中国科学 : 物理学 力学 天文学 2015 年 第 45 卷 第 3 期 : 030001
SCIENTIA SINICA Physica, Mechanica & Astronomica phys.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

论 文

量子稳定子码的码字纠缠

陈小余*

浙江工商大学信息与电子工程学院, 杭州 310018
* 联系人, E-mail: xychen@zjgsu.edu.cn

收稿日期: 2014-08-26; 接受日期: 2014-12-05; 网络出版日期: 2015-01-20
国家自然科学基金资助项目 (批准号: 11375152, 60972071)

摘要 量子计算和量子通信是量子信息科学的两个重要组成部分. 量子算法通常用到实系数等权重纯态, 其中重要的一类是图态, 图态的纠缠已经得到系统的研究. 量子通信中不可避免地要用量子纠错码, 其中最广泛使用的是与图态紧密相关的量子稳定子码, 可以看作是由图态与经典编码两个要素构成的. 本文将论证量子编码复杂度与量子码字纠缠的关系. 为研究量子码字的纠缠, 将证明几何测度、对数鲁棒纠缠和相对熵纠缠等纠缠测度对于量子稳定子码字而言是相等的, 纠缠的上下界可由量子编码的生成元确定. 用经典编码可以构造一类量子码, 称为 CSS 码. 其中最常用的是对偶包含法. 对于 CSS 对偶包含码的码字, 证明它的纠缠等于其经典生成元的个数. 本文给出 Gottesman 码以及相关码的纠缠公式, 还发展了迭代算法用来数值计算纠缠量.

关键词 量子编码, 多组分纠缠, 量子测量

PACS: 03.67.Mn, 03.65.Ud, 03.67.Ac

doi: 10.1360/SSPMA2014-00327

1 引言

量子编码对于量子通信和量子计算都非常重要, 携带量子信息的量子态容易受到环境消相干的影响而退化, 因此需要对量子态进行编码保护. 量子编码使用一系列量子比特门实现, 其中单量子比特门比较容易实现, 双量子比特门或多量子比特门涉及量子比特间的相互作用, 实现的难度大一些, 双量子比特门和多量子比特门的总数目实际上可以作为衡量量子编码复杂度的一种合理方法. 显然, 同一个量子码会有不同的量子线路实现方法, 因此存在最小量子编码复杂度的问题. 因为量子门操作中也会带有消相干, 故多余的量子门是有害的, 需要尽可能简化量子线路. 观察已有的由量子线路实现的量子编码发现, 量子编码复杂度不小于本文将研究的量子编码码字纠缠量 (表 1). 该经验观察结果有一定的理论依据, 因为纠缠是量子比特间相互作用形成的, 选取合适的纠缠测度则纠缠可以示性量子比特间相互作用的广泛程度. 因此, 量子码字纠缠可以作为量子编码复杂度的可能的下界, 是简化量子线路的一个指向.

量子编码的一种实现办法是使用量子图态 [1], 并且在实验中已经实现用 4 量子比特图态进行的量子编码 [2]. 量子图态的纠缠已经得到了广泛的研究 [3−6], 但是量子编码具有多样性, 一种量子编码可

引用格式: 陈小余. 量子稳定子码的码字纠缠. 中国科学: 物理学 力学 天文学, 2015, 45: 030001
Chen X Y. Entanglement of stabilizer codewords (in Chinese). Sci Sin-Phys Mech Astron, 2015, 45: 030001, doi: 10.1360/SSPMA2014-00327

以对应多个图态, 同时一个量子图态也可以编多种量子码. 因此研究量子码的码字纠缠具有独立的价值和意义.

量子编码是用较多的有冗余的物理量子比特表示逻辑量子比特 [7]. 如果逻辑量子比特被 3 个或者更多的组分所拥有, 一个组分可以包含 1 个或多个物理量子比特, 那么量子码字就可以看作一种多组分态, 通常是多组分纠缠态. 多组分纠缠的定量化是非常活跃的研究领域, 即使对于多组分纯态也有许多未解决的问题. 已经提出各种不同的多组分纠缠测度. 包括对数鲁棒纠缠 [8], 相对熵纠缠 [9,10] 和几何测度 [11] 和平均熵等 [12,13]. 将多组分纠缠态与量子噪声混合则混合后态的纠缠将减少, 加入过多的量子噪声则混合后态不再是纠缠态, 对数鲁棒纠缠用混合态不再纠缠所能允许加入的最少的任意态 (包括量子噪声) 的比例来表示混合前多组分纠缠态的纠缠量. 几何测度是一个态到其最近乘积态按保真度度量的距离. 相对熵纠缠是一个态与它的最近分离态的相对熵. 多组分纠缠的定量化通常很困难, 因为大多数的纠缠度量方法定义中含有难以求解的变分问题. 即便是多组分纯态, 也只得到一些特定态的纠缠, 稳定子态是其中之一. 稳定子态是一类多组分纯态, 是泡利群中对易可观察量完全集的唯一的共同本征矢量, 泡利群是由泡利矩阵和单位矩阵的所有张量积构成的群. 幸运的是, 根据对数鲁棒纠缠, 相对熵纠缠和几何测度 [14−16] 三者间的不等式, 对于稳定子态而言, 该三种纠缠测度是相等的 [5]. 如果泡利群中的对易可观察量集不完备, 则稳定了一个 Hilbert 子空间而不只是稳定子态, 该 Hilbert 子空间就是量子稳定子码 [4]. 码字则是稳定子码的基. 人们可能会问这三种纠缠测度对于一般的量子稳定子码字是否相等, 回答是肯定的, 将在本文第 2 节中介绍.

2 量子码字的纠缠测度

一个纠缠态与一个任意态混合得到的态可能纠缠也可能是可分离的, 取决于混入的任意态的比例 t, 量子态 ρ 的全局鲁棒纠缠 $R(\rho)$[8] 定义为

$$R(\rho)=\min t \tag{1}$$

使得存在一个态 Δ(任意态) 满足

$$\sigma=(\rho+t\Delta)/(1+t)\in Sep. \tag{2}$$

这里 Sep 是可分离态的集合. 因此全局鲁棒纠缠就是能混入量子态 ρ 的任意态最少比例, 使得混合后的态可分离; 或者说破坏量子态的纠缠所需的最小任意噪声. 对数鲁棒纠缠表示为

$$LR(\rho)=\log_2(1+R(\rho)). \tag{3}$$

相对熵纠缠定义为纠缠态 [10] 到其最近乘积态的相对熵, 可以认为是一种 “距离”,

$$E_r(\rho)=\min_{\omega\in Sep} S(\rho\|\,\omega), \tag{4}$$

其中 $S(\rho\|\,\omega)=-S(\rho)-tr\{\rho log_2\omega\}$ 是相对熵, $S(\rho)=-tr\{\rho log_2\rho\}$ 是冯 · 诺依曼熵. 对于纯态 $|\psi\rangle$, 几何测度定义为

$$E_g(|\psi\rangle)=\min_{|\phi\rangle\in Pro} -\log_2|\langle\phi|\,\psi\rangle|^2, \tag{5}$$

式中, Pro 是直积态的集合. 上述定义扩展以后也可以用于混合态 ρ, 有 $E_g(\rho)=\min_{\omega\in Sep}-\log_2 tr(\rho\omega)$, 不过, E_g 仅仅对于纯态 $\rho=|\psi\rangle\langle\psi|$ 具有纠缠单调性. 几何测度可以在实验中 [17,18] 直接测量到. 已经表明一个量子纯态集合 $\{|\psi_i\rangle\,|i=1,...,N\}$, 若可以用局域操作和经典通信 (LOCC) 进行可靠相互区分, 则集合能含有的量子纯态的最大数目 N 由其所含的平均纠缠量所限制 [15]:

$$\log_2 N\leqslant n-\overline{LR(|\psi_i\rangle)}\leqslant n-\overline{E_r(|\psi_i\rangle)}\leqslant n-\overline{E_g(|\psi_i\rangle)}, \tag{6}$$

这里 $n=\log_2 D_H$, D_H 是希尔伯特空间的总维数, $\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i$ 表示 “平均值”.

