $|v\rangle$ 和 $|u\rangle$ 的 Hermite 内积定义为

$$\langle u|v\rangle=\sum_{i=1}^{K}\overline{u_i}v_i\in\mathbb{C},$$

其中 $\overline{u_i}$ 是 u_i 的复共轭.

称 $B=\{v_1,v_2,\ldots,v_K\}$ 为 $\mathbb{C}^K$ 中一组标准正交基是指

$$\langle v_i|v_j\rangle=\begin{cases}1, & \text{若 } 1\leqslant i=j\leqslant K,\\ 0, & \text{若 } 1\leqslant i\neq j\leqslant K.\end{cases}$$

英文引用格式: Wang W Y, Zhang A X, Feng K Q. Constructions of approximately mutually unbiased bases and symmetric informationally complete positive operator-valued measures by Gauss and Jacobi sums (in Chinese). Sci Sin Math, 2012, 42(10): 971–984, doi: 10.1360/012012-186

记 $\mathbb{C}S^{K-1}$ 为 $\mathbb{C}^K$ 中所有长度为 1 的向量组成的集合, 称其为复球面. 即

$$\mathbb{C}S^{K-1}=\{|v\rangle\in\mathbb{C}:\ \langle v|v\rangle=1\}.$$

1974 年 Welch 给出了下面的结果:

引理 1 (Welch 界 [11]) 令 C 是 $\mathbb{C}S^{K-1}$ 的一个有限子集, $N=|C|>K$. 则对于任意正整数 k,

$$\frac{1}{N^2}\sum_{u,v\in C}|\langle u|v\rangle|^{2k}\geqslant\left(\begin{array}{c}K+k-1\\k\end{array}\right)^{-1}. \tag{1.1}$$

定义 1 t 是一个正整数, C 是 $\mathbb{C}S^{K-1}$ 的一个子集. 如果 $|C|=N>K$ 并且 (1.1) 中的公式对于 $k=1,2,\ldots,t$ 等号均成立, 则称 C 为一个复球面 t- 设计或复射影 t- 设计.

定义 2 B_i $(1\leqslant i\leqslant m)$ 是 $\mathbb{C}^K$ 中的 m 组标准正交基. $\mathcal{B}=\{B_1,B_2,\ldots,B_m\}$ 称为 $\mathbb{C}^K$ 中的 MUB 是指, 对于任意 $v_i\in B_i$, $v_j\in B_j$ 和任意 $1\leqslant i\neq j\leqslant m$ 都有

$$|\langle v_i|v_j\rangle|=\frac{1}{\sqrt{K}}. \tag{1.2}$$

记 $f(K)$ 为 $\mathbb{C}^K$ 中的 MUB $\mathcal{B}=\{B_1,B_2,\ldots,B_m\}$ 包含的标准正交基的最多组数 (即最大的 m). 在 Welch 界公式中, 考虑 $C=\bigcup_{i=1}^m B_i$, $k=1$ 可知 $f(K)\leqslant K+1$. 如果 $f(K)=K+1$, $\mathbb{C}^K$ 中包含 $K+1$ 组标准正交基的 MUB $\mathcal{B}=\{B_1,B_2,\ldots,B_{K+1}\}$ 称为完全 MUB. 容易看出完全 MUB 是复球面 2- 设计.

关于 $f(K)$ 现在已有的结果如下:

(1) 当 K 为素数 p 的方幂 p^l 时, $f(p^l)=p^l+1$. [12–14] 利用有限域的加法特征 ($p\geqslant 3$) 和 Galois 环 ($p=2$) 构造出了完全 MUB, [7] 利用 Heisenberg-Weyl 群构造出了完全 MUB.

(2) 对于 $K_1,K_2\geqslant 2$, 通过把一个 $\mathbb{C}^{K_1}$ 中的 MUB 和一个 $\mathbb{C}^{K_2}$MUB 做张量积, 可以证明 $f(K_1K_2)\geqslant\min\{f(K_1),f(K_2)\}$. 则由 (1) 可知对于所有的 $K\geqslant 2$, $f(K)\geqslant 3$.

(3) $f(K^2)\geqslant L(K)+2$ [15], 其中 $L(K)$ 是 K ($\geqslant 2$) 阶正交拉丁方的最大个数. 由这个结论可知对于某些 m (例如 $m=6$) $f((4m+2)^2)\geqslant 6$.

(4) $f(K)\neq K$ [16]. 即对任意 $K\geqslant 2$, $f(K)=K+1$ 或 $f(K)\leqslant K-1$.

(5) 对任意 $K\neq p^l$, $f(K)$ 的准确值都还未知. 甚至 $f(6)$ 是否等于 3 还是未知的 [17].

鉴于目前还没有关于 $K\neq p^l$ 时完全 MUB 的存在性结果, [1,18] 等文献中考虑了将内积条件 (1.2) 放松为对 $1\leqslant i\neq j\leqslant K$, $|\langle v_i|v_j\rangle|\leqslant\frac{1}{\sqrt{K}}(1+o(1))$, $\frac{1}{\sqrt{K}}(2+o(1))$, $O(\frac{1}{\sqrt{K}})$ 甚至 $O(\frac{\log K}{\sqrt{K}})$ 的近似 MUB. 本文采用 [1] 中给出的近似 MUB 的定义, 即把内积条件放松为上面第一种情形.

定义 3 $\mathbb{C}^K$ 中 m 组标准正交基 $\mathcal{B}=\{B_1,B_2,\ldots,B_m\}$, 如果它们满足对所有的 $v_i\in B_i$, $v_j\in B_j$ $(1\leqslant i\neq j\leqslant m)$ 都有

$$|\langle v_i|v_j\rangle|^2\leqslant\frac{1}{K}(1+o(1)),$$

则称这 m 组标准正交基为近似 MUB, 简称为 AMUB.

Klappenecker 等人在 [1] 中, 对于所有 $K=p-1$, 构造出了 $m=K+1$ 的 AMUB (p 为素数), 并且断言对于 $K=q-1$ (q 为素数方幂) 也可以通过类似的方法构造 AMUB. 本文的第 3 节将给出一种构造 $K=q-1$ 时 $m=K+1$ 的 AMUB 的方法 (定理 3.1). 在第 3 节中, 我们还给出一种构造 $k=q-1$ 时 $m=K+2$ 的 AMUB 的方法 (定理 3.2), 这说明了 $\mathbb{C}^K$ 中的 AMUB 包含的标准正交基的组数可以大于 $K+1$. 第 3 节还给出了一种对于 $K=q+1$ 时 $m=K-1$ 的 AMUB 的构造方法 (定理 3.3).

下面介绍 SIC-POVM 的定义.

定义 4 $\mathbb{C}^K$ 中的一个 SIC-POVM 是 K^2 个长度为 1 的向量组成的集合, $\{v_i \in \mathbb{C}S^{K-1}\ (1 \leqslant i \leqslant K^2)\}$, 其中对任意的 (i,j), $1 \leqslant i \neq j \leqslant K$,

$$|\langle v_i|v_j\rangle| = \frac{1}{\sqrt{K+1}}. \tag{1.3}$$

容易验证 SIC-POVM 是一个复球面 2- 设计. Zauner [19] 猜想对所有的 $K \geqslant 2$, $\mathbb{C}^K$ 中的 SIC-POVM 都存在. 但是到目前为止只对有限多个维数 K, SIC-POVM 被发现存在 (见 [20]).

