中国科学 : 数学　2017 年　第 47 卷　第 11 期 : 1387 ∼ 1408
SCIENTIA SINICA　Mathematica
综　述

量子信息理论中的几个数学问题

献给万哲先教授 90 华诞

冯克勤[1*]，金玲飞[2]

1. 清华大学数学科学系, 北京 100084;
2. 复旦大学计算机科学技术学院, 上海 201203
E-mail: kfeng@math.tsinghua.edu.cn, lfjin@fudan.edu.cn

收稿日期: 2016-09-12; 接受日期: 2016-11-29; 网络出版日期: 2017-04-18; * 通信作者
国家自然科学基金 (批准号: 11471178 和 11571007)、清华大学 “信息科学与技术” 国家重点实验室和上海市科委青年科技英才扬帆计划 (批准号: 15YF1401200) 资助项目

摘要　20 世纪 80 年代以来, 量子通信理论和技术成为信息领域的热门研究课题. 本文综述量子信息理论中一些数学问题的研究进展, 特别强调组合数学 (包括图论)、数论、代数学和代数几何 (有限域上代数曲线的算术理论) 在研究量子测量和量子纠错等问题中所起的作用.

关键词　乘积态　彼此无偏基　量子纠错码
MSC (2010) 主题分类　81P45, 11B75, 11T71

1　引言

20 世纪 60 年代以来, 由于数字通信和数字计算机的发展, 离散型数学 (包括组合学、图论、数论、代数和代数几何学) 成为通信领域的重要数学工具. 另一方面, 20 世纪 80 年代以来, 量子通信理论和技术成为信息领域的热门研究课题. 近年来, 这种以量子物理和量子力学为基础的新型通信和计算手段不仅在技术实现上取得快速进展, 并且在理论上不断有重要突破, 为它在量子通信和量子计算领域的应用展示出广泛的前景.

量子力学的数学基础是泛函分析和算子理论 (有限维 Hilbert 空间中的酉线性算子谱理论). 由于量子状态具有粒子 (离散性) 和波 (连续性) 的双重特性, 以及量子通信和经典的数字通信有着天然的联系, 离散型数学也已成为研究量子通信的数学工具. 本文将介绍量子通信中的某些数学问题, 以及组合数学、图论、数论、代数和代数几何在其中发挥的作用, 希望能引起更多人士的关注和研究兴趣.

限于篇幅和作者的知识所限, 我们挑选了量子通信中一部分重要问题, 它们有清晰的数学描述形式, 并且只需要少量的物理背景. 对于本文所需的量子通信基本概念只作简要的介绍, 详细内容可参见文献 [1]. 本文所需要的代数 (特别是有限域理论)、数论、图论、组合设计和代数编码理论等方面的知识可见参见文献 [2–7]. 本文涉及的每个课题都有大量的研究文献, 为节省篇幅, 这里只列出其中的一小部分文献.

英文引用格式: Feng K Q, Jin L F. Several mathematical problems in quantum information theory (in Chinese). Sci Sin Math, 2017, 47: 1387–1408, doi: 10.1360/N012016-00159

2 UPB (不可扩充的乘积态集合)

量子通信中的一个量子位 (qubit) 是 k 维复向量空间 $\mathbb{C}^k$ ($k \geqslant 2$) 中的一个非零向量, 在 $\mathbb{C}^k$ 中有 (Hermite) 内积: 对于 $|\boldsymbol{v}\rangle = (v_1, \ldots, v_k)$ 和 $|\boldsymbol{u}\rangle = (u_1, \ldots, u_k) \in \mathbb{C}^k$, 它们的内积定义为

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

其中 $\overline{u}_i$ 为 u_i 的复共轭. 在量子通信中, 彼此相差一个常数倍的两个向量 $|\boldsymbol{v}\rangle$ 和 $|\boldsymbol{u}\rangle$ (即 $|\boldsymbol{v}\rangle = \alpha|\boldsymbol{u}\rangle = (\alpha u_1, \ldots, \alpha u_k)$, α 为非零复数) 看作是相同的量子位, 所以, 量子位 $|\boldsymbol{v}\rangle$ 可以标准化为 $\langle \boldsymbol{v}|\boldsymbol{v}\rangle = 1$. 如果 $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = 0$, 称 $|\boldsymbol{v}\rangle$ 和 $|\boldsymbol{u}\rangle$ 是正交的. $\mathbb{C}^2$ 中的量子位称作 qubit.

一个量子状态 (quantum state) 是张量积空间 $V = \mathbb{C}^{k_1} \otimes \cdots \otimes \mathbb{C}^{k_m}$ 中的非零向量. V 为 $k_1 \cdots k_m$ 维复向量空间. 如果对每个 λ ($1 \leqslant \lambda \leqslant m$), 取 $\mathbb{C}^{k_\lambda}$ 的一组基 $\{v_\lambda^{(i)} : 1 \leqslant i \leqslant k_\lambda\}$, 则

$$\{v_1^{(i_1)} \otimes \cdots \otimes v_m^{(i_m)} : 1 \leqslant i_\lambda \leqslant k_\lambda, 1 \leqslant \lambda \leqslant m\} \tag{2.1}$$

便是 V 的一组基, 从而, V 中每个向量可唯一表示成

$$|\boldsymbol{v}\rangle = \sum_{1 \leqslant i_1 \leqslant k_1, \ldots, 1 \leqslant i_m \leqslant k_m} c_{i_1 \cdots i_m} v_1^{(i_1)} \otimes \cdots v_m^{(i_m)}, \quad c_{i_1 \cdots i_m} \in \mathbb{C}. \tag{2.2}$$

定义 1 V 中一个量子状态 $\boldsymbol{v}$ 称作乘积态 (product state), 是指它可以表示成 $\boldsymbol{v} = v_1 \otimes \cdots \otimes v_m$, 其中 $v_i \in \mathbb{C}^{k_i}$ ($1 \leqslant i \leqslant m$) ($\boldsymbol{v} \neq 0$ 相当于对每个 i, 有 $v_i \neq 0$).

每个量子态均可表示成有限个乘积态之和, 但是表达式不唯一, 其中表达式中乘积态的最少个数称作 $\boldsymbol{v}$ 的 Smith 数. 因此, 乘积态就是 Smith 数为 1 的量子态. Smith 数大于 1 的量子态会产生量子纠缠 (entanglement). 量子纠缠是量子通信中一个重要研究课题. 一方面, 它给量子测量造成诸多困难; 另一方面, 它又可用来构作量子密码.

例 1 设 v_1 和 v_2 表示 $\mathbb{C}^2$ 中的一组基, 考虑 $\mathbb{C}^2 \otimes \mathbb{C}^2$ 中的量子态

$$v_1 \otimes v_1 - v_1 \otimes v_2 + v_2 \otimes v_1 - v_2 \otimes v_2,$$

这是 4 个乘积态之和. 但是它为 $(v_1 + v_2) \otimes (v_1 - v_2)$, 其中 $v_1 \pm v_2 \in \mathbb{C}^2$, 从而, 它是乘积态.

两个乘积态 $\boldsymbol{v} = v_1 \otimes \cdots \otimes v_m$ 和 $\boldsymbol{u} = u_1 \otimes \cdots \otimes u_m (v_\lambda, u_\lambda \in \mathbb{C}^{k_\lambda})$ 的内积为

$$\langle \boldsymbol{u}|\boldsymbol{v}\rangle = \prod_{\lambda=1}^{m} \langle u_\lambda | v_\lambda \rangle,$$

从而 $\langle \boldsymbol{u}|\boldsymbol{v}\rangle = 0$ (即 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 正交) 当且仅当至少有一个 λ 使得 $\langle u_\lambda | v_\lambda \rangle = 0$ (即 u_λ 和 v_λ 正交).

由线性代数知, 对于 $k = k_1 \cdots k_m$ 维复向量空间 $V = \mathbb{C}^{k_1} \otimes \cdots \otimes \mathbb{C}^{k_m}$, 如果 $\{v^{(\lambda)} : 1 \leqslant \lambda \leqslant n\}$ 是 V 中彼此正交的量子态 (从而它们线性无关), 当 $n < k$ 时, 必可扩充成 V 的一组正交基, 即可找到 $v^{(\lambda)}$ ($n+1 \leqslant \lambda \leqslant k$), 使得 $\{v^{(\lambda)} : 1 \leqslant \lambda \leqslant k\}$ 为 V 的一组正交基. 但是, 在量子通信中, 为了避免量子纠缠的影响, 希望用彼此正交的一组乘积态进行测量. 问题在于, 如果 $\{v^{(\lambda)} : 1 \leqslant \lambda \leqslant n\}$ 是 V 的一组彼此正交的乘积态, 当 $n < k$ 时, 它不一定能扩大为更大的正交乘积态集合, 即由 $\{v^{(\lambda)} : 1 \leqslant \lambda \leqslant n\}$ 所张成的子空间的正交补空间 (维数 $k - n \geqslant 1$) 中不再有乘积态.

例 2 设 $V=\mathbb{C}^3\otimes\mathbb{C}^3$, 考虑 $\mathbb{C}^3$ 中 5 个向量

$$a_0=(0,1,2),\quad a_1=(1,0,0),\quad a_2=(0,1,1),\quad a_3=(1,1,-1),\quad a_4=(3,-2,1),$$

对每个 i $(0\leqslant i\leqslant 4)$, a_i 和 a_{i+1} 正交 (其中 $a_5=a_0$), 并且其中任 3 个向量均线性无关.

在图论中以 K_5 表示 5 个顶点 $A_0,\ldots,A_4$ 的完全图, 即任意两个不同顶点均有一条边相连. 将 K_5 的 10 条边分解成两个长为 5 的圈 G_1 和 G_2, 每个圈有 5 条边 (如图 1).

我们将图 G_1 的 5 个顶点赋以向量 $A_i=a_i$ $(0\leqslant i\leqslant 4)$, 则 G_1 中任意两个相邻顶点, 它们赋以的向量都是正交的. 同样地, 也把图 G_2 中 5 个顶点赋以如图 1(c) 所示的向量 ($A_0=a_0$, $A_2=a_1$, $A_4=a_2$, $A_1=a_3$, $A_3=a_4$), 则 G_2 中相邻顶点所赋以的向量也是正交的. 现在考虑 $V=\mathbb{C}^3\otimes\mathbb{C}^3$ 中如下 5 个乘积态:

$$v_0=a_0\otimes a_0,\quad v_1=a_1\otimes a_3,\quad v_2=a_2\otimes a_1,\quad v_3=a_3\otimes a_4,\quad v_4=a_4\otimes a_2,$$

即 $v_i=a\otimes a'$, 其中 a 和 a' 分别是顶点 A_i 在图 G_1 和 G_2 中所赋予的向量, 则这个乘积态是彼此正交的 (这是由于任意两个不同顶点 A_i 和 A_j, 它们在图 G_1 和 G_2 中必有边相连). 进而, 设乘积态 $v=b\otimes c$ 和这 5 个乘积态均正交 (其中 b 和 c 均为 $\mathbb{C}^3$ 中非零向量) $\langle v|v_i\rangle=0$ $(0\leqslant i\leqslant 4)$. 记 $v_i=b_i\otimes c_i$, 则 $\langle b|b_i\rangle\cdot\langle c|c_i\rangle=0$ $(0\leqslant i\leqslant 4)$. 由于 b_i $(0\leqslant i\leqslant 4)$ 中任意 3 个均线性无关, 即张成整个空间 $\mathbb{C}^3$. 从而, 当 $b\neq 0$ 时, b 至多和两个 b_i 正交, 同样地, c 也至多和两个 c_i 正交. 于是必有一个 i, 使得 $\langle b|b_i\rangle\neq 0$, $\langle c|c_i\rangle\neq 0$. 于是, $\langle v|v_i\rangle\neq 0$. 这表明, $\{v_0,\ldots,v_4\}$ 不能再扩大成 $\mathbb{C}^3\otimes\mathbb{C}^3$ 中的一组正交乘积态 (注意, $\mathbb{C}^3\otimes\mathbb{C}^3$ 的维数为 9).

定义 2 $V=\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$ 中彼此正交的一组乘积态 $\mathcal{B}=\{v_1,\ldots,v_d\}$ 称作不可扩充的 (unextendible product basis, 简记为 UPB), 是指 V 中不存在乘积态和 v_i $(1\leqslant i\leqslant d)$ 均正交. $d=|\mathcal{B}|$ 叫作 $\mathcal{B}$ 的体积.

例 2 中的 $\mathcal{B}=\{v_0,v_1,v_2,v_3,v_4\}$ 是 $\mathbb{C}^3\otimes\mathbb{C}^3$ 中的一个 UPB, 体积为 $|\mathcal{B}|=5$. 另一方面, 由 (2.1) 给出的 $\dim V=k=k_1\cdots k_m$ 一个乘积态为 UPB, 体积为 k (对于 $\mathbb{C}^3\otimes\mathbb{C}^3$, 体积为 9), 所以, V 中 UPB 的体积可以不同 (当 $|\mathcal{B}|<\dim V$ 时, $\mathcal{B}$ 并不是线性代数意义下的一组基, 物理界也把它称为 basis).