一个 n 量子比特的稳定子态 $|S\rangle$ 定义为 n 个独立的相互对易的泡利群元素 M_i 的本征值为 1 的共同本征矢量. n 个本征方程 $M_i|S\rangle=|S\rangle$ 完全确定了态 $|S\rangle$(除全局任意相因子外). 由 n 个算符 M_i 的积组成的群称作稳定子 S, 而 M_i 是群 S 的生成元. S 的一个有 $n-k$ 个生成元的子群也称作稳定子 [19], 记作 M. 不过, $M\subset S$ 稳定了 2^k 维的空间. 原则上, 该空间就是编码空间 $\{|\psi\rangle\,|\,T|\psi\rangle=|\psi\rangle,\forall T\in M\}$, 对应于将 k 量子比特编码到 n 量子比特的稳定子码. 除了 $n-k$ 个稳定子生成元外, 稳定子码还有逻辑操作符

$\overline{X}_1,\cdots,\overline{X}_k$ 和 $\overline{Z}_1,\cdots,\overline{Z}_k$. 用码字基组来表达该量子稳定子码

$$|\overline{0}\rangle = \mathscr{N}\sum_{T\in M} T|0\rangle^{\otimes n},$$
$$|\overline{\boldsymbol{c}}\rangle = \overline{X}_1^{c_1}\cdots\overline{X}_k^{c_k}|\overline{0}\rangle,$$

其中 $\boldsymbol{c}=(c_1,\cdots,c_k)$ 是二进制矢量, $\mathscr{N}$ 是归一化因子. $\overline{Z}_i|\overline{0}\rangle = |\overline{0}\rangle$ 且 $i=1,\cdots,k$.

对稳定子态 $|S\rangle$, 已经证明 [5]

$$LR(|S\rangle) = E_r(|S\rangle) = E_g(|S\rangle). \tag{7}$$

上式对量子稳定子码字 $|\overline{\boldsymbol{c}}\rangle$ 同样适用.

命题 1 对于量子稳定子码字 $|\overline{\boldsymbol{c}}\rangle$ 而言, 对数鲁棒纠缠, 相对熵纠缠和几何测度纠缠都是等价的.

证明 证明对态 $|\overline{0}\rangle$ 成立就足够了, 因为 $|\overline{\boldsymbol{c}}\rangle$ 和 $|\overline{0}\rangle$ 是局域等价的. 注意到 $n-k$ 个生成元 M_1, $\cdots$, M_{n-k} 和 k 个逻辑算符 $\overline{Z}_1,\cdots,\overline{Z}_k$ 稳定了 $|\overline{0}\rangle$ 态. 这 $n-k$ 个生成元和 k 个逻辑算符之间是相互对易并且是相互独立的. 因此, 态 $|\overline{0}\rangle$ 是稳定子态, 其3种纠缠测度相互等价 [5].

对于量子稳定子码字, 我们将这3种纠缠度量统称为纠缠, 记为 $E(|\overline{\boldsymbol{c}}\rangle)$.

3 纠缠上界

生成元由各个量子比特的泡利算符 X,Y,Z 或恒等算符 I 的乘积构成. 若一生成元仅由 Z 算符或恒等算符的乘积构成, 任何量子比特上不包含 X 和 Y 算符, 则称为 Z 型生成元.

命题 2 量子稳定子码的码字纠缠上界由其非 Z 型生成元的最少个数所确定.

证明 码字为 $|\overline{0}\rangle = \mathscr{N}\prod_{i=1}^{n-k}(I+M_i)|0\rangle^{\otimes n}$. 对于 Z 型生成元 M_l, 有等式 $(I+M_l)|0\rangle^{\otimes n} = 2|0\rangle^{\otimes n}$. 在算符的乘积式 $\prod_i(I+M_i)$ 中可以将因子 $(I+M_l)$ 移到最右边并作用后去掉. 因此在将态 $|\overline{0}\rangle$ 分解为直积态线性组合的过程中, 其项数 R 的上限为 $2^{r'}$, 其中 r' 为非 Z 型生成元的个数. 令 $r=\min r'$ 为非 Z 型生成元的最小数目, 可以人为地通过将 Z 型生成元替换为一个 Z 型生成元和一个非 Z 型生成元的乘积来增加非 Z 型生成元的数量. 因此需要计算非 Z 型生成元最小数目. 由此得出 Schmidt 测度 [3]

$$E_S = \min\log_2 R$$

的上界为 r. 几何测度的上界是 Schmidt 测度 [20], 因此命题得证.

对于稳定子群 M, 不计整体相位 $\pm1,\pm i$, 每个生成元都可以写为 $M_i = X^{a_i}Z^{b_i}$, 其中 $X^{a_i} = \bigotimes_j X_j^{a_{ij}}$, $Z^{b_i} = \bigotimes_j Z_j^{b_{ij}}$, 且 a_i 和 b_i 分别是二进制矢量 $(a_{i1},a_{i2},\cdots,a_{in})$ 和 $(b_{i1},b_{i2},\cdots,b_{in})$. 生成元 M_i 的另一种表示法为 $(a_i|\,b_i)$. 可以用生成元矩阵 [4](在文献 [19] 中称之为稳定子矩阵)$(A|\,B)$ 来表示稳定群 M, 其中 A 和 B 是 $(n-k)\times n$ 矩阵, 矩阵元为 $A_{ij}=a_{ij}$, $B_{ij}=b_{ij}$. 通过量子比特位置交换以及将生成元换成稳定子群中的其他群元, 总可以将 $(A|B)$ 写成如下形式 (见文献 [19] 第4章)

$$\left(\begin{array}{cc|cc} I & D & F & G \\ 0 & 0 & J & K \end{array}\right), \tag{8}$$

这里 I 是 $r\times r$ 单位矩阵. 其中 r 是 A 矩阵在 $\mathbb{F}_2$ 域中的秩, 而 $\mathbb{F}_2$ 域是 0,1 两个元素构成的域 $\{0,1\}$, 加法和乘法都是模 2 的. 有了 (8) 式作为生成元矩阵的标准形式, 得以改进纠缠上界. 我们研究泡利测量对码字的影响, 考虑 (8) 式中生成元 M 的前 r 行, 而忽略其余 $(n-k-r)$ 个 Z 型生成元. 对于标准形式的生成元, 有 $M_1 = X\otimes M_1'$ 或 $M_1 = Y\otimes M_1'$, $M_{i+1} = Z\otimes M_{i+1}'$ 或 $M_{i+1} = I\otimes M_{i+1}'$, $(i=1,\cdots,r-1)$. 记 $|\overline{0}_{n-1}\rangle = \mathscr{N}'\prod_{i=1}^{r-1}(I+M_{i+1}')|0\rangle^{\otimes(n-1)}$, 其中 $\mathscr{N}'$ 为归一化因子. 对第一个量子比特的泡利 Z 测量将码字 $|\overline{0}\rangle$ 投影为

$$P_{z+}^{(1)}|\overline{0}\rangle = |0\rangle\otimes|\overline{0}_{n-1}\rangle, \tag{9}$$
$$P_{z-}^{(1)}|\overline{0}\rangle = |1\rangle\otimes M_1'|\overline{0}_{n-1}\rangle. \tag{10}$$