类似于 MUB 的情形, 很多放松了内积条件 (1.3) 的近似 SIC-POVM 被人们所研究 [1]. 例如将内积条件放松为对 $1 \leqslant i \neq j \leqslant K$, $|\langle v_i|v_j\rangle|^2 \leqslant \frac{1}{K}(1+o(1))$, 或 $\frac{2}{K}(1+o(1))$. 但是这样并不一定能够满足在量子测量中所需要的完备性和信息完备性. 本文采用 [1] 中给出的近似 SIC-POVM 的定义.

定义 5 K 是一个正整数 $(K \geqslant 2)$, $A = \{v_i : 1 \leqslant i \leqslant K^2\}$ 是 $\mathbb{C}^K$ 的一个子集并且 $|A| = K^2$ (v_i 不一定是单位向量),

$$E_i = \frac{1}{K}|v_i\rangle\langle v_j| \quad (1 \leqslant i \leqslant K^2),$$

其中对非零向量 $a = (a_1, a_2, \ldots, a_K) \in \mathbb{C}^K$, 投影算子 $|a\rangle\langle a|$ 是下面定义的 1 维 K 阶方阵,

$$|a\rangle\langle a| = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_K \end{pmatrix} (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_K}) = \begin{pmatrix} a_1\overline{a_1} & a_1\overline{a_2} & \cdots & a_1\overline{a_K} \\ a_2\overline{a_1} & a_2\overline{a_2} & \cdots & a_2\overline{a_K} \\ \vdots & \vdots & \ddots & \vdots \\ a_K\overline{a_1} & a_K\overline{a_2} & \cdots & a_K\overline{a_K} \end{pmatrix}.$$

A 称为近似 SIC-POVM (简称为 ASIC-POVM), 如果它满足以下三个条件:

(I) (近似对称) 对于 $1 \leqslant i \neq j \leqslant K^2$, $K^2\mathrm{tr}(E_iE_j) = |\langle v_i|v_j\rangle|^2 \leqslant \frac{1}{K}(1+o(1))$;

(II) (POVM 的完备性) $\sum_{i=1}^{K^2} E_i = I_K$;

(III) (信息完备性) E_i $(1 \leqslant i \leqslant K^2)$ 是 $\mathbb{C}^{K^2}$ 的一组基.

Klappenecker 等 [1] 对于所有的 $K = p^l$ (其中 $l \geqslant 1$, p 是奇素数) 构造出了 ASIC-POVM. 本文在第 4 节中对于 $K = q-1$ (q 是任何素数的方幂) 给出了一种更简单的构造 ASIC-POVM 的方法. 本文给出的所有构造 AMUB 和 ASIC-POVM 的方法都是利用 Gauss 和与 Jacobi 和得到的. 本文第 2 节介绍了文中需要用到的 Gauss 和与 Jacobi 和的基本事实. 第 3 和 4 节分别给出利用 Gauss 和与 Jacobi 和构造 AMUB 和 ASIC-POVM 的方法.

2 Gauss 和与 Jacobi 和

若 p 是一个素数, $q = p^l$ $(l \geqslant 1)$ 是一个素数方幂, $\mathbb{F}_q$ 是一个 q 元有限域, 迹映射 $T : \mathbb{F}_q \to \mathbb{F}_p$ 定义为

$$T(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{l-1}} \quad (\alpha \in \mathbb{F}_q).$$

对正整数 n, 记 $\zeta_n = \mathrm{e}^{\frac{2\pi\sqrt{-1}}{n}}$ 为 1 的复 n 次根. $(\mathbb{F}_q, +)$ 的加法特征群为

$$\mathbb{F}_q^\wedge = \{\lambda_b : b \in \mathbb{F}_q\},$$

其中加法特征 $\lambda_b : \mathbb{F}_q \to \langle\zeta_p\rangle$ 定义为

$$\lambda_b(x) = \zeta_p^{T(bx)} \quad (x \in \mathbb{F}_q),$$

$\lambda_0 = 1$ 称为平凡特征. 取 $\mathbb{F}_q$ 的一个本原元 γ. 即 γ 是 $\mathbb{F}_q$ 的乘法群 $\mathbb{F}_q^\times = \mathbb{F}_q\backslash\{0\} = \langle\gamma\rangle$ 的一个生成元. 则 $\mathbb{F}_q$ 的乘法特征群为

$$(\mathbb{F}_q^\times)^\wedge = \{\psi^i : 0 \leqslant i \leqslant q-2\},$$

其中 $\psi : \mathbb{F}_q^\times \to \langle\zeta_{q-1}\rangle$ 定义为

$$\psi(\gamma^i) = \zeta_{q-1}^j \quad (0 \leqslant j \leqslant q-2),$$

$\psi^0 = 1$ 称为平凡乘法特征. 一个乘法特征 χ 在乘法特征群中的逆元素为它的共轭 $\overline{\chi}(\alpha) = \overline{\chi(\alpha)}$ $(\alpha \in \mathbb{F}_q^\times)$. 我们假定对所有的乘法特征 χ, $\chi(0) = 0$.

定义 6 λ 是 $\mathbb{F}_q$ 的一个加法特征, χ, χ_1 和 χ_2 是 $\mathbb{F}_q$ 的乘法特征, 有限域 $\mathbb{F}_q$ 上的 Gauss 和 $G(\lambda,\chi)$ 以及 Jacobi 和 $J(\chi_1,\chi_2)$ 定义如下:

$$G(\lambda,\chi) = \sum_{x\in\mathbb{F}_q} \lambda(x)\chi(x) \in \mathbb{Z}[\zeta_{p(q-1)}],$$

$$J(\chi_1,\chi_2) = \sum_{x\in\mathbb{F}_q\backslash\{0,1\}} \chi_1(x)\chi_2(1-x) \ (= J(\chi_2,\chi_1) \in \mathbb{Z}[\zeta_{q-1}]).$$

下面关于 Gauss 和与 Jacobi 和的基本事实可以参见有关有限域的书 (例如 [21]) .

引理 2 (1) 对 $\mathbb{F}_q$ 的加法特征 λ 和乘法特征 χ,

$$G(\lambda,\chi) = \begin{cases} q-1, & \text{若} \quad \lambda = 1 \text{ 且 } \chi = 1, \\ 0, & \text{若} \quad \lambda = 1 \text{ 且 } \chi \neq 1, \\ -1, & \text{若} \quad \lambda \neq 1 \text{ 且 } \chi = 1, \end{cases}$$

如果 λ 和 χ 均不是平凡特征 $|G(\lambda,\chi)| = \sqrt{q}$.