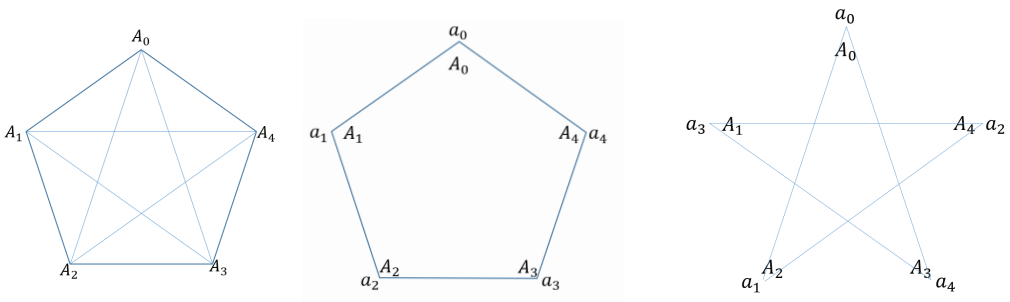
关于 UPB 的基本数学问题如下:

(I) 以 $f(k_1,\ldots,k_m)$ $(k_i\geqslant 2)$ 表示 $V=\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$ 中 UPB 的最小体积, 求它的值.

更一般地,

(II) 决定 V 中 UPB 所有可能的体积, 即决定集合 $S(k_1,\ldots,k_m)=\{|\mathcal{B}|:\mathcal{B}$ 为 V 的 UPB$\}$.

首先, 不难给出 $f(k_1,\ldots,k_m)$ 的上界和下界.



(a) (b) (c)

图 1 (a) 图 K_5; (b) 图 G_1; (c) 图 G_2

定理 1 设 $V=\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$ $(k_\lambda\geqslant 2)$, $n(k_1,\ldots,k_m)=1+\sum_{\lambda=1}^m(k_\lambda-1)$, 则

$$n(k_1,\ldots,k_m)\leqslant f(k_1,\ldots,k_m)\leqslant k_1\cdots k_m.$$

证明 上界是显然的, 因为每个 UPB 的体积不超过 $\dim V=k_1\cdots k_m$. 另一方面, 设 $\mathcal{B}=\{v_1,\ldots,v_d\}$ 是 V 中彼此正交的乘积态组, $v_i=v_i^{(1)}\otimes\ldots v_i^{(m)}$, $v_i^{(\lambda)}\in\mathbb{C}^{k_\lambda}$. 我们构作 $v^{(1)}\otimes\cdots\otimes v^{(m)}$, 使得非空向量 $v^{(1)}$ 和 k_1-1 个 v_i 的第 1 分量 $v_i^{(1)}$ 正交, 非零向量 $v^{(2)}$ 和另外 k_2-1 个 v_i 的第 2 分量 $v_i^{(2)}$ 均正交. 如此下去, 如果 $d\leqslant\sum_{\lambda=1}^m(k_{\lambda-1})$, 则得到非零乘积态 $v^{(1)}\otimes\cdots\otimes v^{(m)}$, 它和 $\mathcal{B}$ 中每个 v_i 均正交, 即 $\mathcal{B}$ 是可扩充的. 这就表明 V 的 UPB 至少包含 $\sum_{\lambda=1}^m(k_{\lambda-1})+1=n(k_1,\ldots,k_m)$ 个乘积态, 即 $f(k_1,\ldots,k_m)\geqslant n(k_1,\ldots,k_m)$. □

例 2 中 $(k_1,k_2)=(3,3)$, $n(3,3)=2+2+1=5$. 例 2 给出了 $\mathbb{C}^3\otimes\mathbb{C}^3$ 中达到下界的 5 个乘积态构成的 UPB.

著名组合学家 Alon 和 Lovász [8] 于 2001 年决定了 $f(k_1,\ldots,k_m)$ 等于下界的所有 $(k_1,\ldots,k_m)$.

定理 2 [8] 设 $m\geqslant 2$, $k_\lambda\geqslant 2$ $(1\leqslant\lambda\leqslant m)$, 则 $f(k_1,\ldots,k_m)=n(k_1,\ldots,k_m)$ 当且仅当下列两情形不成立:

(1) $m=2$, $(k_1,k_2)=(2,k)$;

(2) $(k_1,\ldots,k_m)\neq(2,k)$, $2\mid k_1\cdots k_m$, 并且 $n(k_1,\ldots,k_m)$ 是奇数.

定理 2 的证明利用了图的边染色和 k- 连通性的结果.

文献 [9–12] 讲述了 UPB 在量子通信中的意义, 其中文献 [9–11] 已经得到了达到下界的如下例子:

$$f(3,3)=5,\quad f(7,7)=13,\quad f(9,9)=17,\quad f(3,3,3)=7,$$

且有如下猜想: 若 p 为素数, $p\equiv 1\pmod 4$, $k=\frac{p+1}{2}$, 则 $f(k,k)=2k-1$. 这是定理 2 的特例, 不过文献 [8] 还是给出了 $\mathbb{C}^k\otimes\mathbb{C}^k$ 中体积为 $2k-1$ 的 UPB 明显的构作方式, 利用二次 Gauss 和的计算证明了乘积态的正交性, 利用分圆域 $\mathbb{Q}(\zeta_p)$ 为有理数域 $\mathbb{Q}$ 的 $p-1$ 次扩张证明了乘积态集合的不可扩张性, 这里 $\zeta_p=\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}}$ 是 p 次本原单位根.

2006 年, 文献 [13] 确定了 $f(k_1,\ldots,k_m)$ 达到上界 $k_1,\ldots,k_m$ 的所有情形.

定理 3 [13] 设 $m\geqslant 3$, $k_i\geqslant 2$ $(1\leqslant i\leqslant m)$, 则 $f(k_1,\ldots,k_m)=k_1\cdots k_m$ 当且仅当为定理 2(1), 即 $m=2$ 并且 $(k_1,k_2)=(2,k)$.

于是只剩下情形 (2), 即 $(k_1,\ldots,k_m)\neq(2,k)$, $2\mid k_1\cdots k_m$ 并且 $n(k_1,\ldots,k_m)=1+\sum_{i=1}^m(k_i-1)$ 为奇数. 对于情形 (2), 有 $f(k_1,\ldots,k_m)\geqslant 1+n(k_1,\ldots,k_m)$. 文献 [13] 证明了达到 $1+n(k_1,\ldots,k_m)$ 的一些情形.

定理 4 [13] (1) 对每个 $m\geqslant 0$, 有 $f(2^{[4m+2]})=4m+4$ (这里 $2^{[4m+2]}$ 表示 $4m+2$ 个 2);

(2) $f(2^{[4]})=6$, $f(2,2,3)=6$, $f(2^{[3]},4)=6$, $f(4,4)=8$, $f(2,2,5)=8$, $f(2^{[4]},5)=10$.

定理 4 的证明采用图论的另一种工具: 完全图的因子分解.

一个图 $G=(V,E)$ 称作 l 度正则图, 是指每个顶点均有 l 个邻点, 即每个顶点均恰有 l 条边与其他顶点相连. 例如, 一个 1 度正则图有 $2s$ 个定点, 而边集合 E 是互不相交的 s 条边. 2 度正则图是互不相交的一些圈.

图 $G=(X,E)$ 的一个分解是 G 的 m 个 (部分) 子图 $G_\lambda=(X,E_\lambda)$ $(1\leqslant\lambda\leqslant m)$, 其中每个图 G_λ 的顶点集合均是图 G 的顶点集合 X, 而边集合 $\{E_1,\ldots,E_m\}$ 为图 G 的边集合 E 的一个分拆, 即 $E_i\subset E$, 并且 E 中每条边恰好在某一个 E_i 之中. 如果 G_λ 为 l 度正则图, 则称 G_λ 为图 G 的一个 l- 因子. 如果 G_λ $(1\leqslant\lambda\leqslant m)$ 均是 G 的 l- 因子, 则称 $\{G_1,\ldots,G_m\}$ 为图 G 的一个 l- 因子分解.

设 $V=\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$, 考虑完全图 $K_d=(X,E)$ 的一个因子分解 $G_\lambda=(X,E_\lambda)$ $(1\leqslant\lambda\leqslant m)$, 其中 $X=\{v_1,\ldots,v_d\}$ 是它们的公共顶点集合. 对每个子图 G_λ, 将每个定点 v_i 赋以 $\mathbb{C}^{k\lambda}$ 中一个非零向量 $a_i^{(\lambda)}$. 称 $\{a_1^{(\lambda)},\ldots,a_d^{(\lambda)}\}$ 为图 G_λ 在 $\mathbb{C}^{k\lambda}$ 中的一个正交表示, 是指若 v_i 和 v_j 在图 G_λ 中有边, 则 $\langle a_i^{(\lambda)}|a_j^{(\lambda)}\rangle=0$ (即这两顶点赋以的向量是正交的).

现在考虑 $V=\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$ 中的乘积态集合 $\mathcal{B}=\{a_1,\ldots,a_d\}$, 其中

$$a_i=a_i^{(1)}\otimes\cdots\otimes a_i^{(m)},\quad 1\leqslant i\leqslant d. \tag{2.3}$$

定理 5 设 G_λ $(1\leqslant\lambda m)$ 为完全图 K_d 的一个因子分解, 对每个 λ, $\{a_1^{(\lambda)},\ldots,a_d^{(\lambda)}\}$ 是图 G_λ 在 $\mathbb{C}^{k\lambda}$ 中的正交表示, 则

(1) (2.3) 定义 d 个乘积态 a_i $(1\leqslant i\leqslant d)$ 彼此正交;

(2) 若对每个 λ, G_λ 的正交表示向量 $\{a_1^{(\lambda)},\ldots,a_d^{(\lambda)}\}$ 当中任意 n_λ 个均线性无关, 并且 $\sum_{\lambda=1}^m(n_\lambda-1)>d$, 则 $\mathcal{B}=\{v_1,\ldots,v_d\}$ 为 $V=\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$ 中的 UPB, 从而, $f(k_1,\ldots,k_m)\leqslant d$.

证明 (1) 对于两个乘积态

$$a_i=a_i^{(1)}\otimes\cdots\otimes a_i^{(m)},\quad a_j=a_j^{(1)}\otimes\cdots\otimes a_j^{(m)},$$

其中 $1\leqslant i\neq j\leqslant d$. 顶点 v_i 和 v_j 在某个 G_λ 中有边, 于是, $\langle a_i^{(\lambda)}|a_j^{(\lambda)}\rangle=0$, 从而, $\langle a_i|a_j\rangle=0$.

(2) 用例 2 中类似的推理可证明 $\mathcal{B}$ 是不可扩充的. □

例 2 关于 $f(3,3)=5$ 的证明就采用了定理 5 的方法: 将完全图 K_5 分解为 2- 因子 G_1 和 G_2, 它们有 $\mathbb{C}^3$ 中的正交表示, 并且 5 个表示向量当中任何 3 个均线性无关, 即 $n_1=n_2=3$. 从而, $(n_1-1)+(n_2-1)=4<d=5$, 因此, $\{v_1,\ldots,v_5\}$ 是 $\mathbb{C}^3\otimes\mathbb{C}^3$ 的 UPB, 于是, $f(3,3)\leqslant5$. 但是 $f(3,3)\geqslant n(3,3)=5$, 从而 $f(3,3)=5$.

采用完全图因子分解方法似乎比文献 [8] 中边染色和连通性方法更加有效, 我们可以利用完全图因子分解的大量研究结果 (参见文献 [14]). 例如, 为了证明定理 4 中的 $f(2^{4m+2})=4m+4$ $(\forall\, m\geqslant0)$, 就可用下面的已知结果.

引理 1 (参见文献 [15, 定理 1]) 设 G 是 $2s$ 个顶点的 d 度正则图, $s\geqslant3$, $0\leqslant d\leqslant4$, 则除了一个例外, G 在 K_{2s} 中的补图 $\bar{G}$ 具有 1- 因子分解. 这个例外为 $2s=6$, $d=3$, 而 $G=K_{3,3}$ (这时, $\bar{G}$ 为两个三角形 K_3 的非交并).

现在取 K_{4m+4} 的一个 2- 因子 G_1, 它由 $m+1$ 个长为 4 的圈组成, 正交表示见图 2, 其中 a_i 和 $a_i^\perp$ $(1\leqslant i\leqslant m+1)$ 为 $\mathbb{C}^2$ 中非零向量, a_i 和 $a_i^\perp$ 正交, 并且这 $2(m+1)$ 个向量的任何两个均线性无关. 根据引理 1 知, G_1 在 K_{4m+4} 中的补图 $\bar{G}$ 有 1- 因子分解, 考虑到 K_{4m+4} 为 $4m+3$ 度正则图, 边数为 $\binom{4m+3}{2}$, G_1 为 2 度正则图, 边数为 $4m+4$, 每个 1- 因子是 $2m+2$ 条彼此不相交的边, 因此, $\bar{G}_1$ 的 1- 因子个数为 $[\binom{4m+4}{2}-(4m+4)]/(2m+2)=4m+1$. 将 $\bar{G}_1$ 的这 $4m+1$ 个 1- 因子 $G_2,\ldots,G_{4m+2}$ 均作成如图 3 的正交表示, 其中 b_i, $b_i^\perp\in\mathbb{C}^2$ $(1\leqslant i\leqslant2m+2)$, b_i 和 $b_i^\perp$ 正交, 并且任意两个向量均线性无

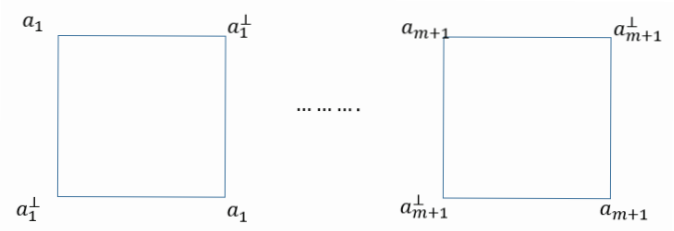


图 2 K_{4m+4} 的因子分解

图 3　$\bar{G}_1$ 的因子

关, 于是, $G_1,\dots,G_{4m+2}$ 是 K_{4m+4} 的因子分解, $n_1=n_2=\cdots=n_{4m+2}=2$, $\sum_{\lambda=1}^{4m+2}(n_\lambda-1)=4m+2<4m+4=d$, 由定理 5 给出 $f(2^{[4m+2]})\leqslant 4m+4=n(2^{[4m+2]})+1$, 但是, $f(2^{[4m+2]})\geqslant n(2^{[4m+2]})+1$, 于是, $f(2^{[4m+2]})=4m+4$.