对第 j 个量子比特的投影测量算符为 $P_{z\pm}^{(j)} = \frac{1}{2}(I\pm Z_j)$. 两种测量结果 ±1 以等概率出现. 同理, 除了 X 或者 Y 的测量只有一个结果的特殊情况之外, 对第一个量子比特的 X 或者 Y 测量也会等概率地将码字投影到测度结果为 ±1 的两个对应态. 当 $M_1 = X\otimes M_1'$ 时, 泡利 X,Y 算符对第一个量子比特的测量将码字 $|\overline{0}\rangle$ 投影到 $P_{x\pm}^{(1)}|\overline{0}\rangle = \frac{1}{2}(|0\rangle\pm|1\rangle)\otimes(I\pm M_1')|\overline{0}_{n-1}\rangle$, $P_{y\pm}^{(1)}|\overline{0}\rangle$

$=\frac{1}{2}(|0\rangle \pm i|1\rangle)\otimes(I\mp iM_1')\left|\overline{0}_{n-1}\right\rangle$. 当 $M_1=Y\otimes M_1'$ 时, 泡利 X,Y 算符对第一个量子比特的测量将码字 $\left|\overline{0}\right\rangle$ 投影到 $P_{x\pm}^{(1)}\left|\overline{0}\right\rangle=\frac{1}{2}(|0\rangle\pm|1\rangle)\otimes(I\pm iM_1')\left|\overline{0}_{n-1}\right\rangle$, $P_{y\pm}^{(1)}\left|\overline{0}\right\rangle=\frac{1}{2}(|0\rangle\pm i|1\rangle)\otimes(I\pm M_1')\left|\overline{0}_{n-1}\right\rangle$. 有一种情况是 $\left|\overline{0}_{n-1}\right\rangle$ 恰为 M_1' 的本征矢量, 这时测量结果只有一种.

任何局域投影测量序列都是将态矢 $|\psi\rangle$ 逐步分解到每个测量结果中, 最终分解为完全分离的态. 由 Schmidt 测度的定义 [3], 得到它的上界

$$E_S(|\psi\rangle)\leqslant\log_2(N_{\rm mea}), \tag{11}$$

其中 $N_{\rm mea}$ 为概率不为零的最终测量结果数目.

用局域泡利测量分解一个量子稳定子码字到完全分离态所需的最少泡利测量步数称为泡利韧性. 考虑由 (8) 式作为生成元矩阵生成的量子码字, 其非 Z 型生成元最小数目是 r, 依次进行 r 步泡利测量, 则态分解为乘积态. 因此泡利韧性不会大于 r. 事实上 (8) 式生成的码字态的项数不会超过 2^r 项. 如为 2^r 项, 进行 r 次泡利测量总是可以将其分解为分离态的. 少于 2^r 项的话, 可以用更少的测量次数.

命题 3 量子稳定子码字 $|\bar{c}\rangle$ 的纠缠以泡利韧性为上界.

证明 由方程 (11), 以及对码字测量得到不同测量结果的概率为 1/2, 同时 Schmidt 测度是几何测度的上界, 命题得证.

例如, 考虑 $[[8,1,3]]$ 码 (见脚注 1))[21], 其标准形式的稳定子矩阵为

$$\begin{bmatrix} X & Z & Z & Z & Z & Z & Z & Y\\ I & X & I & Z & I & Z & I & Z\\ I & I & X & Z & I & I & Z & Z\\ Z & Z & Z & X & I & I & I & I\\ I & Z & Z & I & Y & Z & Z & X\\ Z & Z & I & I & Z & X & I & I\\ Z & Z & I & I & I & I & X & Y \end{bmatrix},$$

对 1,5,7 量子比特进行泡利 Z 算符测量. 对每个量子比特测量后, 删除其所在的行和列. 剩下的量子比特的稳定子矩阵是

$$\begin{bmatrix} X & I & Z & Z & Z\\ I & X & Z & I & Z\\ Z & Z & X & I & I\\ Z & I & I & X & I \end{bmatrix}. \tag{12}$$

由 (12) 生成的态 $\left|\overline{0}_5\right\rangle$ 是图态 $|G_4\rangle$ 与 $|0\rangle$ 的直积, 即 $\left|\overline{0}_5\right\rangle=|G_4\rangle\otimes|0\rangle$. 删除 (12) 式的最后一列得到一个新的稳定子矩阵, 正是图态 $|G_4\rangle$ 的生成元矩阵. 图态 $|G_4\rangle$ 的泡利韧性已知为 2, 因此在 Grassl 码表 (见脚注 1))[21] 中定义的 $[[8,1,3]]$ 码的码字泡利韧性为 5.

如果我们将 $[[8,1,3]]$ 码的稳定子矩阵写成 (8) 式的形式, 可以看出选择 1,5,7 量子比特进行测量的原因在于消去矩阵 D, 使得余下的新稳定子矩阵不包含 D 部分, 从而对 1,5,7 进行测量操作以后的态可以写成 2 部分的直积. 其中一部分纠缠为零.

不在表 1 中的码字可以简单地根据命题 2 得到码字纠缠的上界, 表 1 中的码字可由命题 3 确定其更精确的纠缠上界.

4 纠缠下界

将物理量子比特的下标表示为 $\mathscr{I}=\{1,2,\ldots,n\}$, 对于一个二组分划分, 可以分配 m 个量子比特给 $\mathscr{A}$, 剩下 $n-m$ 个量子比特给 $\mathscr{B}$. $\mathscr{A}$ 和 $\mathscr{B}$ 下标的集合分别为 $\mathscr{I}_{\mathscr{A}}$ 和 $\mathscr{I}_{\mathscr{B}}=\mathscr{I}-\mathscr{I}_{\mathscr{A}}$. 码字 $\left|\overline{0}\right\rangle$ 的约化态为 $\rho_{\mathscr{B}}=Tr_{\mathscr{A}}\left|\overline{0}\right\rangle\left\langle\overline{0}\right|$. 划分为二组分 $\{\mathscr{I}_{\mathscr{A}},\mathscr{I}_{\mathscr{B}}\}$ 后的 2 组分纠缠为 $-Tr\rho_{\mathscr{B}}\log_2\rho_{\mathscr{B}}$, 即态 $\rho_{\mathscr{B}}$ 的熵.

命题 4 码字的纠缠下界由该码字的任意二组分纠缠确定.

$$E\geqslant -Tr\rho_{\mathscr{B}}\log_2\rho_{\mathscr{B}}. \tag{13}$$

证明 如果定义 E_{rbi} 为态的某二组分划分的相对熵纠缠, 当完全可分离态是该二组分可分离态的子集时, 有 $E_r\geqslant E_{rbi}$. 注意到 $E_r=E$, 对于纯态 E_{rbi} 与二组分纠缠 $E_{bi}=-Tr\rho_{\mathscr{B}}\log_2\rho_{\mathscr{B}}$ 相等, 命题得证.

通过对角化 $\rho_{\mathscr{B}}$ 得到 $\rho_{\mathscr{B}}$ 的熵, 而且熵最后可以

1) Grassl M. Table of Quantum Error-Correcting Codes. http://iaks-www.ira.uka.de /home/grassl/QECC/circuits/index.html

用稳定子矩阵来表示. 码字纠缠的下界由所有的二组分划分中最大的二组分纠缠确定.

因为 Z 型生成元不贡献新的项给码字 $|\overline{0}\rangle$, 故不考虑 Z 型生成元. 下文考虑 $(A\,|B) = (I\,D|E\,F)$. A,B 为 r 个非 Z 型生成元的 $r\times n$ 二进制矩阵, 且 $r\leqslant n-k$.