(2) 对于 $b \in \mathbb{F}_q^\times$, $G(\lambda_b,\chi) = G(\chi)\overline{\chi}(b)$, 其中

$$G(\chi) = G(\lambda_1,\chi) = \sum_{x\in\mathbb{F}_q^\times} \chi(x)\zeta^{T(x)}.$$

(3) 对 $\mathbb{F}_q$ 的乘法特征 χ_1 和 χ_2,

$$J(\chi_1,\chi_2) = \begin{cases} q-2, & \text{若} \quad \chi_1 = \chi_2 = 1, \\ -1, & \text{若} \quad \chi_1 = 1, \chi_2 \neq 1 \text{ 或 } \chi_1 \neq 1, \chi_2 = 1, \\ -\chi_1(-1), & \text{若} \quad \chi_1 \neq 1 \text{ 且 } \chi_1 = \overline{\chi_2}, \end{cases}$$

如果 χ_1, χ_2 和 $\chi_1\chi_2$ 均不是平凡乘法特征, $J(\chi_1,\chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}$, 于是 $|J(\chi_1,\chi_2)| = \sqrt{q}$.

3 AMUB 的构造

本节将给出三种非常简洁的利用 Gauss 和与 Jacobi 和构造 AMUB 的方法. 二次 Gauss 和在 [12–14] 中被用来构造 MUB 和 SIC-POVM.

首先对 $K=q-1$ 的情形给出一种利用 Jacobi 和构造 $\mathbb{C}^K$ 中包含 $K+1$ 组标准正交基的 AMUB 的方法, 其中 q 是某个素数 p 的方幂.

定理 1 若 $K=q-1$, $\mathbb{F}_q\backslash\{0,1\}=\{x_1,x_2,\ldots,x_{K-1}\}$. 对任意两个 $\chi,\chi'\in(\mathbb{F}_q^\times)^\wedge$, 令

$$\tilde{c}_{\chi,\chi'}=\frac{1}{\sqrt{K}}(\chi(x_1)\chi'(1-x_1),\chi(x_2)\chi'(1-x_2),\ldots,\chi(x_{K-1})\chi'(1-x_{K-1}),1)\in\mathbb{C}S^{K-1}.$$

对每一个 $\chi\in(\mathbb{F}_q^\times)^\wedge$, 令

$$B_\chi=\{\tilde{c}_{\chi,\chi'}:\chi'\in(\mathbb{F}_q^\times)^\wedge\},\quad |B_\chi|=K.$$

记 $B_*=\{e_1,e_2,\ldots,e_K\}$ 为 $\mathbb{C}^K$ 的平凡标准正交基, 即

$$e_1=(1,0,\ldots,0),\quad e_2=(0,1,0,\ldots,0),\quad \ldots,\quad e_K=(0,\ldots,0,1).$$

则 $\mathcal{B}=\{B_\chi:\chi\in(\mathbb{F}_q^\times)^\wedge\}\cup\{B_*\}$ 是 $\mathbb{C}^K$ 中的一个 AMUB, 且 $|\mathcal{B}|=K+1$.

证明 先证明 B_χ 是 $\mathbb{C}^K$ 的一组标准正交基. 对任意 $\chi'\in(\mathbb{F}_q^\times)^\wedge$,

$$\langle\tilde{c}_{\chi,\chi'}|\tilde{c}_{\chi,\chi'}\rangle=\frac{1}{K}\Bigg(1+\sum_{\substack{x\in\mathbb{F}_q\\x\neq0,1}}\overline{\chi}(x)\overline{\chi'}(1-x)\chi(x)\chi'(1-x)\Bigg)=1.$$

对于 $(\mathbb{F}_q^\times)^\wedge$ 中不同的 χ_1 和 χ_2, 有

$$\begin{aligned}\langle\tilde{c}_{\chi,\chi_1}|\tilde{c}_{\chi,\chi_2}\rangle&=\frac{1}{K}\Bigg(1+\sum_{\substack{x\in\mathbb{F}_q\\x\neq0,1}}\overline{\chi}(x)\overline{\chi_1}(1-x)\chi(x)\chi_2(1-x)\Bigg)\\&=\frac{1}{K}\Bigg(1+\sum_{\substack{x\in\mathbb{F}_q\\x\neq0,1}}\overline{\chi_1}\chi_2(1-x)\Bigg)\\&=\frac{1}{K}\Bigg(1+\sum_{x\in\mathbb{F}_q^\times}\overline{\chi_1}\chi_2(x)-\overline{\chi_1}\chi_2(1)\Bigg)\\&=\frac{1}{K}(1-1)\quad(\text{因为 }\overline{\chi_1}\chi_2\neq1)\\&=0.\end{aligned}$$

这说明对每一个 $\chi\in(\mathbb{F}_q^\times)^\wedge$, B_χ 都是 $\mathbb{C}^K$ 的一组标准正交基.

下面说明 $\mathcal{B}$ 是一个 AMUB. 对于 $\tilde{c}_{\chi,\chi'}\in B_\chi$ 和 $e_i\in B_*$ 显然有 $|\langle e_i|\tilde{c}_{\chi,\chi'}\rangle|=\frac{1}{\sqrt{K}}$. 对于不同的 χ 和 χ', $\tilde{c}_{\chi,\chi_1}\in B_\chi$ 和 $\tilde{c}_{\chi',\chi_2}\in B_{\chi'}$ 有:

$$\begin{aligned}\langle\tilde{c}_{\chi,\chi_1}|\tilde{c}_{\chi',\chi_2}\rangle&=\frac{1}{K}\Bigg(1+\sum_{\substack{x\in\mathbb{F}_q\\x\neq0,1}}\overline{\chi}(x)\overline{\chi_1}(1-x)\chi'(x)\chi_2(1-x)\Bigg)\\&=\frac{1}{K}\Bigg(1+\sum_{\substack{x\in\mathbb{F}_q\\x\neq0,1}}\varphi(x)\psi(1-x)\Bigg)\quad(\text{其中 }\varphi=\overline{\chi}\chi'\neq1,\ \varphi=\overline{\chi_1}\chi_2)\\&=\frac{1}{K}(1+J(\varphi,\psi)).\end{aligned}$$

由引理 2(3), 可得

$$|\langle\tilde{c}_{\chi,\chi_1}|\tilde{c}_{\chi',\chi_2}\rangle|^2=\begin{cases}\dfrac{1}{K^2}(1-1)=0, & \text{若 } \psi=1\,(\Leftrightarrow \chi_1=\chi_2),\\ \dfrac{1}{K^2}(1-\varphi(-1))\leqslant\dfrac{2}{K^2}, & \text{若 } \psi=\overline{\varphi},\\ \dfrac{1}{K^2}|1+J(\varphi,\psi)|^2\leqslant\dfrac{(1+\sqrt{K+1})^2}{K^2}=\dfrac{1}{K}+\dfrac{2(\sqrt{K+1}+1)}{K^2}, & \text{否则.}\end{cases}$$

因此 $\mathcal{B}$ 是 $\mathbb{C}^K$ 中的一个 AMUB, $|\mathcal{B}|=K+1$. □

下面对 $K=q-1$ 的情形给出一种利用 Gauss 和构造 $\mathbb{C}^K$ 中包含 $K+2$ 组标准正交基的 AMUB 的方法.