最后再以 $f(2^{[4]})=6$ 为例, 以表明需要用 $\mathbb{C}^{k_1}\otimes\mathbb{C}^{k_2}$ 中的向量构作完全图因子的正交表示. 将 K_6 分解为因子 G_{12}、G_3 和 G_4, 其中 G_{12} 是 3 度正则图, G_3 和 G_4 是 2 度正则图. G_3 和 G_4 如前一样构作 $\mathbb{C}^2$ 中的正交表示, 而 G_{12} 用 $\mathbb{C}^2\otimes\mathbb{C}^2$ 中向量构作正交表示, 见图 4.

于是得到 $V=\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ 中一个正交乘积态集合 $\mathcal{B}=\{v_1,\dots,v_6\}$, 其中

$$
\begin{aligned}
v_1&=a_1\otimes a_1\otimes b_1\otimes b_1, \quad & v_4&=a_2\otimes a_1^{\perp}\otimes b_2^{\perp}\otimes b_3^{\perp},\\
v_2&=a_1^{\perp}\otimes a_2\otimes b_2\otimes b_2, \quad & v_5&=a_2^{\perp}\otimes a_2^{\perp}\otimes b_3^{\perp}\otimes b_1^{\perp},\\
v_3&=a_1\otimes a_1^{\perp}\otimes b_3\otimes b_3, \quad & v_6&=a_2\otimes a_1\otimes b_1^{\perp}\otimes b_2^{\perp}.
\end{aligned}
$$

不难验证, $\mathbb{C}^2\otimes\mathbb{C}^2$ 中每个非零乘积态 $u_1\otimes u_2$ 至多和 G_{12} 中顶点向量正交, 而 G_3 和 G_4 中任意两个向量均线性无关. 再由 $2+1+1=4<6$, 可知 $\mathcal{B}$ 是 V 中 UPB. 于是 $f(2^{[4]})\leqslant 6$, 再由 $f(2^{[4]})\geqslant 1+n(2^{[4]})=6$ 可得 $f(2^{[4]})=6$.

近来, 文献 [16,17] 采用完全图因子分解方法得到了如下结果.

(I) $f(2^{[m]})$ 完全解决. 已经知道当 $2\nmid m$ 时 $f(2^{[m]})=n(2^{[m]})=m+1$. 当 $m=4$ 或 $m\equiv 2\pmod 4$ 时, $f(2^{[m]})=n(2^{[m]})+1=m+2$. 文献 [17] 给出了 $f(2^{[8]})=2+n(2^{[8]})=11$, 而当 $m\equiv 0\pmod 4$ 时, $m\geqslant 12$, $f(2^{[m]})=m+4$.

(II) $f(k_1,k_2)$ 完全解决. 已经知道 $f(2,k)=2k$ $(k\geqslant 2)$, 当 $2\mid k_1k_2$ 且 $2\nmid k_1k_2-1=n(k_1,k_2)$ 时 (即 k_1 和 k_2 均偶), 文献 [17] 给出了 $f(k_1,k_2)=n(k_1,k_2)+1=k_1+k_2$. 其他情形已知 $f(k_1,k_2)=n(k_1,k_2)=k_1+k_2-1$.

文献 [16,17] 在构作因子 G_i 的正交表示时要用到代数几何, 但是推导似乎有值得商榷之处.

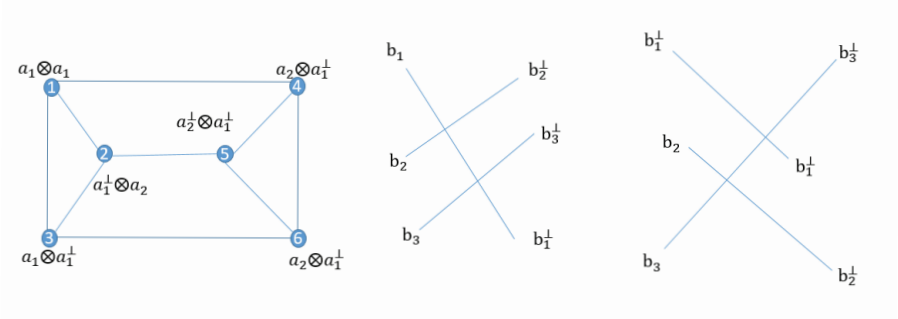


图 4　K_6 的因子

3 MUB 和 SIC-POVM

本节介绍的内容在数学上属于球面设计理论范围. 首先介绍球面设计的基本概念和问题, 以感受所介绍内容的数学难度 (关于复球面设计可参见文献 [18]). K 维复向量空间 $\mathbb{C}^K$ 中的所有单位向量组成的集合

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

称作 $K-1$ 维复球面. 我们要在其上寻找 N 个点 $C=\{v_1,\dots,v_N\}\subseteq S^{K-1}$, 其中 $N>K$, 使得任意两个 v_i 和 v_j $(1\leqslant i\neq j\leqslant N)$ 内积的绝对值 $|\langle v_i|v_j\rangle|$ 均很小. 首先要弄清它们能小到何种程度.

引理 2 设 $N>K$, $C=\{v_1,\dots,v_N\}\subseteq S^K$, 则对任意的正整数 k, 有

$$\sum_{\boldsymbol{u},\boldsymbol{v}\in C}|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{2k}\geqslant N^2\Big/\binom{K+k-1}{k}.$$

这相当于 $\{|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{2k}:\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}\}$ 的均值为

$$\frac{1}{N(N-1)}\sum_{\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}}|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{2k}\geqslant\frac{1}{N(N-1)}\left(N^2\Big/\binom{K+k-1}{k}-N\right).\tag{3.1}$$

例如, 当 $k=1$ 和 $k=2$ 时, 有

$$\frac{1}{N(N-1)}\sum_{\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}}|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{2}\geqslant\frac{N-K}{K(N-1)},\tag{3.2}$$

$$\frac{1}{N(N-1)}\sum_{\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}}|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{4}\geqslant\frac{2N-K(K+1)}{(N-1)K(K+1)}.\tag{3.3}$$

定义 3 C 称作球面 k- 设计, 是指 (3.1) 为等式. 进而令

$$\mathrm{Max}^{(k)}=\max\{|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{2k}:\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}\},$$

如果 $\mathrm{Max}^{(k)}$ 等于 (3.1) 的右边, 这也相当于对 C 中的任意两个不同的单位向量 $\boldsymbol{u}$ 和 $\boldsymbol{v}$, $|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^{2k}$ 均等于 (3.1) 的右边. 这时称 C 为球面 S^{K-1} 上的 tight k- 设计 (在大数据压缩感知和存储理论中, 这称作 tight frame).

可以证明, 对于 $t\geqslant 2$, 如果 C 是球面 tight t- 设计, 则 C 也是球面 tight $(t-1)$- 设计. 构作球面 1- 设计和球面 tight 1- 设计不太困难, 构作球面 2- 设计, 特别是球面 tight 2- 设计则要困难很多. 历史上, 球面 t- 设计来源于球面上的数值积分计算.

定理 6 设 $C=\{v_1,\dots,v_N\}\subseteq S^{K-1}$, 则对每个次数 $\leqslant t$ 的复系数多项式 $f(\zeta_1,\dots,\zeta_K)=f(\zeta)\in\mathbb{C}[\zeta_1,\dots,\zeta_K]$, 均有

$$\int_{S^{K-1}}f(\zeta)d\sigma_K=\Delta_K\cdot\frac{1}{N}\sum_{i=1}^{N}f(v_i),$$

当且仅当 C 是 S^{K-1} 上的球面 tight t- 设计 (其中 σ_K 为 S^{K-1} 上的体积元, $\Delta_K=\int_{S^{K-1}}d\sigma_K$ 为 S^{K-1} 的体积).

构作球面 tight 1- 设计的一个有效方法是利用有限交换群的差集合. 设 G 是 v 阶有限加法交换群. G 的一个 k 元子集 $D=\{g_1,\dots,g_k\}$ 称作参数 (v,k,λ) 的差集合, 是指每个 G 中的非零元素 a,

都恰有 λ 种方式表达成 $g-g'$, 其中 g 和 g' 为 D 中不同的元素. 令 $\widehat{G}$ 为 G 的特征群, 对每个特征 $\chi\in\widehat{G}$, 向量

$$v_\chi=\frac{1}{\sqrt{k}}(\chi(g_1),\dots,\chi(g_k))$$

是 $\mathbb{C}^k$ 中的单位向量. 利用特征的正交关系和差集合参数关系 $k(k-1)=\lambda(v-1)$, 可以证明对任意两个不同的特征 χ 和 χ', 有 $|\langle v_\chi|v_{\chi'}\rangle|^2=\frac{v-k}{(v-1)k}$, 即 $C=\{v_\chi:\chi\in\widehat{G}\}$ 是球面 S^{k-1} 上的 tight 1- 设计 $(N=|C|=v)$.

现在要介绍量子通信中的两个问题均是球面 2- 设计.

$\mathbb{C}^K$ 的一组标准正交基 $\{v_1,\dots,v_K\}$ 是指它们为彼此正交的单位向量. 设 $\mathbb{B}=\{B_1,\dots,B_\ell\}$, $\ell\geqslant 2$, 其中每个 B_i 均为 $\mathbb{C}^K$ 的一组标准正交基. 称 $\mathbb{B}$ 是无偏的标准正交基组, 是指存在常数 α (正实数), 使得不同基中的任意两个向量 $v_i\in B_i$ 和 $v_j\in B_j$ $(1\leqslant i\neq j\leqslant\ell)$, 均有 $|\langle v_i|v_j\rangle|=\alpha$. 考虑这 ℓ 个基的并集 $C=\bigcup_{i=1}^{\ell}B_i$, $N=|D|=\ell K$. 由 (3.2) 可知,

$$\frac{\ell K-K}{(\ell K-1)K}\leqslant\frac{1}{\ell K(\ell k-1)}\sum_{\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}}|\langle\boldsymbol{u}|\boldsymbol{v}\rangle|^2=\frac{1}{\ell K(\ell k-1)}\ell(\ell-1)K^2\alpha^2=\frac{(\ell-1)K\alpha^2}{(\ell K-1)}.$$

因此, $\alpha\geqslant\frac{1}{\sqrt{K}}$. 现在取 $\alpha=\frac{1}{\sqrt{K}}$, 再由 (3.3) 给出

$$\frac{2K\ell-K(K+1)}{(\ell K-1)K(K+1)}\leqslant\frac{\ell(\ell-1)K^2\alpha^4}{(\ell K-1)\ell K}=\frac{\ell-1}{(\ell K-1)K},$$

可得 $\ell\leqslant K+1$.

定义 4 设 B_i $(1\leqslant i\leqslant\ell)$ 是 $\mathbb{C}^K$ 的 ℓ 个标准正交基. $\mathbb{B}=\{B_1,\dots,B_\ell\}$ 称作 $\mathbb{C}^K$ 的彼此无偏基组 (mutually unbiased bases, MUB), 是指对任意两个不同基中的 (单位) 向量 $\boldsymbol{v}_i\in B_i$ 和 $\boldsymbol{v}_j\in B_j$ $(1\leqslant i\neq j\leqslant\ell)$, 均有 $|\langle\boldsymbol{v}_i|\boldsymbol{v}_j\rangle|=\frac{1}{\sqrt{K}}$. $\mathbb{B}$ 中 ℓK 个向量是一类特殊的球面 2- 设计.

以 $f(K)$ 表示 $\mathbb{C}^K$ 中的所有 MUB 的最大体积 ℓ. 由上述知 $f(K)\leqslant K+1$. 当 $f(K)=K+1$ 时, 体积为 $K+1$ 的 MUB$\{B_1,\dots,B_{K+1}\}$ 称作完备 (complete) MUB.

MUB 的基本问题为, 对每个正整数 $K\geqslant 2$, 决定 $f(K)$ 的值. 下面是目前已得到的主要结果.

(1) 若 $K=p^m$ 为素数 p 的方次幂 $(m\geqslant 1)$, 则 $f(K)=K+1$, 即 $\mathbb{C}^K$ 中存在完备 MUB. 文献 [19] 给出了代数构作方式. 先设 $p\geqslant 3$ (奇素数), 我们有 $K=p^m$ 元有限域 $\mathbb{F}_K=\{x_1,\dots,x_K\}$. 记 $T:\mathbb{F}_K\to\mathbb{F}_p$ 为有限域的迹 (trace) 映射. 对于 $a,b\in\mathbb{F}_K$, 我们有 $\mathbb{C}^K$ 中的单位向量

$$v_{a,b}=\frac{1}{\sqrt{K}}(\zeta_p^{T(ax_1^2+bx_1)},\dots,\zeta_p^{T(ax_K^2+bx_K)}),\quad\zeta_p=\mathrm{e}^{\frac{2\pi\sqrt{-1}}{p}}.$$

不难验证, 对于每个 $a\in\mathbb{F}_K$, $\mathcal{B}_a=\{v_{a,b}:b\in\mathbb{F}_K\}$ 均是 $\mathbb{C}^K$ 的标准正交基, 即当 $b\neq b'$ 时, $\langle v_{a,b}|v_{a,b'}\rangle=0$. 此外还有标准正交基 $\mathcal{B}^*=\{e_1,\dots,e_K\}$, 其中 $e_1=(1,0,\dots,0)$, $e_2=(0,1,0,\dots,0),\dots,e_k=(0,0,\dots,1)$.