码字

$$\begin{aligned}|\overline{0}\rangle &= \mathscr{N}\sum_{\mu\in\{0,1\}^{\otimes r}}(-1)^{\alpha(\mu)}X^{\mu A}\,|0\rangle^{\otimes n}\\ &= \mathscr{N}\sum_{\mu\in\{0,1\}^{\otimes r}}(-1)^{\alpha(\mu)}\bigotimes_{j\in\mathscr{I}_{\mathscr{A}}}X_j^{(\mu A)_j}\bigotimes_{l\in\mathscr{I}_{\mathscr{B}}}X_l^{(\mu A)_l}\,|0\rangle^{\otimes n},\end{aligned}$$

其中 $(\mu A)_j$ 是二进制矢量 μA 的第 j 个元素, $\mathscr{N}$ 是归一化因子. 这里 $\alpha(\mu)$ 为

$$\alpha(\mu) = \frac{1}{2}[\mu\Gamma\mu^{\mathrm{T}} - \mathrm{Tr}(\Lambda\Gamma\Lambda)] = \frac{1}{2}\mu\Gamma_1\mu^{\mathrm{T}}, \tag{14}$$

其中 $\Lambda = \mathrm{diag}\{\mu_1,\cdots,\mu_r\}$, 且 Γ_1 是将 Γ 的对角元素变为零而得. 而

$$\Gamma = AB^{\mathrm{T}} = F^{\mathrm{T}} + DG^{\mathrm{T}}.$$

式中的加法取模 2. Γ 是对称的, 因为任何 2 个生成元之间相互对易, 即 $AB^{\mathrm{T}} + B^{\mathrm{T}}A = 0$. 约化态

$$\begin{aligned}\rho_{\mathscr{B}} = &\sum_{\mu,\mu'}\prod_{j\in\mathscr{I}_{\mathscr{A}}}\delta_{(\mu A)_j,(\mu' A)_j}(-1)^{\alpha(\mu)+\alpha(\mu')}\\ &\bigotimes_{l,l'\in\mathscr{I}_{\mathscr{B}}}X_l^{(\mu A)_l}\,|0\rangle^{\otimes(n-m)}\langle 0|^{\otimes(n-m)}X_{l'}^{(\mu' A)_{l'}},\end{aligned}$$

不计归一化, 结果

$$\rho_{\mathscr{B}} = \sum_{\mu,\mu'}\prod_{j\in\mathscr{I}_{\mathscr{A}}}\delta_{(\mu A)_j,(\mu' A)_j}(-1)^{\alpha(\mu)+\alpha(\mu')}|(\mu A)_{\mathscr{B}}\rangle\langle(\mu A)_{\mathscr{B}}|,$$

且 $|(\mu A)_{\mathscr{B}}\rangle = \left|(\mu A)_{\mathscr{I}_{m+1}},\ldots(\mu A)_{\mathscr{I}_n}\right\rangle$.

为了得到它的熵, 对角化 $\rho_{\mathscr{B}}$. 不失一般性, 设 $\mathscr{I}_1 = 1$, $\mathscr{I}_2 = 2$, $\mathscr{I}_m = m\leqslant r$, 且记 $\mu = (\nu,\tau)$, 其中 $\nu = (\mu_1,\ldots,\mu_m), \tau = (\mu_{m+1},\ldots,\mu_r)$. 则 $|(\mu A)_{\mathscr{B}}\rangle = |\mu_{m+1},\ldots,\mu_r,(\mu D)_1,\ldots,(\mu D)_{n-r}\rangle = |\tau,\mu D\rangle$. 记 $|\Psi(\nu)\rangle = \sum_\tau(-1)^{\alpha(\mu)}\,|(\mu A)_{\mathscr{B}}\rangle$, 则

$$\begin{aligned}\rho_{\mathscr{B}} &= \sum_{\nu,\nu',\tau,\tau'}\delta_{\nu,\nu'}(-1)^{\alpha(\mu)+\alpha(\mu')}\,|(\mu A)_{\mathscr{B}}\rangle\,\langle(\mu A)_{\mathscr{B}}|\\ &= \sum_{\nu,\nu'}\delta_{\nu,\nu'}\,|\Psi(\nu)\rangle\,\langle\Psi(\nu')| = \sum_{\nu}|\Psi(\nu)\rangle\,\langle\Psi(\nu)|.\end{aligned}$$

对于 $|\Psi(\nu)\rangle$ 态的正交性, 考虑

$$\begin{aligned}\langle\Psi(\nu')\,|\Psi(\nu)\rangle &= \sum_{\tau,\tau'}(-1)^{\alpha(\mu)+\alpha(\mu')}\delta_{\tau\tau'}\delta_{\mu D,\mu' D}\\ &= \sum_{\tau}(-1)^{\alpha(\nu,\tau)+\alpha(\nu',\tau)}\delta_{(\nu,\tau)D,(\nu',\tau)D}.\end{aligned} \tag{15}$$

当所有的 $|\Psi(\nu)\rangle$ 态之间相互正交时, 码字的二组分纠缠至少为 m, 这由下式可知

$$\rho_{\mathscr{B}} = \frac{1}{2^m}\sum_{\nu=(0,0,\cdots,0)}^{(1,1,\cdots,1)}|\Psi(\nu)\rangle\,\langle\Psi(\nu)|,$$

式中 $|\Psi(\nu)\rangle$ 是正交归一化的. 仅当一些 $|\Psi(\nu)\rangle$ 态之间非正交时, 二组分纠缠才可能小于 m. $\langle\Psi(\nu')\,|\Psi(\nu)\rangle$ 不为零的条件是

$$(\nu+\nu',\mathbf{0})D = 0, \tag{16}$$

$$(\nu+\nu')\Gamma_3 = 0, \tag{17}$$

其中 $\mathbf{0}$ 表示 $r-m$ 维零矢量 $(0,0,\cdots,0)$. Γ_3 是通过删除 $r\times r$ 矩阵 Γ_1 的前 m 列和后 $(r-m)$ 行得到的. 故 Γ_3 是矩阵 Γ_1 的 $m\times(r-m)$ 子矩阵. 更明确地可以将 Γ_1 写为

$$\Gamma_1 = \begin{bmatrix}\Gamma_2 & \Gamma_3\\ \Gamma_3^{\mathrm{T}} & \Gamma_4\end{bmatrix}.$$

故 $\alpha(\nu,\tau)+\alpha(\nu',\tau) = \frac{1}{2}(\nu\Gamma_2\nu^{\mathrm{T}} + \nu'\Gamma_2\nu'^{\mathrm{T}}) + (\nu+\nu')\Gamma_3\tau^{\mathrm{T}} + \tau\Gamma_4\tau^{\mathrm{T}}$. 因 Γ_4 是对称的并且对角元为零, Γ_4 项在方程 (15) 的求和中总是贡献 $+1$ 因子. 而 Γ_2 项在方程 (15) 的求和中贡献一个常数因子. 故有 (17) 式. 令 D' 是 D 通过删除其最末 $r-m$ 行而保留 D 的前 m 行而得到的矩阵, 对于 $\mathscr{A}$ 含前 m 个量子比特而 $\mathscr{B}$ 含后 $n-m$ 个量子比特这样一种 2 组分划分, $m\times(n-m)$ 矩阵 $Q(\mathscr{A},\mathscr{B}) = (\Gamma_3, D')$ 的秩确定了独立矢量 $|\Psi(\nu)\rangle$ 的数目. 对除 $m>r$ 情况之外的所有二组分划分的秩取最大值, 得到最大的二组分纠缠并将其作为总纠缠的下界.

$$E_l = \max[rank_{\mathbb{F}_2}Q(\mathscr{A},\mathscr{B})]. \tag{18}$$

因 $Q(\mathscr{A},\mathscr{B})$ 是一个 $m\times(n-m)$ 矩阵, 其秩不超过 $\min\{m,n-m\}\leqslant\lfloor\frac{n}{2}\rfloor$, 故有 $E_l\leqslant\lfloor\frac{n}{2}\rfloor$.

考虑当 $r=m$ 的特殊情况, 则 Γ_3 是一个 $r\times 0$ 阶矩阵因此不存在. 因此方程 (17) 消失, 只要考虑方程 (16). 如果 $rank_{\mathbb{F}_2}D = r$, 则仅当 $\nu=\nu'$ 时, 方程 (16) 是成立的. 故有 $E_l = r$.