定理 2 $K=q-1$, 记 $\mathbb{F}_q^\times=\{x_1,x_2,\ldots,x_{q-1}\}$. 对于 $b\in\mathbb{F}_q$ 和 $\chi\in(\mathbb{F}_q^\times)^\wedge$, 令

$$c_{b,\chi}=\frac{1}{\sqrt{K}}(\lambda_b(x_1)\chi(x_1),\lambda_b(x_2)\chi(x_2),\ldots,\lambda_b(x_{q-1})\chi(x_{q-1}))\in\mathbb{C}S^{K-1}.$$

对每个 $b\in\mathbb{F}_q$, 令

$$B_b=\{c_{b,\chi}:\chi\in(\mathbb{F}_q^\times)^\wedge\},\quad |B_b|=K.$$

则 $\mathcal{B}=\{B_b:b\in\mathbb{F}_q\}\cup\{B_*\}$ 是 $\mathbb{C}^K$ 中的一个 AMUB, 且 $|B|=K+2$, 其中 B_* 是 $\mathbb{C}^K$ 中平凡的标准正交基.

证明 对于 $b\in\mathbb{F}_q$ 以及 $\mathbb{F}_q$ 的两个乘法特征 χ_1 和 χ_2,

$$\begin{aligned}\langle c_{b,\chi_1}|c_{b,\chi_2}\rangle&=\frac{1}{K}\sum_{x\in\mathbb{F}_q^\times}\overline{\lambda_b}(x)\overline{\chi_1}(x)\lambda_b(x)\chi_2(x)\\&=\frac{1}{K}\sum_{x\in\mathbb{F}_q^\times}\overline{\chi_1}\chi_2(x)\\&=\begin{cases}1, & \text{若 } \chi_1=\chi_2,\\ 0, & \text{若 } \chi_1\neq\chi_2.\end{cases}\end{aligned}$$

从而对每个 $b\in\mathbb{F}_q$, B_b 是 $\mathbb{C}^K$ 中的一组标准正交基. 对于 $c_{b,\chi}\in B_b$ 和 $e_i\in B_*$, 则有 $|\langle c_{b,\chi}|e_i\rangle|^2=\frac{1}{K}$. 对于 $c_{b,\chi}\in B_b$ 和 $c_{b',\chi'}\in B_{b'}$, 其中 $b,b'\in\mathbb{F}_q$, $b\neq b'$ 有

$$\begin{aligned}\langle c_{b,\chi}|c_{b',\chi'}\rangle&=\frac{1}{K}\sum_{x\in\mathbb{F}_q^\times}\overline{\lambda_b}(x)\overline{\chi}(x)\lambda_{b'}(x)\chi'(x)\\&=\frac{1}{K}\sum_{x\in\mathbb{F}_q^\times}\lambda_a(x)\overline{\chi}\chi'(x)\quad(a=b'-b\in\mathbb{F}_q^\times).\end{aligned}$$

则由引理 2(1) 可知

$$\langle c_{b,\chi}|c_{b'\chi'}\rangle=\begin{cases}-\dfrac{1}{K}, & \text{若 } \chi=\chi',\\ \dfrac{1}{K}\chi\overline{\chi'}(a)G(\overline{\chi}\chi'), & \text{若 } \chi\neq\chi'.\end{cases}$$

从而

$$|\langle c_{b,\chi}|c_{b'\chi'}\rangle|^2=\begin{cases}\dfrac{1}{K^2}, & \text{若 } \chi=\chi',\\ \dfrac{1}{K^2}|G(\overline{\chi}\chi')|^2=\frac{K+1}{K^2}=\frac{1}{K}+\frac{1}{K^2}, & \text{若 } \chi\neq\chi'.\end{cases}$$

因此 $\mathcal{B}=\{B_b:\ b\in\mathbb{F}_q\}\cup\{B_*\}$ 是 $\mathbb{C}^K$ 中的一个 AMUB, 且 $|B|=K+2$. □

在这一节的最后, 我们给出一种构造 $\mathbb{C}^K$ $(K=q+1)$ 中包含 $K-1$ 组标准正交基的 AMUB 的方法. 对任意 $n\geqslant 1$, 令 $T_q^{q^n}:\mathbb{F}_{q^n}\to\mathbb{F}_q$ 为从 $\mathbb{F}_{q^n}$ 到它的子域 $\mathbb{F}_q$ 的迹映射. 即对于 $\alpha\in\mathbb{F}_{q^n}$,

$$T_q^{q^n}(\alpha)=\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{n-1}}\in\mathbb{F}_q.$$

特别地, 对于 $\alpha\in\mathbb{F}_{q^2}$, $T_q^{q^2}=\alpha+\alpha^q$. 熟知 $T_q^{q^n}$ 是一个满的 $\mathbb{F}_q$- 线性映射, 从而对任意 $a\in\mathbb{F}_q$, 以下子集

$$D_a=\{\alpha\in\mathbb{F}_{q^n}:\ T_q^{q^n}(\alpha)=a\}$$

都是子空间 D_0 的一个陪集, 且 $|D_a|=q^{n-1}$.

定理 3 $q=p^m$, 若 γ 是 $\mathbb{F}_{q^2}$ 中一个本原元, 并且

$$\begin{aligned}D&=\{\alpha\in\mathbb{F}_{q^2}:\ T_q^{q^2}(\alpha)=1\}\\&=\{x_1,x_2,\ldots,x_q\}.\end{aligned}$$

令 $K=q+1$, $(\mathbb{F}_{q^2}^\times)^\wedge$ 为 $\mathbb{F}_{q^2}$ 的乘法群的特征群, 对任意 $\chi\in(\mathbb{F}_{q^2}^\times)^\wedge$, 令

$$\tilde{c}_\chi=\frac{1}{\sqrt{K}}(\chi(x_1),\chi(x_2),\ldots,\chi(x_q),\chi(\xi))\in\mathbb{C}S^{K-1},$$

其中

$$\xi=\begin{cases}\gamma^{\frac{q+1}{2}}, & \text{若 } 2\nmid q,\\ 1, & \text{若 } 2\mid q.\end{cases}$$

若 ψ 是 $\mathbb{F}_{q^2}$ 的一个乘法特征, 且 $\psi(\gamma)=\zeta_{q^2-1}$, 则 $(\mathbb{F}_{q^2}^\times)^\wedge=\{\psi^i:\ 0\leqslant i\leqslant q^2-2\}$. 令 B_* 是 $\mathbb{C}^K$ 中的平凡标准正交基. 对每个 i, $0\leqslant i\leqslant q-2=K-3$, 令

$$B_i=\{\tilde{c}_{\psi^{i+l(q-1)}}:\ l=0,1,\ldots,q\},$$

则 $\mathcal{B}=\{B_0,B_1,\ldots,B_{K-3},B_*\}$ 是 $\mathbb{C}^K$ 中的一个 AMUB, $|\mathcal{B}|=K-1$.