当 $v_{a,b}\in\mathcal{B}_a$, $e_i\in\mathcal{B}^*$ 时, 易知 $\langle v_{a,b}|e_i\rangle=\frac{1}{\sqrt{K}}$. 对于 $v_{a,b}\in\mathcal{B}_a$ 和 $v_{a',b'}\in\mathcal{B}_{a'}$ $(a'\neq a)$, 利用有限域 $\mathbb{F}_K$ 中关于二次乘法特征 η 的 Gauss 和计算公式可知, $\langle v_{a,b}|v_{a',b'}\rangle=\frac{1}{\sqrt{K}}$. 这就表明 $\mathcal{B}=\{\mathcal{B}_a:a\in\mathbb{F}_K\}\cup\{\mathcal{B}^*\}$ 是 $\mathbb{C}^K$ 的一个完备 MUB. 当 $p=2$ 时, 要用 Galois 环 $\mathrm{GR}(4,m)$ 来构作 $\mathbb{C}^{2^m}$ 中的完备 MUB.

对于 $K\neq p^m$ 的情形, 目前没有决定出任何一个 $f(K)$ 的值. 人们猜想对于 $K\neq p^m$, $\mathbb{C}^K$ 中均不存在完备 MUB, 即 $f(K)\leqslant K$. 已知如下结果:

(2) 若 $K=K_1K_2$, 其中 $K_1,K_2\geqslant 2$, 则 $f(K)\geqslant \min\{f(K_1),f(K_2)\}$. 证明采用张量积构作方法. 于是, 若 $2\leqslant K=p_1^{a_1}\cdots p_s^{a_s}$, 其中 $p_1,\ldots,p_s$ 为不同素数, $a_1,\ldots,a_s\geqslant 1$, $s\geqslant 1$, 则

$$f(K)\geqslant \min\{f(p_1^{a_1}),\ldots,f(p_s^{a_s})\}=\min\{p_1^{a_1}+1,\ldots,p_s^{a_s}+1\}\geqslant 3,$$

即对每个 $K\geqslant 2$, 均有 $f(K)\geqslant 3$. 猜想 $f(6)=3$, 但是至今未能解决.

(3) $f(K^2)\geqslant L(K)+2$, 其中 $L(K)$ 为 K ($\geqslant 2$) 阶正交 Latin 方的最大个数. 由此可知对某些 m (例如, $m=6$), 有 $f((4m+2)^2)=6$.

(4) $f(K)\neq K$, 即若 $f(K)\neq K+1$, 则 $f(K)\leqslant K-1$.

由于 $K\neq p^m$ 时结果甚少, 人们也研究 "近似 MUB", 参见文献 [20,21].

现在介绍量子通信中的第二个问题.

$\mathbb{C}^K$ 中 N 个单位向量 $\mathcal{B}=\{v_1,\ldots,v_N\}$ 称作 tight frame (在代数组合学中也称作 equiangular lines), 是指 $N>K$, 并且存在正实数 α, 使得当 $1\leqslant i\neq j\leqslant N$ 时, $|\langle v_i|v_j\rangle|=\alpha$. 在量子测量中希望 $\alpha=\frac{1}{\sqrt{K+1}}$. 这时由 (3.2) 知, $\frac{1}{K+1}=\alpha^2\geqslant\frac{N-K}{(N-1)K}$, 即 $N\leqslant K^2$. 当 $N=K^2$ 时, 可验证 (3.3) 为等式. 从而, $\mathcal{B}$ 是球面 $\mathbb{C}^K$ 上的 tight 2- 设计.

定义 5 设 $K\geqslant 2$, $\mathbb{C}^K$ 中 K^2 个单位向量组成的集合 $\mathcal{B}=\{v_1,\ldots,v_{K^2}\}$ 称作 SIC-POVM (symmetric informationally complete positive operator-valued measure), 是指当 $1\leqslant i\neq j\leqslant K^2$ 时, $|\langle v_i|v_j\rangle|=\frac{1}{\sqrt{K+1}}$.

1999 年, Zauner [22] 在他的博士论文中提出了如下的猜想.

对每个 $K\geqslant 2$, $\mathbb{C}^K$ 中均存在 SIC-POVM.

事实上, Zauner [22] 还提出了更强的猜想.

猜想 1 (Zauner 强猜想) 对每个 $K\geqslant 2$, $\mathbb{C}^K$ 中均存在一个单位向量 (称作 fiducial state) $v=(v_0,\ldots,v_{K-1})$, 使得下面 K^2 个单位向量构成 $\mathbb{C}^K$ 中的 SIC-POVM:

$$v_{ij}=(v_i,v_{i+1}\varsigma_K^j,v_{i+2}\varsigma_K^{ij},\ldots,v_{i+K-1}\varsigma_K^{(K-1)j}),\quad 0\leqslant i,j\leqslant K-1,$$

其中 $\varsigma_K=\mathrm{e}^{\frac{2\pi\sqrt{-1}}{K}}$, 而对 $0\leqslant l\leqslant K-1$, 有 $v_{l+K}=v_l$.

至今为止, 对于 $K=2,3,4,5,6,7,8,9,10,11,12,13,15,19$, 研究者均证明了 Zauner 强猜想是正确的, 文献 [23] 通过上机计算, 显示出对于 $K\leqslant 67$ 都支持 Zauner 强猜想的正确性. 这里举 $K=2,3,4$ 作为例子.

对于 $K=2$, 可取 $v=\frac{1}{\sqrt{6}}(\sqrt{3+\sqrt{3}},\varsigma_8\sqrt{3-\sqrt{3}})=(v_0,v_1)$ 为 fiducial state, 即 $(v_0,\pm v_1)$ 和 $(v_1,\pm v_0)$ 这 4 个单位向量构成 $\mathbb{C}^2$ 中的一个 SIC-POVM.

对于 $K=3$, 可取 $v=(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$ 为 fiducial state, 即

$$\begin{array}{lll}
\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right), & \left(\frac{1}{\sqrt{2}},\varsigma_3\frac{1}{\sqrt{2}},0\right), & \left(\frac{1}{\sqrt{2}},\varsigma_3^2\frac{1}{\sqrt{2}},0\right),\\
\left(0,\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}\right), & \left(0,\varsigma_3\frac{1}{\sqrt{2}},\varsigma_3^2\frac{1}{\sqrt{2}}\right), & \left(0,\varsigma_3^2\frac{1}{\sqrt{2}},\varsigma_3\frac{1}{\sqrt{2}}\right),\\
\left(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}}\right), & \left(\frac{1}{\sqrt{2}},0,\varsigma_3^2\frac{1}{\sqrt{2}}\right), & \left(\frac{1}{\sqrt{2}},0,\varsigma_3\frac{1}{\sqrt{2}}\right)
\end{array}$$

构成 $\mathbb{C}^3$ 中一个 SIC-POVM.

对于 $K=4$, $v=(r_0, r_+\mathrm{e}^{\mathrm{i}\theta_+}, \mathrm{i}r_1, r_-\mathrm{e}^{\mathrm{i}\theta_-})$ 是 $\mathbb{C}^4$ 中一个 fiducial state, 其中

$$r_0=\frac{1-\frac{1}{\sqrt{5}}}{2\sqrt{2-\sqrt{2}}},\quad r_1=(\sqrt{2}-1)r_0,$$
$$r_\pm=\frac{1}{2}\sqrt{1+\frac{1}{\sqrt{5}}\pm\sqrt{\frac{1}{5}+\frac{1}{\sqrt{5}}}},$$

而 $\theta_\pm=\pm\frac{\alpha}{2}+\frac{\beta}{4}+\frac{\pi}{4}$, 其中 α 和 β 由 $0\leqslant\alpha,\beta\leqslant 2\pi$, $\cos\alpha=\frac{2}{\sqrt{5+\sqrt{5}}}$, $\sin\beta=\frac{2}{\sqrt{5}}$ 所决定.

如果 $\mathbb{C}^K$ 中存在 fiducial state, 不难看到它的坐标是有理数域上一些代数方程组的解, 从而都是代数数. 它们属于哪个代数数域似乎是一个很大的秘密. 此外, 由于这个问题似乎相当困难, 人们也找到相对容易的方法构作 "近似" 的 SIC-POVM, 参见文献 [21, 24].

4 量子纠错码

与数字通信情形一样, 纠错问题是量子通信和量子计算得以实现的必要保障之一. 1995 年以前, 人们普遍认为解决量子纠错问题比数字通信纠错要困难许多, 这是由于量子物理的特殊通信机制造成的 (不可复制性、测量与环境的相互影响、纠缠态、量子态的连续性等). 但是在 1995–1996 年, 量子纠错在物理方面取得重要突破, Shor 和 Steane 在物理上把复杂的纠缠态错误归结和简化为只需考虑在每个量子位上独自产生的三种类型错误 (即 Pauli 错误算子 σ_x、σ_z 和 $\sigma_y=\mathrm{i}\sigma_x\sigma_z$). 基于此, Shor 构作出了世界上第一个量子纠错码 $[[9,1,3]]$, 用 9 个量子位的码可以纠正任何一位的任何量子错误, 码空间为 2 维复空间. 不久人们把所需的 9 位码长减至最佳可能的 5 位. 1998 年, Calderbank、Rain、Shor 和 Sloane 等给出了量子码理论的数学形式, 并且给出了构作量子码的第一种系统而有效的数学方法, 并由此建立了经典纠错码与量子纠错码之间的联系. 此后量子纠错码的数学理论得到快速发展. 关于量子纠错码在 2010 年以前的工作可参见文献 [25] 中所列文献.

为简单起见, 我们先介绍二元 (binary) 量子纠错码的纠错机制, 并且与经典二元纠错码加以比较. 如第 1 节中所述, 一个量子位 (qubit) 为 $\mathbb{C}^2$ 中的非零向量, 固定 $\mathbb{C}^2$ 中的一组标准正交基 $|0\rangle$ 和 $|1\rangle$, 则每个量子位唯一表示成

$$|v\rangle=\alpha|0\rangle+\beta|1\rangle,\quad \alpha,\beta\in\mathbb{C}^2,\quad (\alpha,\beta)\neq(0,0).$$

一个量子状态 (n-qubit) 是 n 个 $\mathbb{C}^2$ 的张量积 $(\mathbb{C}^2)^{\otimes n}\cong\mathbb{C}^{2^n}$ 中的非零向量. 这个空间有如下一组标准正交基:

$$|a_1\rangle\otimes|a_2\rangle\otimes\cdots\otimes|a_n\rangle,\quad a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n,\quad \mathbb{F}_2=\{0,1\}.$$

上述向量以后简记成 $|a_1\cdots a_n\rangle$ 或者 $|a\rangle$. 于是, 每个 n- 量子态可唯一表示成

$$|v\rangle=\sum_{a\in\mathbb{F}_2^n}c(a)|a\rangle,$$

其中 $c(a)\in\mathbb{C}$, 不全为零.

例如, 当 $n=2$ 时, $|v\rangle=\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle=\alpha|0\rangle\otimes|0\rangle+\beta|0\rangle\otimes|1\rangle+\gamma|1\rangle\otimes|0\rangle+\delta|1\rangle\otimes|1\rangle$, 其中 $\alpha,\beta,\gamma,\delta\in\mathbb{C}$, 且不全为零.

在数字通信中, 一个位 (bit) 为二元域 $\mathbb{F}_2$ 中的 0 或 1, 而一个状态为 $\mathbb{F}_2^n$ 中的向量 $c=(c_1,\dots,c_n)$. 如果信道出现 l 位错, 相当于 c 加上一个 Hamming 重量 $w_H(\epsilon)$ 为 l 的错误向量. 例如, $c=(1011)$, $\epsilon=(0101)$, $w_H(\epsilon)=2$ (即 ϵ 有两个分量为 1), 则 $c+\epsilon=(1110)$, 即 c 的第二和四位出错. 在量子通信中, 量子错误是一个酉 (unitary) 算子的作用. 每个量子位上共有三种量子错误 σ_x、σ_y 和 σ_z, 它们表示成二阶酉方阵:

$$\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad \sigma_y=\mathrm{i}\sigma_x\sigma_z=\begin{pmatrix}0&\mathrm{i}\\-\mathrm{i}&0\end{pmatrix},$$

σ_x 和 σ_z 分别为位错和相错. 它们不仅是酉阵 ($AA^{-\mathrm{T}}=I_2$), 也是 Hermite 阵 ($A^{-\mathrm{T}}=A$). 它们对于量子位 $|v\rangle=\alpha|0\rangle+\beta|1\rangle$ 的作用为

$$\sigma_x|v\rangle=\beta|0\rangle+\alpha|1\rangle,\quad \text{即}\quad \sigma_x\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}\beta\\\alpha\end{pmatrix},$$

$$\sigma_z|v\rangle=\alpha|0\rangle-\beta|1\rangle,\quad \text{即}\quad \sigma_z\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}\alpha\\-\beta\end{pmatrix},$$

$$\sigma_y|v\rangle=-\mathrm{i}\beta|0\rangle+\mathrm{i}\alpha|1\rangle,\quad \text{即}\quad \sigma_y\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}=\begin{pmatrix}-\mathrm{i}\beta\\\mathrm{i}\alpha\end{pmatrix}.$$

特别地,

$$\sigma_x|0\rangle=|1\rangle,\quad \sigma_x|1\rangle=|0\rangle,\quad \sigma_z|0\rangle=|0\rangle,\quad \sigma_z|1\rangle=-|1\rangle.$$

这可以表示成

$$\sigma_x|a\rangle=|a+1\rangle,\quad \sigma_z|a\rangle=(-1)^a|a\rangle.$$

错误算子 σ_x、σ_z 和 σ_y 之间有如下的关系:

$$\sigma_x^2=\sigma_z^2=\sigma_y^2=I_2,\quad \sigma_x\sigma_z=-\sigma_z\sigma_x,$$