5 CSS 码字纠缠

5.1 对偶包含 CSS 码

量子码中重要的一类是用经典码构造的, 由 Calderbank, Shor[22] 和 Steane[23] 等人提出, 其具有的生成元矩阵形式为 [24]

$$(A|B)=\left(\begin{array}{c|c} U & 0 \\ 0 & V \end{array}\right), \tag{19}$$

其中 U 和 V 是 $l\times n$ 矩阵. 要求 $UV^{\mathrm{T}}=0$ 确保了生成元之间的相互对易. 因为有 $2l$ 个稳定子条件作用于 n 个量子比特的态, 编码将 $k=n-2l$ 个量子比特编入为 n 个量子比特态. 可以将经典奇偶校验矩阵 U 写成系统形式,

$$U=\left[\begin{array}{cc} I & D \end{array}\right]. \tag{20}$$

因为 $AB^{\mathrm{T}}=0$, 对于所有的二进制矢量 μ 得到 $\alpha(\mu)=0$. 当 $m=l$ 时, $\nu=\mu$. 故 $\langle\Psi(\nu')|\Psi(\nu)\rangle=\delta_{\nu D,\nu' D}$. 由 $\nu D=\nu' D$, 得出 $(\nu+\nu')D=0$. 因此 $|\Psi(\nu)\rangle$ 相互正交的条件为

$$\nu D=0\ \Rightarrow\ \nu=0, \tag{21}$$

对于所有的二进制矢量 ν 成立. 当条件 (21) 成立时, 码字纠缠的下界为 l. 对于对偶包含码有 $V=U$, 所以 $UU^{\mathrm{T}}=0$, 即 $DD^{\mathrm{T}}=I$, 满足 (21) 式. 纠缠的下界为 $E_l=l=\frac{n-k}{2}$.

码字 $|\overline{0}\rangle$ 的纠缠上界 E_u 为 X 生成元的个数, 即为 l. 因而 CSS 对偶包含码的码字纠缠为

$$E=\frac{n-k}{2}. \tag{22}$$

若 CSS 码不是对偶包含码, 纠缠上界 E_u 仍为 X 生成元的个数 l, 下界为二进制矩阵 D 的秩.

5.2 CSS 码的图态

具有稳定子生成元 $M_1,\cdots,M_{n-k}$ 以及逻辑算符 $\overline{X}_1,\cdots,\overline{X}_k$ 和 $\overline{Z}_1,\cdots,\overline{Z}_k$ 的稳定子码与根据码字稳定子 $\{M_1,\cdots,M_{n-k},\overline{Z}_1,\cdots,\overline{Z}_k\}$ 和 $\overline{X}_i$ 的乘积构成的字算符所定义的码字稳定子码 (CWS) 是等价的 [1]. 任何 CWS 码与标准形式的 CWS 码是局域 Clifford 等价的, 后者由图态稳定子和仅含 Z 算符的字算符构成. 标准稳定子码字由 $X_iZ^{\boldsymbol{r}_i}$ 生成. 矢量集合 $\boldsymbol{r}_i$ 形成 CWS 图态 [1] 的邻接矩阵. 因此, 给定一个量子稳定子纠错码, 能找到它相应的图态. 量子稳定子码的码字纠缠和图态纠缠是类似的, 因为它们局域 Clifford 等价. CSS 码具有生成元矩阵 (19), 且 U 可以进一步写为式 (20) 的形式. 现在来构建图态的稳定子. $\{M_1,\cdots,M_{n-k},\overline{Z}_1,\cdots,\overline{Z}_k\}$ 的生成元矩阵为

$$\left(\begin{array}{c|c} U & 0 \\ 0 & V \\ 0 & W \end{array}\right), \tag{23}$$

其中 $(0\,|W)$ 是逻辑算符 $\overline{Z}_1,\cdots,\overline{Z}_k$ 的生成元矩阵. 经过初等行变换, 将 U 转变为系统形式 $\left[\begin{array}{cc} I & D \end{array}\right]$. 同时表明将 $\left[\begin{array}{c} V \\ W \end{array}\right]$ 转变为 $\left[\begin{array}{cc} D' & I \end{array}\right]$ 的形式是可以的, 这里 I 是 $(n-l)\times(n-l)$ 单位矩阵. 先将 $\left[\begin{array}{c} V \\ W \end{array}\right]$ 转换为 $\left[\begin{array}{cc} R & P \end{array}\right]$, 其中 P 是一个上三角方阵, 即当 $i>j$ 时 $P_{ij}=0$. 当 $P_{jj}=0$ 时, 将第 j 个量子比特与其后的量子比特互换, 从而得到 $P_{jj}=1$. 这总是可行的, 因为 P 的第 j 行元素不会全为零, 否则 $\left[\begin{array}{cc} R & P \end{array}\right]$ 的第 j 行元素就全为零. 这是由于生成元彼此对易, 即 $UV^{\mathrm{T}}=0$ 和 $UW^{\mathrm{T}}=0$. 也就是说

$$IR^{\mathrm{T}}+DP^{\mathrm{T}}=0. \tag{24}$$

从上面的等式可以推导出如果 P 的第 j 行元素全为零的话, 那么对于所有的 $i\leqslant l$ 有 $R_{ji}=0$. 在 $\left[\begin{array}{cc} R & P \end{array}\right]$ 中, 一个全零的行意味着这一行的生成元为恒等算子, 这显然不对. 很容易将 $\left[\begin{array}{cc} R & P \end{array}\right]$ 转换为 $\left[\begin{array}{cc} D' & I \end{array}\right]$, 那么方程 (24) 可以写为

$$D'=D^{\mathrm{T}}.$$

对后面的 $n-l$ 个量子比特进行 Hadamard 转换, 生成元矩阵所受转换为

$$\left(\begin{array}{cc|cc} I & D & 0 & 0 \\ 0 & 0 & D^{\mathrm{T}} & I \end{array}\right)\Rightarrow\left(\begin{array}{cc|cc} I & 0 & 0 & D \\ 0 & I & D^{\mathrm{T}} & 0 \end{array}\right).$$

因此, CSS 码字的局域 Clifford 等价图态的邻接矩阵为

$$\gamma=\begin{bmatrix}0 & D\\ D^{\mathrm{T}} & 0\end{bmatrix}. \tag{25}$$

邻接矩阵 (25) 式表示的图态是双色可染色图的图态, 给前 l 个量子比特一种颜色, 剩下的 $n-l$ 个量子比特为另一种颜色. 纠缠的上界为 $E_u=n-(n-l)=l$[25]. 纠缠的二组分划分下界为 [3]$E_l=\frac{1}{2}rank_{F_2}\gamma=rank_{F_2}D$.

对于一个对偶包含 CSS 码, 除双色可染色图外, 其相应的图态还有一个特点是 $DD^{\mathrm{T}}=I$. 故 D 是满秩矩阵, 而且纠缠的上下界是一致的. 由图态理论和公式 (25) 也可以确定码字纠缠是 $E=l$.