证明 若 $\tilde{c}_\chi$ 和 $\tilde{c}_{\chi'}$ 是 B_i 中两个不同的向量, 则

$$\chi=\psi^{i+l(q-1)},\quad \chi'=\psi^{i+l'(q-1)},\quad 0\leqslant l\neq l'\leqslant q-2.$$

从而

$$\begin{aligned}\langle\tilde{c}_\chi|\tilde{c}_{\chi'}\rangle&=\frac{1}{K}\left(\overline{\chi}\chi'(\xi)+\sum_{x\in D}\overline{\chi}\chi'(x)\right)\\&=\frac{1}{K}\left(\varphi(\xi)+\sum_{x\in D}\varphi(x)\right),\end{aligned}\tag{3.1}$$

其中 $\varphi=\overline{\chi}\chi'=\psi^{(l'-l)(q-1)}\neq 1$, 故对每个 $a\in\mathbb{F}_q^\times$, $\varphi(a)=\psi^{l'-l}(a^{q-1})=1$. 由 D 的定义可知

$$\sum_{x\in D}\varphi(x)=\sum_{\substack{x\in\mathbb{F}_{q^2}^\times\\ T_q^{q^2}(x)=1}}\varphi(x)=\frac{1}{q}\sum_{x\in\mathbb{F}_{q^2}^\times}\varphi(x)\sum_{y\in\mathbb{F}_q}\zeta_p^{T_p^q(y(T_q^{q^2}(x)-1))}$$

$$
\begin{aligned}
&= \frac{1}{q}\sum_{y\in\mathbb{F}_q^\times}\overline{\zeta_p}^{T_p^q(y)}\sum_{x\in\mathbb{F}_{q^2}^\times}\zeta_p^{T_p^{q^2}(xy)}\varphi(x)\\
&= \frac{1}{q}G_{q^2}(\varphi)\sum_{y\in\mathbb{F}_q^\times}\overline{\zeta_p}^{T_p^q(y)}\overline{\varphi}(y)\\
&= \frac{1}{q}G_{q^2}(\varphi)\sum_{y\in\mathbb{F}_q^\times}\overline{\zeta_p}^{T_p^q(y)}\\
&= -\frac{1}{q}G_{q^2}(\varphi), \qquad (3.2)
\end{aligned}
$$

其中

$$G_{q^2}(\varphi)=\sum_{x\in\mathbb{F}_{q^2}^\times}\varphi(x)\zeta_p^{T_p^{q^2}(x)}$$

是域 $\mathbb{F}_{q^2}$ 上的 Gauss 和. 熟知 $\mathbb{F}_q^\times=\langle\gamma^{q+1}\rangle$ 是 $\mathbb{F}_{q^2}^\times$ 的子群, 并且 $\mathbb{F}_{q^2}^\times$ 是 $\mathbb{F}_q^\times$ 的 $q+1$ 个陪集 $C_i=\gamma^i\mathbb{F}_q^\times$ $(i=0,1,\ldots,q)$ 的不交并. 对于 $\alpha\in C_i$ 有 $\varphi(\alpha)=\varphi(\gamma^i)$. 从而

$$
\begin{aligned}
G_{q^2}(\varphi)&=\sum_{i=0}^{q}\varphi(\gamma^i)\sum_{y\in\mathbb{F}_q^\times}\zeta_p^{T_p^{q^2}(\gamma^i y)}\\
&=\sum_{i=0}^{q}\varphi(\gamma^i)\sum_{y\in\mathbb{F}_q^\times}\zeta_p^{T_p^q(yT_q^{q^2}(\gamma^i))}\\
&=(q-1)\sum_{\substack{i=0\\ T_q^{q^2}(\gamma^i)=0}}^{q}\varphi(\gamma^i)-\sum_{\substack{i=0\\ T_q^{q^2}(\gamma^i)\neq 0}}^{q}\varphi(\gamma^i)\\
&=q\sum_{\substack{i=0\\ T_q^{q^2}(\gamma^i)=0}}^{q}\varphi(\gamma^i)-\sum_{i=0}^{q}\varphi(\gamma^i).
\end{aligned}
$$

由于 $\varphi(\mathbb{F}_q^\times)=1$, 可以把 φ 看做商群 $\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times=\{\gamma^i\mathbb{F}_q^\times:0\leqslant i\leqslant q\}$ 的一个非平凡特征. 因此 $\sum_{i=0}^{q}\varphi(\gamma^i)=0$, 并且

$$G_{q^2}(\varphi)=q\sum_{\substack{i=0\\ T_q^{q^2}(\gamma^i)=0}}^{q}\varphi(\gamma^i).$$

由 $T_q^{q^2}(\gamma^i)=\gamma^i+\gamma^{qi}$, 可知 $T_q^{q^2}(\gamma^i)=0$ 当且仅当 $\gamma^{(q-1)i}=-1$. 如果 $2\mid q$, 则 $\gamma^{(q-1)i}=1$ $(0\leqslant i\leqslant q)$ 只有 $i=0$ 这一个解, 从而 $G_{q^2}(\varphi)=q\varphi(1)=q$. 如果 $2\nmid q$, 则 $\gamma^{(q-1)i}=-1=\gamma^{\frac{q^2-1}{2}}$ $(0\leqslant i\leqslant q)$ 只有解 $i=\frac{q+1}{2}$, 从而 $G_{q^2}(\varphi)=\varphi(\gamma^{\frac{q+1}{2}})q$. 因此 $G_{q^2}(\varphi)=q\varphi(\xi)$, 并且由 (3.1) 和 (3.2) 可得

$$\langle\tilde{c}_\chi|\tilde{c}_{\chi'}\rangle=\frac{1}{K}\left(\varphi(\xi)-\frac{1}{q}q\varphi(\xi)\right)=0,$$

这说明 B_i $(i=0,1,\ldots,K-3)$ 是标准正交基.

对于 $\tilde{c}_\chi\in B_i$ 和 $e_m\in B_*$, 有 $|\langle\tilde{c}_\chi|e_m\rangle|^2=\frac{1}{K}$. 对于 $\tilde{c}_\chi\in B_i$ 和 $\tilde{c}_{\chi'}\in B_{i'}$ $(0\leqslant i\neq i'\leqslant q)$, 有 $\overline{\chi}\chi'(\mathbb{F}_q^\times)\neq 1$. 即 $\overline{\chi}\chi'$ 是 $\mathbb{F}_q^\times$ 的一个非平凡乘法特征. 类似上面的过程进行计算, 可知

$$\langle\tilde{c}_\chi|\tilde{c}_{\chi'}\rangle=\frac{1}{K}\left(\varphi(\xi)+\sum_{x\in D}\varphi(x)\right)\quad(\varphi=\overline{\chi}\chi',\ \varphi(\mathbb{F}_q^\times)\neq 1),$$

$$= \frac{1}{K}\left(\varphi(\xi) - \frac{1}{q}G_{q^2}(\varphi)\overline{G_q(\varphi)}\right), \tag{3.3}$$

其中

$$G_q(\varphi) = \sum_{y\in\mathbb{F}_q^\times} \zeta_p^{T_p^q(y)}\varphi(y)$$

是 $\mathbb{F}_q$ 上的一个 Gauss 和. 因为 φ 是 $\mathbb{F}_q$ 的一个非平凡特征, 由引理 2 可知 $|G_q(\varphi)| = \sqrt{q}$ 且 $|G_{q^2}(\varphi)| = q$. 再由 (3.3) 可得

$$\begin{aligned} |\langle\tilde{c}_\chi|\tilde{c}_{\chi'}\rangle|^2 &\leqslant \frac{1}{K^2}(1+\sqrt{q})^2 \\ &= \frac{K+2\sqrt{K-1}}{K^2} \\ &= \frac{1}{K} + \frac{2\sqrt{K-1}}{K^2}, \end{aligned}$$

于是 $\mathcal{B} = \{B_0, \ldots, B_{K-2}, B_*\}$ 是 $\mathbb{C}^K$ 的一个 AMUB. □

4 ASIC-POVM 的构造

本节对于 $K = q-1$ (q 是一个素数方幂) 的情形, 给出一种利用 Gauss 和构造 $\mathbb{C}^K$ 上 ASIC-POVM 的方法. 这种构造方法使用了 [22] 和 [1] 中给出的一种技巧.