其中 $I_2=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ 代表不产生错误. 在量子态空间 $V=(\mathbb{C}^2)^{\otimes n}$ 上每个量子错误有形式

$$\epsilon=\mathrm{i}^\lambda\omega_1\otimes\omega_2\otimes\cdots\otimes\omega_n,$$

其中 $0\leqslant\lambda\leqslant 3$, $\mathrm{i}=\sqrt{-1}$, $\omega_i\in\{\sigma_x,\sigma_y,\sigma_z,I_2\}$ $(1\leqslant i\leqslant n)$. 它在每个量子位上分别作用 ω_i, 即对于 V 的基向量 $|a\rangle=|a_1\cdots a_n\rangle=|a_1\rangle\otimes\cdots\otimes|a_n\rangle$ $(a=(a_1,\dots,a_n)\in\mathbb{F}_2^n)$, e 的作用为

$$e|a\rangle=\mathrm{i}^\lambda(\omega_1|a_1\rangle)\otimes(\omega_2|a_2\rangle)\otimes\cdots\otimes(\omega_n|a_n\rangle).$$

从而, 对 V 中任意量子态 $|v\rangle=\sum_{a\in\mathbb{F}_2^n}c(a)|a\rangle$ $(c(a)\in\mathbb{C})$, 有

$$e|v\rangle=\sum_{a\in\mathbb{F}_2^n}c(a)(e|a\rangle)$$

所有错误算子组合的集合

$$E_n=\{\mathrm{i}^\lambda\omega_1\otimes\cdots\otimes\omega_n\mid 0\leqslant\lambda\leqslant 3,\omega_i\in\{I,\sigma_x,\sigma_y,\sigma_z\}\}$$

形成乘法群, 称作错误算子群, 其中 $e=\mathrm{i}^{\lambda}\omega_1\otimes\cdots\otimes\omega_n$ 和 $e'=\mathrm{i}^{\mu}\omega_1'\otimes\cdots\otimes\omega_n'$ 的乘积自然定义为

$$ee'=\mathrm{i}^{\lambda+\mu}(\omega_1\omega_1')\otimes\cdots\otimes(\omega_n\omega_n'),$$

E_n 是 4^{n+1} 阶非交换群. ee' 为 $e'e$ 或者 $-ee'$. 为了决定正负号, 我们给出错误算子的另一种表达方式. 对于 $a=(a_1,\ldots,a_n)$, $b=(b_1,\ldots,b_n)\in\mathbb{F}_2^n$, 定义

$$X(a)=\omega_1\otimes\cdots\otimes\omega_n,\quad Z(b)=\omega_1'\otimes\cdots\otimes\omega_n',$$

其中

$$\omega_i=\begin{cases}I_2, & a_i=0,\\ \sigma_x, & a_i=1,\end{cases}\qquad \omega_i'=\begin{cases}I_2, & b_i=0,\\ \sigma_z, & b_i=1.\end{cases}$$

引理 3 (1) E_n 中每个错误算子都可表示成 $e=\mathrm{i}^{\lambda}X(a)Z(b)$, 并且 $E_n=\{\mathrm{i}^{\lambda}X(a)Z(b):0\leqslant\lambda\leqslant 3,\ a,b\in\mathbb{F}_2^n\}$;

(2) $X(a)$ 和 $Z(b)$ 在 V 的基向量 $|v\rangle=|v_1\cdots v_n\rangle$ $(v=(v_1,\ldots,v_n)\in\mathbb{F}_2^n)$ 上的作用为

$$X(a)|v\rangle=|a+v\rangle,\quad Z(b)|v\rangle=(-1)^{(b,v)}|v\rangle,$$

其中 (b,v) 表示 $\mathbb{F}_2^n$ 中的内积 $\sum_{i=1}^n b_iv_i\in\mathbb{F}_2$.

(3) 对于 $e=\mathrm{i}^{\lambda}X(a)Z(b)$ 和 $e'=\mathrm{i}^{\mu}X(a')Z(b')$, 有

$$ee'=(-1)^{(a,b')+(a',b)}ee'.$$

从而, e 和 e' 可交换, 当且仅当

$$(a,b')+(a',b)=(a,a')\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}\begin{pmatrix}b\\ b'\end{pmatrix}=0\in\mathbb{F}_2.$$

映射 $\varphi:E_n\to\mathbb{F}_2^{2n}$, $e=\mathrm{i}^{\lambda}X(a)Z(b)\mapsto(a|b)=\varphi(e)$ 是 E_n 到加法群 $\mathbb{F}_2^{2n}$ 的满同态, 核为 $\{\pm1,\pm i\}$. 从而诱导出群同构

$$\overline{\varphi}:\overline{E_n}=E_n/(\{\pm1,\pm\mathrm{i}\})\mapsto\mathbb{F}_2^{2n},\quad \overline{\varphi}(\overline{e})=\varphi(e)=(a|b),$$

而群 E_n 是初级 2- 群 (即每个元素的平方均为 I).

我们在 $\mathbb{F}_2^{2n}$ 中引入辛 (symplectic) 内积:

$$((a|b),(a'|b))_s=(a,b)\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}\begin{pmatrix}a'\\ b'\end{pmatrix}=(a,b')+(a',b),$$

则引理 3 是说, $e=\mathrm{i}^{\lambda}X(a)Z(b)$ 和 $e'=\mathrm{i}^{\mu}X(a')Z(b')$ 可交换, 当且仅当 $\overline{e}=(a|b)$ 和 $\overline{e}'=(a'|b')$ 是辛正交的, 即 $(\overline{e},\overline{e}')_s=0$

对于 $\mathbb{F}_2^n$ 的每个向量子空间 C, 以 $C^{\perp_s}$ 表示它的辛对偶向量空间, 即

$$C^{\perp_s}=\{v\in\mathbb{F}_2^{2n}:\forall\, c\in C,(v,c)_s=0\},$$

我们有 $\dim C+\dim C^{\perp_s}=\dim\mathbb{F}_2^n=2n$. 如果 $C\subseteq C^{\perp_s}$, 则称 C 是辛自正交的. 若 $C=C^{\perp_s}$, 则称 C 是辛自对偶空间. 由引理 3 可知, E_n 的一个子群 G 是交换群, 当且仅当 $\overline{G}$ 是 $\mathbb{F}_2^{2n}$ 的辛自正交空间. 这个事实是今后构作加性量子码的出发点.

错误算子 $e = \mathrm{i}^\lambda \omega_1 \otimes \cdots \otimes \omega_n$ 作用到量子态上, 如果 $\omega_i \in \{\sigma_x, \sigma_y, \sigma_z\}$, 那么量子态第 i 位产生错误. 若 $\omega_i = I_2$, 则第 i 位不发生错误. 形式上, 很自然地引入如下的量子重量 W_Q 的定义. 对于 $e = \mathrm{i}^\lambda X(a)Z(b)$, $\bar{e} = (a|b)$, $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n) \in \mathbb{F}_2^n$, 定义 e 和 $\bar{e}$ 的量子重量 (quantum weight) 为

$$W_Q(e) = W_Q(\bar{e}) = W_Q(a|b) = \#\{i : 1 \leqslant i \leqslant n \ (a_i, b_i) \neq (0,0)\} = \#\{i : 1 \leqslant i \leqslant n, w_i \neq I_2\},$$

则 e 恰好在 $W_Q(e)$ 个量子位发生错误 (σ_x、σ_z 或者 σ_y, 分别对应于 $(a_i, b_i) = (1,0)$, $(a_i, b_i) = (0,1)$, $(a_i, b_i) = (1,1)$).

现在可以给出量子 (纠错) 码的定义.

定义 6 码长为 n 的一个量子 (纠错) 码 Q 是 $V = (\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$ 的一个向量子空间, 并且 $K = \dim Q \geqslant 1$.

我们需要量子码 Q 具有好的纠错能力. 在数字通信中, 一个纠错码 C ($|C| \geqslant 2$) 是 $\mathbb{F}_2^n$ 的子集合. 这个纠错码可以纠正 $\leqslant l$ 位的错误, 是指当码字 $c \in C$ 出现 $\leqslant l$ 位错误成为 $c + \epsilon$ 时 ($\epsilon \in \mathbb{F}_2^n$, $W_H(\epsilon) \leqslant l$), 它都不会是另一个码字 $c' \in C$ ($c \neq c'$) 出现 $\leqslant l$ 位错误 $c + \epsilon'$ ($\epsilon' \in \mathbb{F}_2^n, W_H(\epsilon') \leqslant l$). 也就是说, 收到的 $c + \epsilon$ 只与唯一的码字 c Hamming 距离 $d_H(c, c+\epsilon) = W_H(\epsilon)$ 小于 l, 而与其他码字 c' 的 Hamming 距离 $d_H(c', c+\epsilon)$ 都大于 l. 然后将 $c + \epsilon$ 译成 c 便纠正错误. 如果码 C 的最小距离 $d \geqslant 2l + 1$, 由于 Hamming 距离有性质 $d_H(c, c') \leqslant d_H(c, v) + d_H(v, c')$, 可知 C 必可纠正 l 位错误. 类似地, 对于 $0 \leqslant l \leqslant n$, 令

$$E_l = \{e \in E_n : W_Q(e) \leqslant l\}, \quad \overline{E}_l = \{\bar{e} \in \overline{E}_n : W_Q(\bar{e}) \leqslant l\},$$

它们表示量子重量不超过 l 的所有错误算子构成的集合. 一个量子码 Q 称作可以纠正 $\leqslant l$ 位量子错误, 是指对 Q 中任意两个量子态 $|v\rangle$ 和 $|v'\rangle$, 如果它们 "完全可区分的", 即它们正交 $\langle v|v'\rangle = 0$, 则对任意量子重量不超过 l 的 e 和 $e' \in E_l$, $e|v\rangle$ 和 $e'|v'\rangle$ 仍是正交的, 即 $\langle v|ee'|v'\rangle = 0$. 在这里, 数字通信中两个向量 v 和 v' 可以区分就是这两个向量不同: $v \neq v'$. 而在量子通信中, 两个量子态 $|v\rangle$ 和 $|v'\rangle$ "完全" 可以区分则是指它们正交: $\langle v|v'\rangle = 0$. 由定义不难看出 $W_Q(ee') \leqslant W_Q(e) + W_Q(e')$. 所以, 对于量子码 Q, 如果对于 Q 中任意两个正交的码字 $|v\rangle$ 和 $|v'\rangle$, 以及任意的 $e, e' \in E_{2l+1}$, $e|v\rangle$ 和 $e'|v\rangle$ 均正交, 则量子码 Q 便可以纠正任意 $\leqslant l$ 位的量子错误.

定义 7 量子码 $Q(\subseteq (\mathbb{C}^2)^{\otimes n})$ 的最小 (量子) 距离是指满足下面条件的最大正整数 d: 若 $|v\rangle, |v'\rangle \in Q$ 且 $\langle v|v'\rangle = 0$, 则对每个 $e \in E_{d-1}$, 均有 $\langle v|e|v'\rangle = 0$ (这时, Q 可纠正任意 $\leqslant \lceil \frac{d-1}{2} \rceil$ 位量子错误).

综合上述, 作为 $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$ 的向量空间 Q, 二元量子码 Q 有三个基本参数: 码长 n、维数 $K = \dim Q \geqslant 1$ (或者用 $k = \log_2^K$, $0 \leqslant k \leqslant n$) 和最小距离 $d = d(Q)$, 表示成 $((n, K, d))$ 或者 $[[n, k, d]]$. 量子纠错码理论的基本问题如下:

(1) 构作好的量子码, 即 $R := \frac{k}{n}$ 大 (R 称为码率, 即效率高), 并且 $\delta := \frac{d}{n}$ 大 (δ 为相对极小距离, 即纠错能力强).

(2) 有好的纠错编码和纠错译码算法, 从而得到实际应用.

以下主要讨论构作好的量子码问题. 与经典纠错码类似, 三个参数 n、K (或 k) 和 d 之间有相互依赖的不等式关系, 称作量子码的界. 这些关系成为等式的码便是好的量子码.

定义 8 设 Q 是参数 $[[n, k, d]]$ 的纯量子码, 称 Q 为纯 (pure) 量子码, 是指对 Q 中任意两个 (不必不同的) 码字 $|v\rangle$ 和 $|v'\rangle$, 对于每个 $e \in E_n$, $1 \leqslant W_Q(e) \leqslant d - 1$, 均有 $\langle v|e|v'\rangle = 0$. 当 $k = 0$ (即 $K = 1$) 时, 参数 $[[n, 0, d]]$ 的量子码均指是满足此条件的纯量子码.

定理 7 (1) (量子 Hamming 界) 若 Q 是参数 $((n,K,d))$ 的纯量子码, $l=\lceil\frac{d-1}{2}\rceil$, 则

$$2^n \geqslant K\sum_{i=0}^{l} 3^i\binom{n}{i}.$$

等式成立的 Q 称作完全量子码. 例如, 1996–1997 年构作的 $[[5,1,3]]$ (即 $((5,2,3))$) 是完全量子码.

(2) (量子 Singleton 界) 若存在 $[[n,k,d]]$ 量子码, 则 $n\geqslant k+2d-2$. 等式成立的码称作 MDS (maximum distance separable) 量子码. 例如, $[[5,1,3]]$ 也是 MDS 码.

以上是 1995–1998 年逐渐明确的量子纠错码数学形式. 1998 年, Calderbank 等[26] 在此基础上给出了由经典纠错码构作量子码的系统有效的数学方法.