5.3 Toric 码

Toric 码的提出是为了将量子信息编码于拓扑结构中而得到保护 [26], 它是一种量子 LDPC 码 [24]. Toric 码是一种基于将 $k\times k$ 正方点阵嵌入到轮胎面上的码. 点阵的每条边都携带一个量子比特, 故共有 $n=2k^2$ 个量子比特. 对于每个顶点 s 和每个面 p 定义如下形式的算符:

$$A_s=\prod_{j\in \mathrm{star}(s)}X_j,\ B_p=\prod_{j\in \mathrm{boundary}(p)}Z_j.$$

这些算符之间是相互对易的, 其中 star(s) 是顶点 s 的连接边, boundary(p) 是面 p 的围边. 由 $\prod_s A_s=1$ 和 $\prod_p B_p=1$ 知, 共有 $m=2k^2-2$ 个独立的算符构成 Toric 码的稳定子. 它编码了 $n-m=2$ 个量子比特. 从它的定义看出 Toric 码是一种 CSS 码, 想要说明的是 Toric 码不是一个对偶包含码, 且它纠缠上下界是不一致的. 通过适当地给边编号, 生成元矩阵可以写为如下形式

$$U=\begin{bmatrix}
I & & & & I & \Omega & & & & \\
I & I & & & & & \Omega & & & \\
 & \ddots & \ddots & & & & & \ddots & & \\
 & & I & I & & & & & \Omega & \\
 & & & I' & I' & & & & & \Omega'
\end{bmatrix},$$

$$V=\begin{bmatrix}
\Omega^{\mathrm{T}} & & & & I & & & & I \\
 & \Omega^{\mathrm{T}} & & & I & I & & & \\
 & & \ddots & & & & \ddots & \ddots & \\
 & & & \Omega^{\mathrm{T}} & & & & I & I \\
 & & & & \Omega^{\mathrm{T}\prime} & & & & I' & I'
\end{bmatrix}.$$

其中 I 是 $k\times k$ 单位矩阵, Ω 是有 $2k$ 个非零元素的 $k\times k$ 阶矩阵,

$$\Omega=\begin{bmatrix}
1 & & & & 1 \\
1 & 1 & & & \\
 & \ddots & \ddots & & \\
 & & & 1 & 1
\end{bmatrix},$$

其中 I',Ω' 和 $\Omega^{\mathrm{T}\prime}$ 是分别通过删除 I,Ω 和 Ω^{T} 的最后一行得到的. 为了说明一般情况下 D 不是满秩矩阵, 通过初等行变换将它转变为以下形式:

$$\begin{bmatrix}
I & & & & \Omega \\
 & \Omega & & & \\
 & & \ddots & & \\
 & & & \Omega & \\
0 & \Delta & \cdots & \Delta & \Delta & \mathbf{1}
\end{bmatrix},$$

其中 $\mathbf{1}=(1,1,\cdots,1)^{\mathrm{T}}$ 是 $k-1$ 维的列矢量, $\Delta=[I_{k-1},\mathbf{1}]$. 很明显 $(k^2-1)\times(k^2+1)$ 矩阵 D 不是一个满秩矩阵, 因为矩阵 Ω 的秩为 $k-1$, 得到纠缠的下界为

$$E_l=k^2-k+1.$$

因为 X 型生成元数, 纠缠的上界为 $E_u=k^2-1$. 最近通过其他方法证明下界也是 k^2-1, 码字精确的纠缠值确定为 $E=E_u=k^2-1$ [27].

6 Gottesman 码和相关码的码字纠缠

6.1 Gottesman 码

Gottesman[28] 提出一种达到量子 Hamming 界的量子编码的参数为 $[[2^m,2^m-m-2,3]]$ $(m\geqslant 3)$. 由定义, 前两个稳定子生成元为 $X_1\cdots X_{2^m}$ 和 $Z_1\cdots Z_{2^m}$. 其余 m 个生成元的详细构造由矩阵 $(H|CH)$ 给定, 其中 $H=[h_0,h_1,\cdots,h_{2^m-1}]$ 且第 $(k+1)$ 列 h_k 是表示整数

$k(k=0,1,\cdots,2^m-1)$ 的二进制矢量, C 为任意的可逆的 $m\times m$ 无定点自由矩阵, 即对除 $s=0$ 的所有 $s\in\mathbb{F}_2^m$ 有 $Cs\neq 0$ 和 $Cs\neq s$. 生成元 $Z_1\cdots Z_{2^m}$ 为 Z 型生成元, 下面关于码字纠缠的讨论将忽略它. 可以将 H 通过量子比特重新编号变换为 $H=[H_0,H_1,H_2,\cdots H_m]$, 其中 $H_0=h_0=[0,0,\cdots,0]^{\mathrm{T}}$, $H_1=[h_{2^{m-1}},h_{2^{m-2}},\cdots,h_2,h_1]=I_{m\times m}$, 且 H_j 是 $m\times\binom{m}{j}$ 矩阵, 其列矢量的重量为 j. 后 m 个生成元的生成元矩阵的标准形式为 $(I\ D\mid F\ G)$, 且 $D=[H_2\ H_3\ \cdots\ H_m], F=C, G=CD$,

$$F^{\mathrm{T}}+DG^{\mathrm{T}}=0. \tag{26}$$

已经利用了矩阵 H 的任何两列是正交的事实, 而且 H 的每行重量为偶数, 所以 $\sum_{i=1}^m H_iH_i^{\mathrm{T}}=0$, 和 $\sum_{i=2}^m H_iH_i^{\mathrm{T}}=H_1H_1^{\mathrm{T}}=I$. 方程 (26) 和生成元 $X_1\cdots X_{2^m}$ 不包含任何 Z 算符的事实导致

$$\alpha(\mu)=0,$$

对于所有的 $m+1$ 维二进制矢量 μ 都成立. 为了得到 Gottesman 码字纠缠的下界, 需要验证条件 (21) 是否满足. 将生成元 $X_1\cdots X_{2^m}$ 包含在内, 则 $m+1$ 个生成元的 D 矩阵为

$$D=\begin{bmatrix}\mathbf{1} & \mathbf{0} & \cdots & (\boldsymbol{m}-1)_{\mathbb{F}_2}\\ H_2 & H_3 & \cdots & H_m\end{bmatrix},$$

其中 $\mathbf{1}$ 和 $\mathbf{0}$ 分别是有恰当维数的向量 $(1,1,\cdots,1)$ 和 $(0,0,\cdots,0)$. 进而得到

$$DD^{\mathrm{T}}=\begin{bmatrix}\sum_{i=1}^{m'}\binom{m}{2i} & \sum_{i=1}^{m'}\mathbf{1}H_{2i}^{\mathrm{T}}\\ \sum_{i=1}^{m'}H_{2i}\mathbf{1}^{\mathrm{T}} & \sum_{i=2}^{m}H_iH_i^{\mathrm{T}}\end{bmatrix},$$

其中 $m'=\lfloor m/2\rfloor$. 注意 m 维矢量 $H_{2i}\mathbf{1}^{\mathrm{T}}$ 的第 l 个元素正好是 H_{2i} 的第 l 行的重量, 根据 H 的定义, H_{2i} 的每一行都有相同的重量 t_i, H_{2i} 的每一列都有相同的重量 $2i$, 所以, $mt_i=2i\binom{m}{2i}$ 是矩阵 H_{2i} 的总重量. 故 $t_i=\binom{m-1}{2i-1}$, 且 $\sum_{i=1}^{m'}H_{2i}\mathbf{1}^{\mathrm{T}}=\sum_{i=1}^{m'}t_i=\sum_{i=1}^{m'}\binom{m-1}{2i-1}=2^{m-2}$, 该项当 $m\geqslant 3$ 时在 $\mathbb{F}_2$ 域中等于 0. 因此 $\sum_{i=1}^{m'}H_{2i}\mathbf{1}^{\mathrm{T}}=\mathbf{0}^{\mathrm{T}}$. 同时 $\sum_{i=1}^{m'}\binom{m}{2i}=\sum_{i=0}^{m'}\binom{m}{2i}-1=2^{m-1}-1$, 该项当 $m\geqslant 2$ 时在 $\mathbb{F}_2$ 域中等于 1. 得到

$$DD^{\mathrm{T}}=I,$$

条件 (21) 满足. Gottesman 码字的纠缠下界为 $m+1$. 非 Z 型生成元的个数为 $m+1$ 个, 所以码字的纠缠上界为 $m+1$. 得到结论 Gottesman$[[2^m,2^m-m-2,3]]$ $(m\geqslant 3)$ 码的码字纠缠为 $m+1$. 用编码长度 $n=2^m$ 表示, 码字的纠缠为