与定理 3 中一样, $K = q-1$, $\mathbb{F}_q^\times = \{x_1, x_2, \ldots, x_K\}$. 对 $b \in \mathbb{F}_q$ 和 $\chi \in (\mathbb{F}_q^\times)^\wedge$, 令

$$\begin{aligned} c_{b,\chi} &= \frac{1}{\sqrt{K}}(\lambda_b(x_1)\chi(x_1), \lambda_b(x_2)\chi(x_2), \ldots, \lambda_b(x_K)\chi(x_K)) \in \mathbb{C}S^{K-1}, \\ E_{b,\chi} &= \frac{1}{K}|c_{b,\chi}\rangle\langle c_{b,\chi}| = \frac{1}{K^2}(\lambda_b(x-y)\chi(xy^{-1}))_{x,y\in\mathbb{F}_q^\times}. \end{aligned} \tag{4.1}$$

记 $\{e_1, e_2, \ldots, e_K\}$ 为 $\mathbb{C}^K$ 的平凡标准正交基, 令 $E_i = \frac{1}{K}|e_i\rangle\langle e_i|$. 令

$$M = \sum_{i=1}^K E_i + \sum_{\substack{b\in\mathbb{F}_q^\times \\ \chi\in\mathbb{F}_q^\times, \chi\neq\chi_0}} E_{b,\chi},$$

其中 χ_0 是 $\mathbb{F}_q^\times$ 的平凡乘法特征. 我们可以计算出方阵 M 中的每一个元素:

$$M(x,x) = \frac{1}{K} + \frac{1}{K^2}K(K-1) = 1.$$

如果 $x \neq y$,

$$\begin{aligned} M(x,y) &= \frac{1}{K^2} \sum_{\substack{b\in\mathbb{F}_q^\times \\ \chi\in(\mathbb{F}_q^\times)^\wedge, \chi\neq\chi_0}} \lambda_b(x-y)\chi(xy^{-1}) \\ &= \frac{1}{K^2}\left(\sum_{b\in\mathbb{F}_q^\times}\lambda_b(x-y)\right)\left(\sum_{\substack{\chi\in(\mathbb{F}_q^\times)^\wedge \\ \chi\neq\chi_0}}\chi(xy^{-1})\right) \\ &= \frac{1}{K^2}. \end{aligned}$$

因此 $M=\frac{K^2-1}{K^2}I+\frac{1}{K^2}J$, 其中 I 是单位矩阵, J 是每个元素都是 1 的矩阵. 由于 $\{e_1,e_2,\dots,e_K\}$ 可以生成整个 $\mathbb{C}^K$, 下面的不等式

$$\langle v|M|v\rangle=\sum_{i=1}^{K}|\langle e_i|v\rangle|^2+\sum_{\substack{b\in\mathbb{F}_q^\times\\ \chi\in(\mathbb{F}_q^\times)^\wedge,\chi\neq\chi_0}}|\langle c_{b,\chi}|v\rangle|^2>0$$

对每个非零向量 $|v\rangle\in\mathbb{C}^K$ 都成立, 于是 M 是正定矩阵. 因此 M 可逆, M^{-1} 也是正定矩阵. 并且存在唯一的 K 阶正定方阵 $M^{-\frac{1}{2}}$, 使得 $(M^{-\frac{1}{2}})^2=M^{-1}$.

事实上, 可以计算出

$$\begin{aligned}M^{-1}&=\frac{K^2}{K^2-1}I-\frac{K^2}{(K^2-1)(K^2+K-1)}J,\\ M^{-\frac{1}{2}}&=\frac{K}{\sqrt{K^2-1}}I-\left(\frac{1}{\sqrt{K^2-1}}-\frac{1}{\sqrt{K^2+K-1}}\right)J.\end{aligned}$$

定理 4 q 是一个素数方幂, $K=q-1$, $c_{b,\chi}$,$E_{b,\chi}$ $(b\in\mathbb{F}_q,\chi\in(\mathbb{F}_q^\times)^\wedge)$, e_i, E_i $(1\leqslant i\leqslant K)$ 定义如上. 对于 $b\in\mathbb{F}_q$, $\chi\in(\mathbb{F}_q^\times)^\wedge$ 和 $1\leqslant i\leqslant K$, 令

$$\begin{aligned}|c'_{b,\chi}\rangle&=M^{-\frac{1}{2}}|c_{b,\chi}\rangle,\quad F_{b,\chi}=\frac{1}{K}|c'_{b,\chi}\rangle\langle c'_{b,\chi}|=M^{-\frac{1}{2}}E_{b,\chi}M^{-\frac{1}{2}},\\ |c'_i\rangle&=M^{-\frac{1}{2}}|e_i\rangle,\quad F_i=\frac{1}{K}|c'_i\rangle\langle c'_i|=M^{-\frac{1}{2}}E_iM^{-\frac{1}{2}},\end{aligned}$$

则 $\{|c'_{b,\chi}\rangle:b\in\mathbb{F}_q^\times,\chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}\}\cup\{|c'_i\rangle:1\leqslant i\leqslant K\}$ 是 $\mathbb{C}^K$ 的一个 ASIC-POVM.

证明 我们需要逐条验证定义 5 中的 (I), (II) 和 (III).

(I) 对于 $1\leqslant i\neq j\leqslant K$,

$$\begin{aligned}K^2\mathrm{tr}(F_iF_j)&=|\langle e_i|M^{-1}|e_i\rangle|^2\\ &=\left|\frac{K^2}{K^2-1}\langle e_i|e_j\rangle-\frac{K^2}{(K^2-1)(K^2+K-1)}\langle e_i|J|e_j\rangle\right|^2\\ &=\frac{K^4}{(K^2-1)^2(K^2+K-1)^2}\\ &=\frac{1}{K^4}+o\left(\frac{1}{K^4}\right)\\ &\leqslant\frac{1}{K}+o\left(\frac{1}{K}\right).\end{aligned}$$