定理 8[26] 设 C 是 $\mathbb{F}_2^{2n}$ 中一个辛自正交的向量空间 (即 $C\subseteq C^{\perp_s}$), $\dim C=n-k$ $(0\leqslant k\leqslant n)$, 则存在参数为 $[[n,k,d]]$ 的量子码, 其中 $d=\min\{W_Q(c): c\in C^{\perp_s}\backslash C\}$. 进而, 若 $C_s^{\perp}$ 中没有量子重量 $\leqslant d-1$ 的非零向量, 即 $C^{\perp_s}\cap\overline{E}_{d-1}=\{0\}$, 从而 $d=\min\{W_Q(c): c\in C^{\perp_s}\backslash\{0\}\}$, 则存在参数为 $[[n,k,d]]$ 的纯量子码.

证明大意: 将 C 看作 $\overline{E}_n=\mathbb{F}_2^{2n}$ 的子群. 由于 C 是辛自正交的, 可以将它提升成 E_n 的交换子群 G, $\overline{G}=C$ 并且 $|G|=|C|=2^{n-k}$. G 中元素 $g=\mathrm{i}^{\lambda}X(a)Z(b)$ 对应于 $\mathbb{F}_2^{2n}$ 中向量 $\overline{g}=(a|b)$, 给出乘法群 G 和加法群 C 之间的同构. 交换群 G 在向量空间 $V=(\mathbb{C}^2)^{\otimes n}$ 上的作用给出直和 (以及正交) 分解 $V=\bigoplus_{\chi\in\hat{G}}Q(\chi)$, 其中 $Q(\chi)=\{|v\rangle\in V:\forall\, g\in G, g|v\rangle=\chi(g)|v\rangle\}$, 即 $Q(\chi)$ 是 V 中对应特征值 $\chi(g)$ 的对 G 公共特征子空间. 特别对群 G 的平凡特征 χ_0, $Q(\chi_0)$ 为 V 中群 G 的公共固定子空间. 可以证明对 G 的每个特征 χ, $Q(\chi)$ 的维数均为 2^k, 并且他们作为量子码具有定理 8 中所述的参数.

由定理 8 方式构作的量子码称作加性 (additive) 量子码. 定理 8 的证明是构造性的. 事实上, 群环 $\mathbb{C}[G]$ 有一组本原幂等元

$$\left\{e_\chi=\frac{1}{|G|}\sum_{g\in G}\chi(g)g:\chi\in\hat{G}\right\},$$

而 G- 不变子空间 $Q(\chi)$ 就是 $|G|e_\chi(V)=\{\sum_{g\in G}\chi(g)g|v\rangle:|v\rangle\in V\}$.

例 3 考虑 $\mathbb{F}_2^{10}$ 中以

$$G=\begin{bmatrix}v_1\\v_2\\v_3\\v_4\end{bmatrix}=\begin{bmatrix}1&1&0&0&0&0&0&1&0&1\\0&1&1&0&0&1&0&0&1&0\\0&0&1&1&0&0&1&0&0&1\\0&0&0&1&1&1&0&1&0&0\end{bmatrix}$$

为生成矩阵的二元线性码 C, $n=10/2=5$, $n-k=\dim C=4$, 从而 $k=1$. C 的基向量 $v_1,\ldots,v_4$ 两两 (包括 v_i 和 v_i 自身) 是辛正交的, 从而, C 为辛自正交码, 即 $C\subset C^{\perp_s}$, 其中 $C^{\perp_s}=C\oplus(11111|00000)\mathbb{F}_2\oplus(00000|11111)\mathbb{F}_2)$. $d=\min\{W_Q(c):c\in C^{\perp_s}\backslash C\}=\min\{W_Q(c):c\in C^{\perp_s}\backslash\{0\}\}=3$, 于是, 对每个 $\chi\in\hat{G}$, $Q(\chi)$ 是参数为 $[[n,k,d]]=[[5,1,3]]$ 的纯量子码. 例如, 取 χ 为 G 的平凡特征, 对应的幂等元为 $\frac{1}{|G|}\sum_{g\in G}g$. 将生成矩阵 G 的基向量 $v_i=(a_i|b_i)$ 提升成 $e_i=X(a_i)Z(b_i)$ $(1\leqslant i\leqslant 4)$, 则群 G 是由 e_i $(1\leqslant i\leqslant 4)$ 生成的 2^4 阶交换群:

$$G=\langle e_1,e_2,e_3,e_4\rangle=\{e_1^{\lambda_1}e_2^{\lambda_2}e_3^{\lambda_3}e_4^{\lambda_4}:(\lambda_1,\lambda_2,\lambda_3,\lambda_4)\in\mathbb{F}_2^4\}.$$

从而, 对于 G 的平凡特征 χ_0, 量子码 $Q=Q(\chi_0)$ 中有码字

$$\begin{aligned}|u_1\rangle &= \sum_{g\in G} g|00000\rangle\\ &= |00000\rangle + (|11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle)\\ &\quad - (|10100\rangle + |01010\rangle + |00101\rangle + |10010\rangle + |01001\rangle)\\ &\quad + (|11110\rangle + |01111\rangle + |10111\rangle + |11011\rangle + |11101\rangle),\\ |u_2\rangle &= \sum_{g\in G} g|11111\rangle\\ &= |11111\rangle + (|00111\rangle + |10011\rangle + |11001\rangle + |11100\rangle + |01110\rangle)\\ &\quad - (|01011\rangle + |10101\rangle + |11010\rangle + |01101\rangle + |10110\rangle)\\ &\quad + (|00001\rangle + |10000\rangle + |01000\rangle + |00100\rangle + |00010\rangle).\end{aligned}$$

由于 $\dim Q=2^k=2$, 因此, Q 便是由上面两个量子态张成的 2 维复向量空间, 它可以纠正 5 个量子位中任何 $\lceil\frac{d-1}{2}\rceil=1$ 位的量子错误 (σ_x 和 σ_z, 或者 σ_y).

定理 8 给出了由码长 $2n$ 的经典二元线性码 C 构造量子码 Q 的一般数学方法, 它要求 C 是辛自正交的, 并且 Q 的最小距离由 $C^{\perp_s}\backslash C$ 中向量的量子重量来决定. 下面两个定理是定理 8 的直接推论, 它们只需要码长为 n 的经典二元码 C, 要求 C 对于 $\mathbb{F}_2^n$ 中通常内积的对偶码 $C^\perp$ 是自正交的 (即 $C^\perp\subset(C^\perp)^\perp=C$), 并且给出量子码 Q 的最小 (量子) 距离 d 由 C 或者 $C^\perp$ 的最小 Hamming 距离所决定.

定理 9 若存在参数为 $[n,k,d]$ 的二元线性码 C, 并且 $C^\perp\subset C$ (从而 $n-k=\dim C^\perp\leqslant\dim C=k$, 即 $2k\leqslant n$), 则存在参数为 $[[n,2k-n,d]]$ 的 (加性) 纯量子码.

定理 10 若存在参数分别为 $[n,k_1,d_1]$ 和 $[n,k_2,d_2]$ 的二元线性码 C_1 和 C_2, 并且 $C_1^\perp\subset C_2$ (于是 $n-k_1\leqslant k_2$, 即 $k_1+k_2\geqslant n$), 则存在参数为 $[[n,k_1+k_2-n,\min(d_1,d_2)]]$ 的加性纯量子码.

进而, 文献 [26] 还给出了由 $\mathbb{F}_4$ 上的线性码构作加性量子码的方法. 利用这些方法, 在 1998 年以后, 人们采用各种已知的二元和四元线性码 (RM (Reed-Muller) 码、BCH (Bose-Chaudhuri-Hocquenghem) 码和代数几何码等) 构作出一系列好的加性量子码. 但早在 1999 年, Rains [27] 就发现了一些 $d=2$ 的非加性码, 其性能优于加性码. 利用有限 Fourier 变换, 文献 [28] 给出了量子纠错码的另一种刻画方式.

定理 11 [28] (1) 存在参数 $((n,K,d))$ 的二元量子码 ($K\geqslant 2$), 当且仅当存在 K 个非零映射

$$\varphi_i:\mathbb{F}_2^n\mapsto\mathbb{C},\quad 1\leqslant i\leqslant K \tag{4.1}$$

满足以下条件: 对于 $\{1,2,\ldots,n\}$ 的每个分拆

$$\{1,2,\ldots,n\}=A\cup B,\quad |A|=d-1,\quad |B|=n-d+1 \tag{4.2}$$

和任意 c_A, $c'_A\in\mathbb{F}_2^{d-1}$, $1\leqslant i,j\leqslant K$, 均有

$$\sum_{c_B\in\mathbb{F}_2^{n-d+1}}\overline{\varphi}_i(c_A,c_B)\varphi_j(c'_A,c_B)=\begin{cases}0, & i\neq j,\\ f, & i=j,\end{cases}$$

其中 $f=f(c_A,c'_A)$ 不依赖于 i.

(2) 设 $K \geqslant 1$, 则存在参数为 $((n, K, d))$ 的二元纯量子码, 当且仅当存在如 (4.1) 所示的 K 个非零映射, 使得下列两条件成立:

(2_1) $\mathbb{C}^{2^n}$ 中 K 个非零向量 $\varphi_i = (\varphi_i(c))_{c\in\mathbb{F}_2^n}$ $(1 \leqslant i \leqslant K)$ 是线性无关的;

(2_2) 对于 $\{1, 2, \ldots, n\}$ 的形如 (4.2) 的每个分拆和 $c_A, c'_A \in \mathbb{F}_2^{d-1}$, 均有

$$\sum_{c_B\in\mathbb{F}_2^{n-d+1}} \overline{\varphi}_i(c_A, c_B)\varphi_i(c'_A, c_B) = \begin{cases} 0, & c_A \neq c'_A, \\ \dfrac{(\varphi_i, \varphi_j)}{q^{d-1}}, & c_A = c'_A, \end{cases}$$

其中 $(\varphi_i, \varphi_j) = \sum_{c\in\mathbb{F}_2^n} \overline{\varphi}_i(c)\varphi_j(c)$.

在定理中取 $\varphi_i(x) = (-1)^{f_i(x)}$, 其中 $f_i(x) = f_i(x_1, \ldots, x_n) : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ $(1 \leqslant i \leqslant K)$ 为适当的二次布尔函数, 可以得到 $d = 2$ 的二元非加性量子码, 其维数大于文献 [3] 中的结果, 并且达到 (若 n 为偶数) 或渐近达到 (若 n 为奇数) 量子 Singleton 界.

基于量子通信和量子计算中容错 (fault-tolerant) 的应用, 二元量子码于 21 世纪初被推广为 non-binary 情形, 其中 $\mathbb{F}_2$ 改用有限域 $\mathbb{F}_q$ (q 为素数方幂 p^m). 类似二元情形, 由 $\mathbb{F}_q$ 或 $\mathbb{F}_{q^2}$ 上的经典线性码可以构作 q 元量子码. 事实上, 定理 11 在文献 [28] 中就是以 q 元量子码的形式出现的. 近年来, 关于量子码的构造的文献也很多. 下面这个定理是接下来构造 q 元量子 MDS 码要用到的.

定理 12 若存在参数为 $[n, k, d]$ 的 q^2 元线性码 C 使得 $C^{\perp_H} \subset C$, 则存在参数为 $[[n, 2k-n, \geqslant d]]$ 的 q 元量子码.

4.1 量子 MDS 码

量子 MDS 码是量子码中一类最优的码类之一, 因其参数达到了量子 Singleton 界. 根据经典的 MDS 猜想, 量子 MDS 码的码长也是受限的.

推论 1 若经典 MDS 猜想成立, 则 q 元量子 MDS 码的码长 $n \leqslant q^2+1$, 除了当 q 是偶数且 $d = 4$ 或者 $d = q^2$ 的情形下 $n \leqslant q^2 + 2$.

一个关于量子 MDS 码的纯度的比较有意义的结果是 Rains 给出的.

引理 4 [29] 一个 $k \geqslant 1$ 的 $[[n, k, d]]_q$ 量子 MDS 码至多是关于 $n - d + 2$ 是纯的.

由上面这个结论可以推出所有的量子 MDS 码都是纯的.

在过去的几年里, 众多的研究者在量子 MDS 码方面作出了很多的努力 (参见文献 [30–37]), 目的在于构造出尽可能多的量子 MDS 码. 文献 [38,39] 证明了对所有的 $3 \leqslant n \leqslant q+1$ 和 $1 \leqslant d \leqslant n/2+1$ 的 $[[n, n-2d+2, d]]_q$ 量子 MDS 码的存在性. 此外, 利用 Puncturing 的方法可以得到 $1 \leqslant d \leqslant q$, 码长 $n = q^2$ 和 q^2+1 的量子 MDS 码. 对于构造码长 $3 \leqslant n \leqslant q+1$ 的量子 MDS 码, 我们可以通过具有 Euclid 自正交性质的经典 MDS 码来构造. 但是对于构造码长 $q+1 \leqslant n \leqslant q^2+1$ 的量子 MDS 码则一般通过具有 Hermite 自正交性质的经典 MDS 码来构造, 且该问题较难完全解决. 文献 [34] 通过广义 Reed-Muller 码构造出了一些 $q+1 \leqslant n \leqslant q^2+1$ 的量子 MDS 码.

下面简单介绍文献 [30] 中构造量子 MDS 码的结果. 该文献利用 $\mathbb{F}_{q^2}$ 上的经典 Hermite 自正交广义 Reed-Solomon 码构造出了几类 $q+1 \leqslant n \leqslant q^2+1$ 的 q 元量子 MDS 码.