$$E=\log_2 n+1. \tag{27}$$

6.2 8*m* 系列量子码

文献 [29] 中构造了参数为 $[[8m,8m-l_m-5,3]]$, $l_m=\lceil\log_2 m\rceil$ 的一族码. 该码的另一种生成元矩阵也已构造出来 [30](基于 Gottesman 码的方法). 稳定子生成元的个数为 l_m+5, 其中有一个 Z 型生成元. 因此码字纠缠的上界 (可能不是紧的) 为 $E_u=l_m+4$. 为了得到纠缠的下界, 直接利用文献 [30] 中的生成元矩阵而不是将它们转换为如方程 (8) 的标准形式. 该码可以分为 m 块, 每块有 8 个量子比特. 生成元矩阵可以写为

$$(A\mid B)=(A_1,A_2,\cdots,A_m\mid B_1,B_2,\cdots,B_m), \tag{28}$$

其中 A_i 和 B_i 是 $(l_m+5)\times 8$ 二进制矩阵, 而且 $(A_i\mid B_i)$ 的每行要么是取自 Gottesman[[8, 3, 3]] 码的生成元矩阵, 要么对应于 $I^{\otimes 8}, X^{\otimes 8}, Y^{\otimes 8}$ 或 $Z^{\otimes 8}$. 可以看出对于所有的 i,j 有 $A_iA_j^{\mathrm{T}}=0, A_iB_j^{\mathrm{T}}=0, B_iB_j^{\mathrm{T}}=0$. 于是有

$$\Gamma=AB^{\mathrm{T}}=\sum_i A_iB_i^{\mathrm{T}}=0. \tag{29}$$

因此对于任意的二进制矢量 μ, 有 $\alpha(\mu)=0$ 成立. 同时, 也有 $\sum_i A_iA_i^{\mathrm{T}}=0$, 因而

$$AA^{\mathrm{T}}=0. \tag{30}$$

注意对 A 进行行初等变换仍满足等式 (30). 行初等变换后, A 可以转换为标准形式

$$A\mapsto A'=\begin{bmatrix}I & D\\ 0 & 0\end{bmatrix}. \tag{31}$$

因此

$$A'A'^{\mathrm{T}}=\begin{bmatrix}I+DD^{\mathrm{T}} & 0\\ 0 & 0\end{bmatrix}=0,$$

且

$$DD^{\mathrm{T}} = I. \tag{32}$$

方程 (31) 中单位矩阵的维数至关重要. 有一个明显的 Z 型生成元, 从方程 (31) 和 (32) 中的单位矩阵来看, A 矩阵的秩为 l_m+4. 根据方程 (29) 和 (32), 纠缠下界为 $E_l = l_m+4$, 与上界纠缠值一致. 因此, 长度为 $n=8m$ 这族码的码字纠缠值为

$$E = \lceil \log_2 n \rceil + 1. \tag{33}$$

注意方程 (27) 描述的 Gottesman 码码字纠缠可以合并到方程 (33) 中.

6.3 粘贴码

$[[13,7,3]]$ 码是通过粘贴 Gottesman$[[8,3,3]]$ 码和循环 $[[5,1,3]]$ 码而得到的 [31]. 对于 $[[13,7,3]]$ 码的码字纠缠, 在 6 个生成元中有一个 Z 型生成元, 它的上界为 $E_u = 5$. 直接计算表明它的下界值 E_l 也为 5. 所以得出纠缠值 $E=5$, 验证了方程 (33).

完备码族 $[[n_m, n_m-2m, 3]]$, 其中 $n_m = (4^m-1)/3$, 当 $m \geqslant 3$ 时, 可通过将 Gottesman $2^{2(m-1)}$ 码 (在不复杂的情况下, 偶尔会用长度来表示码) 与 n_{m-1} 码 [21,31] 粘贴得到. n_m 码的码字纠缠的上界为 $E_u = 2m-1$, 因为有 $2m$ 个生成元且只有一个是 Z 型生成元. 至于它的纠缠下界, 首先考虑 $[[21,15,3]]$ 码, 它由 $[[5,1,3]]$ 循环码与 Gottesman2^4 码粘帖得到. 可以运用第 4 节提及的特殊情况, 有 $E_l = rank_{\mathbb{F}_2} D = 5$, 注意 Z 型生成元已经被去掉了. 同样地, 对于 n_m 码, 有 $E_l = 2m-1$. 所以纠缠值为 $E=2m-1$, 且以码长 $n=n_m$ 表示的纠缠可以写为

$$E = \lceil \log_2 n \rceil. \tag{34}$$

另外一类码 $[[8n_m, 8n_m-2m-3, 3]]$, 当 $m \geqslant 3$ 时, 可通过将 $8n_{m-1}$ 个码 [21] 与 Gottesman 2^{2m+1} 码粘贴得到. 根据 $8n_m$ 码的结构可知粘贴码的纠缠上界由 Gottesman 2^{2m+1} 码的非 Z 型生成元的个数决定, 纠缠的上界为 $E_u = 2m+2$. 纠缠的下界值也是 $E_l = 2m+2$, 由于该码是由 Gottesman 码粘贴而成, 通过和 6.2 节相似的方式得到纠缠的下界值为 $E_l = 2m+2$. 因而纠缠值为 $E=2m+2$, 且相应以码长 $n=8n_m$ 表示的纠缠可以写为方程 (34) 的形式.

7 纠缠的迭代算法

将码字 $|\overline{0}\rangle$ 和它的最近乘积态 $|\Phi_S\rangle$ 的内积表示为 $f = \langle\overline{0}|\Phi_S\rangle$, 其中 $|\Phi_S\rangle = \bigotimes_j (x_j|0\rangle + y_j|1\rangle)$ 且 $|x_j|^2 + |y_j|^2 = 1$. 由拉格朗日乘子法, 设 $L = |f|^2 - \sum_j \lambda_j(|x_j|^2 + |y_j|^2 - 1)$, 其中 λ_j 为乘子. 极值方程为 $\frac{\partial f}{\partial x_j} f^* - \lambda_j x_j^* = 0$, $\frac{\partial f}{\partial y_j} f^* - \lambda_j y_j^* = 0$. 令 $z_j = y_j/x_j$, 得到

$$z_j^* = \frac{\partial f/\partial y_j}{\partial f/\partial x_j}. \tag{35}$$

因为群元素 $M_1^{\mu_1} M_2^{\mu_2} \cdots M_{n-k}^{\mu_{n-k}}$ 与 $(\mu A|\,\mu B)$ 是同构的. 其中 $\mu = (\mu_1, \mu_2, \cdots, \mu_{n-k})$ 为二进制矢量. μA 和 μB 是长度为 n 的二进制矢量. 所以

$$\begin{aligned} f &= \mathcal{N}\langle 0|^{\otimes n} \prod_{i=1}^{n-k}(I+M_i) \bigotimes_{j=1}^{n}(x_j|0\rangle + y_j|1\rangle) \\ &= \mathcal{N}\sum_{\mu=\mathbf{0}}^{\mathbf{1}} \langle 0|^{\otimes n} Z^{\mu B} X^{\mu A} (-1)^{\alpha(\mu)} (-i)^{\mu\cdot g} \\ &\quad \bigotimes_{j=1}^{n}(x_j|0\rangle + y_j|1\rangle) \\ &= \mathcal{N}\sum_{\mu=\mathbf{0}}^{\mathbf{1}} (-1)^{\alpha(\mu)} (-i)^{\mu\cdot g} \langle 0|^{\otimes n} X^{\mu A} \\ &\quad \bigotimes_{j=1}^{n}(x_j|0\rangle + y_j|1\rangle) \\ &= \mathcal{N}\sum_{\mu=\mathbf{0}}^{\mathbf{1}} (-1)^{\alpha(\mu)} (-i)^{\mu\cdot g} \prod_{j=1}^{n} x_j^{1-(\mu A)_j} y_j^{(\mu A)_j}. \end{aligned} \tag{36}$$