对于 $1\leqslant i\leqslant K$, $b\in\mathbb{F}_q^\times$, $\chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}$,

$$\begin{aligned}K^2\mathrm{tr}(F_iF_{b,\chi})&=|\langle e_i|M^{-1}|c_{b,\chi}\rangle|^2\\ &=\left|\frac{K^2}{K^2-1}\langle e_i|c_{b,\chi}\rangle-\frac{K^2}{(K^2-1)(K^2+K-1)}\langle e_i|J|c_{b,\chi}\rangle\right|^2\\ &\leqslant\left(\frac{K^2}{K^2-1}\left|\frac{1}{\sqrt{K}}\lambda_b(x_i)\chi(x_i)\right|+\frac{K^2}{(K^2-1)(K^2+K-1)}\left|\frac{1}{\sqrt{K}}G(\lambda_b,\chi)\right|\right)^2\\ &=\left(\frac{K^{3/2}}{K^2-1}+\frac{K^{3/2}\sqrt{K+1}}{(K^2-1)(K^2+K-1)}\right)^2\end{aligned}$$

$$
\begin{aligned}
&= \frac{K^3(K^2+K+\sqrt{K+1}-1)^2}{(K^2-1)^2(K^2+K-1)^2}\\
&= \frac{1}{K}+o\bigg(\frac{1}{K}\bigg).
\end{aligned}
$$

对于 $b\in\mathbb{F}_q^\times$, $\chi,\chi'\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}$ 和 $\chi\neq\chi'$,

$$
\begin{aligned}
K^2\mathrm{tr}(F_{b,\chi}F_{b,\chi'}) &= \bigg|\frac{K^2}{K^2-1}\langle c_{b,\chi}|c_{b,\chi'}\rangle-\frac{K^2}{(K^2-1)(K^2+K-1)}\langle c_{b,\chi}|J|c_{b,\chi'}\rangle\bigg|^2\\
&\leqslant \frac{K^4}{(K^2-1)^2(K^2+K-1)^2}\bigg|\frac{1}{K}\overline{G(\lambda_b,\chi)}G(\lambda_b,\chi')\bigg|^2\\
&= \frac{K^2(K+1)^2}{(K^2-1)^2(K^2+K-1)^2}\\
&= \frac{1}{K^4}+o\bigg(\frac{1}{K^4}\bigg)\\
&\leqslant \frac{1}{K}+o\bigg(\frac{1}{K}\bigg).
\end{aligned}
$$

对于 $b,b'\in\mathbb{F}_q^\times$, $b\neq b'$, $\chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}$,

$$
\begin{aligned}
K^2\mathrm{tr}(F_{b,\chi}F_{b',\chi}) &= \bigg|\frac{K^2}{K^2-1}\langle c_{b,\chi}|c_{b',\chi}\rangle-\frac{K^2}{(K^2-1)(K^2+K-1)}\langle c_{b,\chi}|J|c_{b',\chi}\rangle\bigg|^2\\
&\leqslant \bigg(\frac{K^2}{K^2-1}\bigg|\frac{1}{K}G(\lambda_{b'-b},\chi_0)\bigg|\\
&\quad+\frac{K^2}{(K^2-1)(K^2+K-1)}\bigg|\frac{1}{K}\overline{G(\lambda_b,\chi)}G(\lambda'_b,\chi)\bigg|\bigg)^2\\
&= \bigg(\frac{K}{K^2-1}+\frac{K}{(K-1)(K^2+K-1)}\bigg)^2\\
&= \frac{K^4(K+2)^2}{(K^2-1)^2(K^2+K-1)^2}\\
&= \frac{1}{K^2}+o\bigg(\frac{1}{K^2}\bigg)\\
&\leqslant \frac{1}{K}+o\bigg(\frac{1}{K}\bigg).
\end{aligned}
$$

对于 $b,b'\in\mathbb{F}_q^\times$, $\chi,\chi'\in(\mathbb{F}_q^\times)^\wedge$, $b\neq b'$, $\chi\neq\chi'$,

$$
\begin{aligned}
K^2\mathrm{tr}(F_{b,\chi}F_{b'\chi'}) &= \bigg|\frac{K^2}{K^2-1}\langle c_{b,\chi}|c_{b',\chi'}\rangle-\frac{K^2}{(K^2-1)(K^2+K-1)}\langle c_{b,\chi}|J|c_{b',\chi'}\rangle\bigg|^2\\
&\leqslant \bigg(\frac{K^2}{K^2-1}\bigg|\frac{1}{K}G(\lambda_{b-b},\overline{\chi}\chi')\bigg|\\
&\quad+\frac{K^2}{(K^2-1)(K^2+K-1)}\bigg|\frac{1}{K}\overline{G(\lambda_b,\chi)}G(\lambda_{b'},\chi')\bigg|\bigg)^2\\
&= \frac{K^2}{(K-1)^2(K+1)}+\frac{2K^2\sqrt{K+1}}{(K-1)^2(K+1)(K^2+K-1)}\\
&\quad+\frac{K^2}{(K-1)^2(K^2+K-1)^2}
\end{aligned}
$$

$$= \frac{1}{K} + o\left(\frac{1}{K}\right).$$

于是这个集合满足条件 (I).

(II)

$$\sum_{i=1}^{K} F_i + \sum_{\substack{b\in\mathbb{F}_b^\times \\ \chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}}} F_{b,\chi} = M^{-\frac{1}{2}}\left(\sum_{i=1}^{K} E_i + \sum_{\substack{b\in\mathbb{F}_b^\times \\ \chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}}} E_{b,\chi}\right) M^{-\frac{1}{2}}$$
$$= M^{-\frac{1}{2}} M M^{-\frac{1}{2}} = I.$$

(III) 只需要证明集合中的矩阵 $\{E_i:\ 1\leqslant i\leqslant K\}\cup\{E_{b,\chi}:\ b\in\mathbb{F}_q^\times, \chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}\}$ 在 $\mathbb{F}^{K^2}$ 中线性无关. 考虑下面这个等式:

$$\sum_{i=1}^{K} \alpha_i E_i + \sum_{\substack{b\in\mathbb{F}_q \\ \chi\in(\mathbb{F}_q^\times)^\wedge}} \alpha_{b,\chi} E_{b,\chi} = 0, \tag{4.2}$$

其中 $\alpha_{0,\chi}=0$ $(\chi\in(\mathbb{F}_q^\times)^\wedge)$, $\alpha_{b,\chi_0}=0$ $(b\in\mathbb{F}_q)$. 假定存在 $\alpha_i\in\mathbb{C}$, $\alpha_{b,\chi}\in\mathbb{C}$ $(b\neq 0,\chi\neq\chi_0)$, 使上面这个等式成立. 由 (4.1), 对于不同的 $x,y\in\mathbb{F}_q^\times$,

$$\sum_{\substack{b\in\mathbb{F}_q \\ \chi\in(\mathbb{F}_q^\times)^\wedge}} \alpha_{b,\chi}\lambda_b(x-y)\chi(xy^{-1}) = 0.$$

令 $a=xy^{-1}$, 则上述等式变为

$$\sum_{\substack{b\in\mathbb{F}_q \\ \chi\in(\mathbb{F}_q^\times)^\wedge}} \alpha_{b,\chi}\lambda_b(y(a-1))\chi(a) = 0 \quad (\forall\, a\in\mathbb{F}_q^\times\backslash\{1\}, y\in\mathbb{F}_q^\times).$$

再令 $f_a(b)=\sum_{\chi\in(\mathbb{F}_q^\times)^\wedge}\alpha_{b,\chi}\chi(a)$, $f_a(\cdot)$ 是 $\mathbb{F}_q$ 上的一个复值函数. 于是

$$\sum_{b\in\mathbb{F}_q} f_a(b)\lambda_{y(a-1)}(b) = 0 \quad (\forall\, a\in\mathbb{F}_q^\times\backslash\{1\}, y\in\mathbb{F}_q^\times). \tag{4.3}$$