选取 $\mathbb{F}_{q^2}$ 中 n 个不同的元素 $\alpha_1, \ldots, \alpha_n$, 以及 $\mathbb{F}_{q^2}$ 中 n 个非零元素 $v_1, \ldots, v_n$. 对于 $1 \leqslant k \leqslant n$, 定义广义 Reed-Solomon (GRS) 码

$$\mathrm{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(a_n)) : f(x) \in \mathbb{F}_{q^2}[x], \deg f(x) \leqslant k-1\},$$

其中 $\alpha=(\alpha_1,\ldots,\alpha_n)$, $\boldsymbol{v}=(v_1,\ldots,v_n)$.

$\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})$ 的对偶码 $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^\perp$ 是广义 RS 码 $\mathrm{GRS}_{n-k}(\boldsymbol{\alpha},\boldsymbol{u})$, 其中 $\boldsymbol{u}$ 是下面方程组的一个解:

$$\begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-2} & v_2\alpha_2^{n-2} & \cdots & v_n\alpha_n^{n-2} \end{pmatrix}\boldsymbol{x}^{\mathrm{T}}=\boldsymbol{0}. \tag{4.3}$$

因此, 若 $\boldsymbol{v}=\boldsymbol{u}, k\leqslant\frac{n}{2}$, 则 $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})$ 是 Euclid 自正交的.

注意到无论删除上面的系数矩阵的哪一列, 剩下的矩阵都是一个 $(n-1)\times(n-1)$ 的 Vandermonde 矩阵, 因此, 上面的方程组的解空间的维数是 1, 而且每个非零解的所有分量都是非零的.

在以下的内容中, 我们将考虑 $\mathbb{F}_{q^2}$ (q 是一个素数幂) 上的 GRS 码. 对于向量 $\boldsymbol{v}=(v_1,\ldots,v_n)\in\mathbb{F}_{q^2}^n$, 对于所有的 $m\geqslant 1$, 定义 $\boldsymbol{v}^m=(v_1^m,\ldots,v_n^m)$. 对于 $\mathbb{F}_{q^2}^n$ 中的一个子集 S, 定义 S^m 为集合 $\{\boldsymbol{v}^m:\boldsymbol{v}\in S\}$. 然后我们易证, 若 V 是 $\mathbb{F}_{q^2}^n$ 中的一个子空间, m 是 $\mathbb{F}_{q^2}$ 的特征的幂次, 则 V^m 也是 $\mathbb{F}_{q^2}^n$ 的一个子空间. 此外, 我们易知对于一个 q^2 元线性码 C, 它的 Hermite 对偶 $C^{\perp_H}$ 等于 C^q 的 Euclid 对偶 $(C^q)^\perp$. 因此, C 是 Hermite 自正交的当且仅当 $C\subseteq(C^q)^\perp$, 即 $C^q\subseteq C^\perp$.

注 1 为了构造 Hermite 自正交 GRS 码, 一个常用的方法就是找到向量 $\boldsymbol{\alpha}=(\alpha_1,\ldots,\alpha_n)$ 和 $\boldsymbol{v}$ 使得 $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^q\subseteq\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^\perp$, 这样, $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})$ 就是 Hermite 自正交的. 我们有两种方法可以实现.

(i) 首先, 我们注意到 $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^q\subseteq\mathrm{GRS}_{q(k-1)+1}(\boldsymbol{\alpha},\boldsymbol{v}^q)$. 然后, 假如我们可以找到一个向量 $\boldsymbol{v}\in((\mathbb{F}_{q^2}^*)^n)$ 使得 $\boldsymbol{v}^{q+1}$ 是下面方程的一个解:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_n^{n-2} \end{pmatrix}\boldsymbol{x}^{\mathrm{T}}=\boldsymbol{0}, \tag{4.4}$$

则 $\mathrm{GRS}_{q(k-1)+1}(\boldsymbol{\alpha},\boldsymbol{v}^q)=\mathrm{GRS}_{n-q(k-1)-1}(\boldsymbol{\alpha},\boldsymbol{v})^\perp$. 因此, 若 $k\leqslant(n-1+q)/(q+1)$ (即 $k\leqslant n-q(k-1)-1$), 则 $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^q\subseteq\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^\perp$, 从而, $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})\subseteq\mathrm{GRS}_{n-q(k-1)-1}(\boldsymbol{\alpha},\boldsymbol{v})$.

(ii) 假设可以找到一个向量 $\boldsymbol{\alpha}$ 使得对于任意的 $V\in(\mathbb{F}_{q^2}^*)^n$ 都有 $\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^q\subseteq\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v}^q)$. 因此, 若 V^{q+1} 是 (4.4) 的一个解且 $k\leqslant n/2$, 则有

$$\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^q\subseteq\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v}^q)=\mathrm{GRS}_{n-k}(\boldsymbol{\alpha},\boldsymbol{v})^\perp\subseteq\mathrm{GRS}_k(\boldsymbol{\alpha},\boldsymbol{v})^\perp.$$

利用以上两种方法, 文献 [30] 构造了一系列的量子码. 对于码长为 q^2+1 的量子 MDS 码的构造, 我们可以在 GRS 上添加无穷远点的来构造.

定理 13 (i) 对于任意的 $2\leqslant k\leqslant q/2$, 都存在一个 q 元 $[[q^2+1,q^2+1-2k,k+1]]$- 量子 MDS 码.

(ii) 对于任意的 $2\leqslant k\leqslant q-2$, 都存在一个 q 元 $[[q^2,q^2-2k,k+1]]$- 量子 MDS 码.

(iii) 对于任意的 $2\leqslant k\leqslant q/2$, 都存在一个 q 元 $[[q^2-1,q^2+1-2k,k+1]]$- 量子 MDS 码.

对于任意长度的 q 元量子 MDS 码的结果如下.

定理 14 设 $4 \leqslant n \leqslant q^2$, n 为整数. 我们将 n 写成 $n = mq - r$, $1 \leqslant m \leqslant q$ 且 $0 \leqslant r \leqslant q-1$, 从而, 我们可以得到对于任意的 $2 \leqslant k \leqslant (q - 1 - \lfloor \frac{r}{m} \rfloor)/2$ 都存在一个 q 元 $[[n, n-2k, k+1]]$- 量子 MDS 码.

下面将固定一个量子码的极小距离, 并且给出对于 $q \geqslant 4d-5$, 都有一个 q 元量子 MDS 码.

定理 15 设 $k \geqslant 1$ 且是一个整数, 则对于任意的素数次幂 $q \geqslant 4k-1$ 且 $2k \leqslant n \leqslant q^2$, 都存在一个 q 元 $[[n, n-2k, k+1]]$- 量子 MDS 码.

除了利用具有一定自正交性质的广义 Reed-Solomon 码外, 我们还可以利用经典 Hermite 自正交循环码或常循环码来构造量子 MDS 码, 如文献 [36,37]. 我们简单介绍如何利用经典的 Hermite 自正交常循环码来构造量子 MDS 码.

同样, 我们考虑 $\mathbb{F}_{q^2}$ 上的码. 假设 n 和 q 互素, $\lambda \in \mathbb{F}_{q^2}^*$, $\mathbb{F}_{q^2}$ 上的一个码长为 n 的线性码 C 称为 λ- 常循环 (constacyclic) 的, 是指若 $(c_0, c_1, \ldots, c_{n-1}) \in C$, 则 $(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. 特别地, 若 $\lambda = 1$, 则 λ- 常循环码就称为循环码; 若 $\lambda = -1$, 则 λ- 常循环码就称为负循环码.

对于每一个 $(c_0, c_1, \ldots, c_{n-1}) \in C$, 我们都可以写成 $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ 的多项式的形式. 这样, 每一个 λ- 常循环码其实就对应于 $\mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle$ 中的一个理想. 我们知道 C 是可以由 $x^n - \lambda$ 的某个因子 $g(x)$ 唯一确定. 这个 $g(x)$ 就称为 C 的生成多项式, 记 $C = \langle g(x)\rangle$. 特别地, 若我们能确定 $x^n - \lambda$ 在 $\mathbb{F}_{q^2}[x]$ 上的完全分解, 我们就可以确定所有的 $\mathbb{F}_{q^2}$ 上码长为 n 的常循环码.

设 $\lambda \in \mathbb{F}_{q^2}^*$ 是一个 r 次本原单位根, 那么就存在一个 rn 次本原单位根 ($\mathbb{F}_{q^2}$ 的某个扩域上) η 使得 $\eta^n = \lambda$. 这样, $x^n - \lambda$ 的根就可以写成 η^{1+ri}, $0 \leqslant i \leqslant n-1$. 记 $\theta_{r,n} = \{1 + ri \mid 0 \leqslant i \leqslant n-1\}$. 从而, 码长为 n 的常循环码 $C = \langle g(x)\rangle$ 的定义集 (defining set) 就是 $Z = \{j \in \theta_{r,n} \mid \eta^j \text{ 是 } g(x) \text{ 的根}\}$. 不难得知, 定义集 Z 是一些模 rn 的 q^2 分圆陪集的并且 $\dim_{\mathbb{F}_{q^2}}(C) = n - |Z|$. 类似于循环码, 常循环码也有如下的 BCH 界.

引理 5 设 C 是 $\mathbb{F}_{q^2}$ 上码长为 n 的 λ- 常循环码, 其中 λ 是 r 次本原单位根. η 是 $\mathbb{F}_{q^2}$ 的扩域上的一个 rn 次本原单位根且满足 $\eta^n = \lambda$. 若 C 的生成多项式的根包含 $\{\eta\zeta^i \mid i_1 \leqslant i \leqslant i_1 + d - 1\}$, $\zeta = \eta^r$, 则 C 的极小距离至少为 d.

若 C 的定义集为 Z, 则 $C^{\perp_H}$ 的定义集为 $Z^{\perp_H} = \{z \in \theta_{r,n} \mid -qz \mod rn \notin Z\}$. 为了构造码长 $q+1 < n \leqslant q^2+1$ 的量子 MDS 码, 我们需要考虑包含 Hermite 对偶 (或者 Hermite 自正交) 的 q^2 元常循环码的存在性条件. 我们有以下的结果.

引理 6 若 C 是 $\mathbb{F}_{q^2}$ 上码长为 n 的 λ- 常循环码, 定义集 $Z \subseteq \theta_{r,n}$, 则 $C^{\perp_H} \subset C$ 当且仅当 $Z \cap Z^{-q} = \emptyset$, 其中 $Z^{-q} = \{-qz \mod rn \mid z \in Z\}$.

在已有文献中, 作者们研究了很多情形使得引理 6 中的 $Z \cap Z^{-q} = \emptyset$ 成立, 从而构造出包含 Hermite 对偶码的常循环码. 最后, 他们可以构造出许多量子 MDS 码, 如文献 [32,37].

在已有的文献中, 关于量子 MDS 码的文章颇多, 我们将其中的主要结果概括如下 (不是所有的结果):

对于下面的 n 和 d, 都存在 q 元 $[[n, n-2d+2, d]]$ 量子 MDS 码.

(i) $n = q^2+1$, $d = q+1$ (参见文献 [34]); $n = q^2+1$, $d \leqslant q+1$, q 为偶数, d 为奇数 (参见文献 [35]); $n = q^2+1$, $d \leqslant q+1$, $q \equiv 1 \mod 4$, d 为偶数 (参见文献 [36]).

(ii) $n = q^2$, $d \leqslant q$ (参见文献 [30,34,38]).

(iii) $n = (q^2+1)/2$, $q/2 + 1 < d \leqslant q$, q 为奇数 (参见文献 [36]).

(iv) $n = (q^2-1)/2$, $2 < d \leqslant q$, q 为奇数 (参见文献 [37]).

(v) $n = r(q+1)$, $r \mid q-1$, $\frac{q-1}{r}$ 是偶数, $2 \leqslant d \leqslant \frac{q+r+1}{2}$ (参见文献 [32]).

(vi) $n=r(q-1)$, $2\leqslant d\leqslant (q+1)/2+r-1$, $q+1=rt$, r 是偶数 (参见文献 [40]).

(vii) $n=r(q-1)+1$, $d\leqslant (q+r+1)/2$, $q\equiv r-1 \mod 2r$ (参见文献 [31]).

(viii) $n=r(q+1)$, $2\leqslant d\leqslant (q+1)/2+r$, $r\mid q-1$, r 和 q 均为奇数 (参见文献 [37]).

(ix) $n=2r(q+1)$, $2\leqslant d\leqslant (q+1)/2+2r$, $r\mid q-1$, r 为奇数, $q\equiv 1 \mod 4$ 为奇数 (参见文献 [37]).

基于以上的结果, 我们还可以通过文献 [41] 中的 propagation 规则得到更多的量子 MDS 码. 虽然量子 MDS 码的结果已经很多, 但是其中构造距离较大的量子码, 即 $d>\frac{q+2}{2}$ 的 q 元量子码较为困难, 且尚未完全解决. 若该问题能够被系统地解决将是很有意思的结果.

量子 MDS 码虽然是最优的一类码之一, 但是其码长是受限的. 因此, 人们还考虑了其他一般的量子码. 例如, 利用经典 BCH 码和代数几何码等构造一般的量子码使得码的参数尽可能地好 (参见文献 [42–44]).

4.2 渐近的情形

如前面所讲, 对于参数为 $[[n,k,d]]_q$ 的量子码, 固定 q 时, 我们希望码率 R 和相对极小距离 δ 尽可能大. 类似地, 我们可以考虑 n 充分大的情形.

对于一个量子码 Q, 我们分别记 $n(Q)$、$K(Q)$ 和 $d(Q)$ 为码长、维数和极小距离. 我们定义 U_q^C 为一些有序对 $(\delta,R)\in[0,1]\times[0,1]$ 的集合使得存在一类 q 元量子码 $\{Q_i\}_{i=1}^{\infty}$ 满足

$$n(Q_i)\to\infty,\quad R=\lim_{i\to\infty}\frac{\log_q K(Q_i)}{n(Q_i)},\quad \delta=\lim_{i\to\infty}\frac{d(Q_i)}{n(Q_i)}.$$

确定 U_q^C 也是量子码中一个非常重要的问题. 然而, 与经典码类似, 我们很难完全确定 U_q^C. 我们可以给出关于 U_q^C 的一些界 (参见文献 [41,45,46]). 首先有下面关于 U_q^C 的一种描述.

定义 9 给定一个素数次幂 q, 设

$$\alpha_q(\delta):=\sup\{R\in[0,1]:(\delta,R)\in U_q\},\quad 0\leqslant\delta\leqslant 1.$$

α_q^Q 可以看成是 $\mathbb{F}_q$ 上给定 δ 时, 最大可达的渐近码率的值. α_q^Q 是 $[0,1]$ 上的一个非增函数. 其中关于 U_q^Q 的一个比较有用描述是由文献 [41] 中给出的: 存在一个函数 $\alpha_q^Q(\delta)$ ($\delta\in[0,1]$) 使得 U_q^Q 是下列集合的并:

$$\{(\delta,R)\in\mathbb{R}^2:0\leqslant R<\alpha_q^Q(\delta),0\leqslant\delta\leqslant 1\},$$

其中有些点在 $\alpha_q^Q(\delta)$ 的边界上. 此外 $\alpha_q(0)=1$. 对于 $1/2\leqslant\delta\leqslant 1$, 有 $\alpha_q^Q(\delta)=0$. $\alpha_q^Q(\delta)$ 在区间 $[0,1]$ 递减.

确定 U_q^Q 几乎等价于确定函数 $\alpha_q^Q(\delta)$. 因此, 研究函数 $\alpha_q^Q(\delta)$ 对于量子码也很重要. 关于 $\alpha_2^Q(\delta)$ 的第一个下界是由代数几何码得出的 (参见文献 [47]). 后来, 这个界分别在文献 [46,48] 中得到了改进. 量子 Gilbert-Varshamov 界是由文献 [45] 给出的, 它是关于量子码的存在性的下界. 文献 [49] 给出了一个有限的量子 Gilbert-Varshamov 界. 该量子 Gilbert-Varshamov 界是通过 Hermite 自正交码得到的. 之后, 文献 [50] 通过 Symplectic 自正交码得到了量子另一版本的 Gilbert-Varshamov 界.

定理 16 [49] (有限量子 Gilbert-Varshamov 界) 设 $n>k\geqslant 2$, $d\geqslant 2$, 并且 $n\equiv k \pmod 2$, 若

$$\frac{q^{n-k+2}-1}{q^2-1}>\sum_{i=1}^{d-1}(q^2-1)^{i-1}\binom{n}{i},$$

则存在 $[[n,k,d]]_q$ 纯加性量子码.

我们可以很容易推导出渐近的量子 Gilbert-Varshamov 界为如下:

$$\alpha_q^Q(\delta) \geqslant 1 - \delta \log_q(q+1) - H_q(\delta), \quad \text{对 } \delta \in \left(0, \frac{1}{2}\right), \tag{4.5}$$

其中 $H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$ 为 q 元熵函数.

与经典码类似, 若 $q=2$, 则这个渐近量子 GV (Gilbert-Varshamov) 界就比文献 [46–48] 中构造性的界要好. 但是对于较大的 q, 我们就可以利用代数几何码改进量子 GV 界 (参见文献 [41]).

定理 17 [41] 设 q 是一个素数幂, 则有

$$\alpha_q^Q(\delta) \geqslant 1 - 2\delta - \frac{2}{A(q)}, \tag{4.6}$$

其中 $A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{q}$.

注意到 (4.6) 对于某些较大的 q 时比 (4.5) 好. 特别地, 当 q 是大于 19^2 的素数平方幂时, (4.6) 能将 (4.5) 改进约 $(q^2-1)/(2q^2-1)$.

对于存在性的界, 文献 [41] 还给出了更多的改进.

定理 18 [41] 设 q 是一个素数幂, 则有

$$\alpha_q^Q(\delta) \geqslant 1 - 2\delta - \frac{2}{A(q)} + \log_q\left(1 + \frac{1}{q^3}\right). \tag{4.7}$$

以上介绍的量子码都是对称的量子码. 2006 年以来, 基于量子信道的不同类型, 量子码又有各种不同的推广, 如量子卷积码、子系统量子码、具有 jump 特性的量子码、借助于纠缠的量子码、非对称量子码和非齐性量子码等, 其中非对称量子码对于量子错误 σ_x 和 σ_y 具有不同的纠错能力, 而非齐性量子码是 $\mathbb{C}^{k_1}\otimes\cdots\otimes\mathbb{C}^{k_m}$ 的线性空间, k_i $(1\leqslant i\leqslant m)$ 可以是不同的正整数. 对于这两种码已有类似于定理 11 的刻画方式 (参见文献 [51,52]). 已有的文献中也有很多关于非对称量子码的结果, 如文献 [53,54]. 其中很多理论都与对称的量子码是平行的. 借助于构作加性和非加性量子码的各种新技巧, 人们不断构作出各种类型的好量子码. 除此之类, 量子通信中还有一些问题也可以转化成量子纠错码的问题. 例如, 纠缠中 k-uniform 的构造就可以转化成 $[[n,0,k+1]]$ 的纯量子码的构造 (这里只考虑 $\mathbb{Z}_d$ 上的量子码的情形). 总之, 关于量子码的研究至今仍然十分活跃.

参考文献

1 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information (影印版). 北京: 高等教育出版社, 2003
2 Ireland K, Rosen M. A Classical Introduction to Modern Number Theory, 3rd ed. GTM 84. New York: Springer-Verlag, 1986
3 Bollobás B. Modern Graph Theory. GTM 184. New York: Springer-Verlag, 1988
4 Wan Z X. Lecture Notes on Finite Fields and Galois Rings. Singapore: Word Scientific, 2003
5 万哲先. 代数与编码 (第三版). 北京: 高等教育出版社, 2007
6 Wan Z X. Design Theory. 北京: 高等教育出版社, 2009
7 万哲先. 代数导引 (第二版). 北京: 科学出版社, 2010
8 Alon N, Lovász L. Unextendible product bases. J Combin Theory Ser A, 2001, 95: 169–179
9 Bennett C H, Divincenzo D P, Mor T, et al. Unextendible product bases and bound entanglement. Phys Rev Lett, 1999, 82: 5385–5388
10 Augusiak R, Stasińska J, Hadley C, et al. Bell inequalities with no quantum violation and unextendable product bases. Phys Rev Lett, 2011, 107: 070401
11 DiVincenzo D P, Mor T, Shor P W, et al. UPB, uncompletable product bases, and bound entanglement. Comm Math Phys, 2003, 238: 379–410

12 Sollid P Ø, Leinaas J M, Myrheim J. UPB and external density matrices with positive partial transpose. Phys Rev A (3), 2011, 84: 042325
13 Feng K. UPB and 1-factorization of complete graphs. Discrete Appl Math, 2006, 154: 942–949
14 Mendelsohn E, Rosa A. One-factorizations of the complete graph—A survey. J Graph Theory, 1985, 9: 43–65
15 Chetwynd A G, Hilton A J W. The edge-chromatic class of regular of graphs of degree 4 and their complements. Discrete Appl Math, 1987, 16: 125–134
16 Chen J, Johnston N. The minimum size of UPB in the bipartite case (and some multipartite cases). Comm Math Phys, 2015, 333: 351–365
17 Johnston N. The minimum size of qubit unextendible product bases. ArXiv:1302.1604, 2013
18 Roy A, Suda S. Complex spherical designs and codes. J Combin Des, 2014, 22: 105–148
19 Klappenecker A, Rötteler M. Constructions of MUB. Lecture Notes in Comput Sci, 2004, 2948: 137–144
20 Shparlinski I E, Winterhof A. Constructions of approximately MUB. Lecture Notes in Comput Sci, 2006, 3887: 793–799
21 王威扬, 张爱仙, 冯克勤. 利用 Gauss 和与 Jacobi 和构造近似 MUB 和 SIC-POVM. 中国科学: 数学, 2012, 42: 971–984
22 Zauner G. Quantum Designs-Grundzüge einer nichtkommutativen Designthorie. PhD Thesis. Vienna: Universität Wien, 1999
23 Scott A J, Grassl M. SIC-POVM: A new computer study. J Math Phys, 2010, 51: 042203
24 Klappencker A, Rötteler M, Shparlinski I E, et al. On approximately SIC-POVM and related system of quantum states. J Math Phys, 2005, 46: 082104
25 冯克勤, 陈豪. 量子纠错码. 北京: 科学出版社, 2010
26 Calderbank A R, Rains E M, Shor P W, et al. Quantum error correction via codes over GF(4). IEEE Trans Inform Theory, 1998, 44: 1369–1387
27 Rains E M. Quantum codes of minimal distance two. IEEE Trans Inform Theory, 1999, 45: 266–271
28 Feng K, Xing C. A new construction of quantum error-correcting codes. Trans Amer Math Soc, 2008, 360: 2007–2019
29 Rains E M. Nonbinary quantum codes. IEEE Trans Inform Theory, 1999, 45: 1827–1832
30 Jin L F, Ling S, Luo J Q, et al. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes. IEEE Trans Inform Theory, 2010, 56: 4735–4740
31 Jin L F, Xing C P. A construction of new quantum MDS codes. IEEE Trans Inform Theory, 2014, 60: 2921–2925
32 Chen B, Ling S, Zhang G. Apllication of constacyclic codes to quantum MDS codes. IEEE Trans Inform Theory, 2015, 61: 1474–1484
33 Feng K. Quantum code $[[6,2,3]]_p$ and $[[7,3,3]]_p$ ($p \geqslant 3$) exists. IEEE Trans Inform Theory, 2002, 48: 2384–2391
34 Li Z, Xing L J, Wang X M. Quantum generalized Reed-Solomon codes: Unified framework for quantum MDS codes. Phys Rev A, 2008, 77: 012308
35 Guardia G G L. New quantum MDS codes. IEEE Trans Inform Theory, 2011, 57: 5551–554
36 Kai X, Zhu S. New quantum MDS codes from negacyclic codes. IEEE Trans Inform Theory, 2012, 59: 1193–1197
37 Kai X, Zhu S, Li P. Constacyclic codes and some new quantum MDS codes. IEEE Trans Inform Theory, 2014, 60: 2080–2086
38 Grassl M, Beth T, Röttler M. On optimal quantum codes. Int J Quantum Inf, 2004, 2: 757–775
39 Röttler M, Grassl M, Beth T. On quantum MDS codes. In: Proceedings of International Symposium on Information Theory. Chicago: IEEE, 2004, 356–356
40 Wang L Q, Zhu S X. New quantum MDS codes derived from constacyclic codes. Quantum Inf Process, 2015, 14: 881–889
41 Feng K Q, Ling S, Xing C P. Asymptotic bounds on quantum codes from algebraic geometry codes. IEEE Trans Inform Theory, 2006, 52: 986–991
42 Jin L F, Xing C P. Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes. IEEE Trans Inform Theory, 2012, 58: 5484–5489
43 Jin L F, Xing C P. A construction of quantum codes via a class of polynomial codes. In: Proceeding of 2012 IEEE International Symposium on Information Theory (ISIT 2012). Boston: IEEE, 2012, 339–342
44 Jin L F. Quantum stabilizer codes from maximal curves. IEEE Trans Inform Theory, 2014, 60: 313–316
45 Ashikhmin A, Knill E. Nonbinary quantum stablizer codes. IEEE Trans Inform Theory, 2001, 7: 3065–3072
46 Chen H, Ling S, Xing C P. Aymptoticially good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound. IEEE Trans Inform Theory, 2001, 47: 2055–2058
47 Ashikhmin A, Litsyn S, Tsfasman M A. Aymptotically good quantum codes. Phys Rev A (3), 2001, 63: 032311
48 Matsumoto R. Improvement of the Ashikhmin-Litsyn-Tsfasman bound for quantum codes. IEEE Trans Inform Theory,

2002, 48: 2122–2124
49 Feng K Q, Ma Z. A finite Gilbert-Varshmov bound for pure stabilizer quantum codes. IEEE Trans Inform Theory, 2004, 50: 3323–3325
50 Jin L F, Xing C P. Quantum Gilbert-Varshamov bound through symplectic self-orthogonal codes. In: Proceeding of 2011 IEEE International Symposium on Information Theory (ISIT 2011). Saint Petersburg: IEEE, 2011, 455–458
51 Wang L, Feng K, Ling S, et al. Asymmetric quantum codes: Characterization and constructions. IEEE Trans Inform Theory, 2010, 56: 2938–2945
52 Wang W, Feng K. Inhomogeneous quantum codes (III): The asymmetric case. Chin Ann Math Ser B, 2014, 35: 271–284
53 Ezerman M F, Ling S, Solé P. Additive asymmetric quantum codes. IEEE Trans Inform Theory, 2011, 57: 5536–5550
54 Ezerman M F, Jitman S, Kiah H M, et al. Pure asymmetric quantum MDS codes from CSS construction: A complete characterization. Int J Quantum Inf, 2013, 11: 1350027

Several mathematical problems in quantum information theory

FENG KeQin & JIN LingFei

Abstract The theory of quantum communication and technology have been one of hot research topics in information science and technology since 1980's. In this paper, we survey some research development of several mathematical problems in quantum information theory. Particularly, we focus on the important role of combinatorics (including graph theory), number theory, algebra and algebraic geometry (the arithmetic theory of algebraic curves over finite field) in investigating quantum measurement and quantum error-correction.

Keywords **product state, mutually unbiased bases, quantum error correcting codes**

MSC(2010) **81P45, 11B75, 11T71**

doi: 10.1360/N012016-00159