令 $\tilde{f}_a(\lambda)=\sum_{b\in\mathbb{F}_q} f_a(b)\lambda(b)$ 为 $f_a(\cdot)$ 的 Fourier 变换. 对于任意固定的 $a\in\mathbb{F}_q^\times\backslash\{1\}$, $y(a-1)$ 跑遍了 $\mathbb{F}_q^\times$, 从而 $\lambda_{y(a-1)}$ 跑遍 $(\mathbb{F}_q,+)^\wedge\backslash\{\lambda_0\}$. 因此, 对任意 $b\in\mathbb{F}_q$, $f_a(b)$ 是一个常数 C_a. 又因为 $f_a(0)=\sum_{\chi\in(\mathbb{F}_q^\times)^\wedge}\alpha_{0,\chi}\chi(a)=0$, 对于任意 $b\in\mathbb{F}_q$, $f_a(b)=0$. 故

$$\sum_{\chi\in(\mathbb{F}_q^\times)^\wedge} \alpha_{b,\chi}\chi(a) = 0 \quad (\forall\, a\in\mathbb{F}_q^\times\backslash\{1\}, b\in\mathbb{F}_q).$$

令 $F_b(\chi)=\alpha_{b,\chi}$. 可以把 $F_b(\chi)$ 看做是关于 $(\mathbb{F}_q^\times)^\wedge$ 的一个函数. 由 Fourier 变换的性质, 对任意 $b\in\mathbb{F}_q$, $F_b(\chi)$ $(=\alpha_{b,\chi})$ 是 $(\mathbb{F}_q^\times)^\wedge$ 上的一个常函数. 因为对任意 $\chi\in(\mathbb{F}_q^\times)^\wedge$ 和 $b\in\mathbb{F}_q$, 都有 $F_b(\chi_0)=\alpha_{b,\chi_0}=0$, $\alpha_{b,\chi}=F_b(\chi)=0$. 方程 (4.2) 又转化为 $\sum_{i=1}^{K}\alpha_i E_i=0$. 显然这个方程成立当且仅当 $\alpha_i=0$ $(1\leqslant i\leqslant K)$.

以上证明了 $\{E_i:1\leqslant i\leqslant K\}\cup\{E_{b,\chi}:b\in\mathbb{F}_q^\times,\chi\in(\mathbb{F}_q^\times)^\wedge\backslash\{\chi_0\}\}$ 是线性无关的. 这就完成了定理 4 的证明. □

参考文献

1 Klappenecker A, Rötteler M, Spharlinski I E, et al. On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states. J Math Phys, 2005, 46: 082104
2 Planat M, Rosu H C, Perrine S. A surey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements. Found Phys, 2006, 36: 1662–1680
3 Roy A, Scott A J. Weighted complex projective 2-designs from bases: optimal state determination by orthogonal meaurements. J Math Phys, 2007, 48: 072110
4 Renes J M, Blume-Kohout R, Scott A J, et al. Symmetric informationally complete quantum measurements. J Math Phys, 2004, 45: 2171
5 Renes J M. Equiangular spherical codes in quantum cryptography. Quantum Inf Comput, 2005, 5: 80–91
6 Zhu H J, Englert B G. Quantum state tomography with joint SIC POMs and product SIC POMs. ArXiv:quant-ph/1105.4561v1
7 Durt T, Emglert B G, Bengtsson I, et al. On mutually unbiased bases. Int J Quantum Inf, 2010, 8: 535–640
8 Godsil C, Roy A. Equianglar line, mutually unbiased bases and spin model. Euro J Combin, 2009, 30: 246–262
9 McConnell G, Gross D. Efficient 2-designs from bases exist. ArXiv:quant-ph/0717.1502vl
10 Belovs A, Smotrovs J. A criterion for attaining the Welch bounds with applications for mutually unbiased bases. Lect Notes Comput Sci, 2008, 5393: 50–69
11 Welch L R. Lower bounds on maximum cross correlation of signals. IEEE trans on Inf Theory, 1974, 20: 397–399
12 Chaturvedi S. Aspects of mutually unbiased bases in odd-prime-power dimensions. Phys Rev A, 2002, 65: 044301
13 Klappenecker A, Rötteler, M. Constructions of mutually unbiased bases. Lect Notes Comput Sci, 2004, 2948: 137–144
14 Planat M, Rosu H. Mutually unbiased phase states, phase uncertainties, and Gauss sums. Euro Phys J D, 2005, 36: 133–139
15 Wocjan P, Beth T. New construction of mutually unbiased bases in square dimensions. Quantum Inf Comput, 2005, 5: 93–101
16 Weiner M. A gap for the maximum number of mutually unbiased bases. ArXiv:math-ph/0902.0635v2
17 Grassl J M. On symmetric informationally complete positive operator-valued measures and mutually unbiased bases in dimension 6. ArXiv:quant-ph/0406175. Proc ERATO Conference on Quantum Information Science, EQIS2004, Tokyo, 2004, 60–61
18 Shparlinski I E, Winterhof A. Constructions of approximately mutually unbiased bases. Lect Notes Comput Sci, 2006, 3887: 793–799
19 Zauner G. Quantendesigns-Grundzüge einer nichkommutativen Designtheorie. PhD Thesis, Universität Wien, 1999
20 Scott A J, Grassl M. Symmetric informationally complete positive-operator-valued measures: a new computer study. J Math Phys, 2010, 51: 042203
21 Berndt B C, Evens R J, Williams K S. Gauss and Jacobi Sums. New York: Wiley-Interscience Pub, 1997
22 Caves C M, Fuchs C A, Schack R. Unknown quantum states: The quantum de Finetti representation. J Math Phys, 2002, 43: 4537

Constructions of approximately mutually unbiased bases and symmetric informationally complete positive operator-valued measures by Gauss and Jacobi sums

WANG WeiYang, ZHANG AiXian & FENG KeQin

Abstract Mutually unbiased bases (MUB) and symmetric informationally complete positive operator-valued measure (SIC-POVM) are both important objects in quantum information theory. While people do not know if there exists a complete MUB for non-prime-power dimension, several versions of approximately MUB have been considered by relaxed the inner product condition. So far there are only finite number of K such that SIC-POVMs in $\mathbb{C}^k$ have been found. As in the MUB case, several versions of approximately SIC-POVM have been considered by relaxed the inner product condition. In this paper, we use the definitions of approximate MUB and

SIC-POVM given by Klappenecker et al. For prime power q, we present simple constructions of q approximately MUB (AMUB) for dimension $q-1$, $q+1$ AMUB for dimension $q-1$, which shows the number of orthonormal bases of an AMUB in $\mathbb{C}^k$ can be more than $K+1$, and q AMUB for dimension $q+1$ by Gauss and Jacobi sums. We also present a construction of approximately SIC-POVM (ASIC-POVM) in dimension $q-1$ by Gauss sum.

Keywords **MUB, SIC-POVM, Gauss sum, Jacobi sum, complex spherical *t*-design**

MSC(2010) **81P15**

doi: 10.1360/012012-186