这里 $g = (g_1, \cdots, g_{n-k})$, g_i 是 M_i 中 Y 算符的个数. 从 (35) 式看出, 对于 z_j, 迭代方程为

$$z_j^* = \frac{\sum\limits_{\mu|(\mu A)_j=1} (-1)^{\alpha(\mu)} (-i)^{\mu\cdot g} \prod\limits_{m\neq j} z_m^{(\mu A)_m}}{\sum\limits_{\mu|(\mu A)_j=0} (-1)^{\alpha(\mu)} (-i)^{\mu\cdot g} \prod\limits_{m\neq j} z_m^{(\mu A)_m}}. \tag{37}$$

注意有时候迭代不会达到 $|f|^2$ 的全局最大值. 所以如果最后的迭代结果分离态 $|\Phi_S\rangle$ 是 $|\overline{0}\rangle$ 的最近乘积态, 从迭代算法中得到量子码码字纠缠为

$$\begin{aligned} E &= -\log_2 |f_*|^2 = n-k-n_s \\ &\quad -2\log_2 \left| \sum_{\mu=\mathbf{0}}^{\mathbf{1}} (-1)^{\alpha(\mu)} \prod_{j=1}^{n} x_{j*}^{1-(\mu A)_j} y_{j*}^{(\mu A)_j} \right|. \end{aligned} \tag{38}$$

表 1 码字纠缠及其上下界和编码复杂度

Table 1 The entanglement of codewords, their entanglement upper and lower bounds and quantum coding complexities

$[[n,k,d]]$	E	E_u	E_l	C
$[[4,1,2]]$	2	2	2	3
$[[4,2,2]]$	2	2	2	2
$[[5,1,3]]$	2.9275	3	2	4
$[[5,2,2]]$	2	2	2	2
$[[6,1,3]]$	2.9275	3	2	4
$[[6,2,2]]$	3	3	3	3
$[[6,3,2]]$	2	2	2	4
$[[6,4,2]]$	2	2	2	4
$[[7,1,3]]$	3	3	3	5
$[[7,2,2]]$	4	4	3	5
$[[7,3,2]]$	4	4	3	6
$[[7,4,2]]$	3	3	3	6
$[[8,1,3]]$	5	5	4	7
$[[8,2,3]]$	4.8549	5	4	7
$[[8,4,2]]$	4	4	4	4
$[[8,5,2]]$	3	3	3	7
$[[8,6,2]]$	2	2	2	7
$[[9,1,3]]$	5	5	4	8
$[[9,2,3]]$	5	5	4	8
$[[9,3,3]]$	5	5	4	9
$[[9,4,2]]$	4	4	4	4
$[[9,5,2]]$	3	3	3	7
$[[9,6,2]]$	2	2	2	7

n_s 为 Z 型生成元的个数, f_*, x_{j*} 和 y_{j*} 分别是 f, x_j 和 y_j 在极值点的值.

由 Grassl(见脚注 1)) 列出的一些量子编码的码字纠缠见表 1(其中 E, E_u, E_l 表示纠缠及其上下界, C 表示量子编码复杂度). 迭代算法用于计算上下界不相等时的纠缠. 由表 1 可见, 量子编码复杂度不小于码子的纠缠.

8 结论

对于量子稳定子码字, 证明了三种纠缠测度 (几何纠缠, 对数鲁棒纠缠和相对熵纠缠) 是等价的. 我们从 9 量子比特以下的量子码归纳出规律: 量子编码复杂度 (这里指双量子比特及多量子比特逻辑门的数目) 以码字纠缠量为其下界. 稳定子码字纠缠的上界是由非 Z 型生成元的最小个数决定的. 一种更紧的上界是所谓泡利韧性, 它是将态分解为分离态所需泡利测量的最小数目. 基于二组分划分导出的纠缠下界, 被化简为计算一类二进制矩阵的最小秩, 这些矩阵由稳定子码的生成元矩阵推导而来. 证明 CSS 对偶包含码的纠缠为其 X 生成元的个数, 可直接由经典码的校验矩阵确定. 推导出一个 CSS 码的相关图态的邻接矩阵. 研究了 Toric 码纠缠的上下界. Gottesman 码 $[[2^m, 2^m-m-2, 3]](m \geqslant 3)$, $8m$ 码和 Gottesman 粘帖码的纠缠值都等于其非 Z 型生成元的最小个数. 对 Gottesman 码及其相关码, 其码字纠缠与码长 n 的关系为 $E = \lceil \log_2 n \rceil + 1$ 或 $E = \lceil \log_2 n \rceil$. 当纠缠的上下界不等时, 发展了迭代算法去计算码字纠缠的值.

参考文献

1 Cross A, Smith G, Smolin J A, et al. Codeword stabilized quantum codes. IEEE Trans Inf Theor, 2009, 55: 433–438

2 Bell B A, Herrera-Martí D A, Tame M S, et al. Experimental demonstration of a graph state quantum error-correction code. Nat Commun, 2014, 5: 3658

3 Hein M, Eisert J, Briegel H J. Multiparty entanglement in graph states. Phys Rev A, 2004, 69: 062311

4 Hein M, Dur W, Eisert J, et al. Entanglement in graph states and its applications. arXiv:quant-ph/0602096

5 Hayashi M, Markham D, Murao M, et al. Entanglement of multiparty-stabilizer, symmetric, and antisymmetric states. Phys Rev A, 2008, 77: 012104

6 Chen X Y. Entanglement of graph states up to eight qubits. J Phys B, 2010, 43: 085507

7 Leng R G, Ma Z. Constructions of new families of nonbinary asymmetric quantum BCH codes and subsystem BCH codes. Sci China-Phys Mech Astron, 2012, 55: 465–469

8 Vidal G, Tarrach R. Robustness of entanglement. Phys Rev A, 1999, 59: 141–155
9 Vedral V, Plenio M B, Rippin M A, et al. Quantifying Entanglement. Phys Rev Lett, 1997, 78: 2275–2279
10 Vedral V, Plenio M B. Entanglement measures and purification procedures. Phys Rev A, 1998, 57: 1619–1633
11 Wei T C, Goldbart P M. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. Phys Rev A, 2003, 68: 042307
12 Cao Y, Li H, Long G L. Entanglement of linear cluster states in terms of averaged entropies. Chin Sci Bull, 2013, 58: 48–52
13 Liu D, Zhao X, Long G L. Multiple entropy measures for multi-particle pure quantum state. Commun Theor Phys, 2010, 54: 825–828
14 Wei T C, Ericsson M, Goldbart P M, et al. Connections between relative entropy of entanglement and geometric measure of entanglement. Quant Inform Comp, 2004, 4: 252–266
15 Hayashi M, Markham D, Murao M, et al. Bounds on multipartite entangled orthogonal state discrimination using local operations and classical communication. Phys Rev Lett, 2006, 96: 040501
16 Wei T C. Relative entropy of entanglement for multipartite mixed states: Permutation-invariant states and dür states. Phys Rev A, 2008, 78: 012327
17 Zhang J, Wei T C, Laflamme R. Experimental quantum simulation of entanglement in many-body systems. Phys Rev Lett, 2011, 107: 010501
18 Daley A J, Pichler H, Schachenmayer J, et al. Measuring entanglement growth in quench dynamics of bosons in an optical lattice. Phys Rev Lett, 2012, 109: 020505
19 Gottesman D. Stabilizer codes and quantum error correction. arXiv: quant-ph/9705052
20 Markham D. Entanglement and symmetry in permutation-symmetric states. Phys Rev A, 2011, 83: 042332
21 Calderbank A R, Rains E M, Shor P W, et al. Quantum error correction via codes over GF(4). IEEE Trans Inf Theor, 1998, 44: 1369–1387
22 Calderbank A R, Shor P W. Good quantum error-correcting codes exist. Phys Rev A, 1996, 54: 1098–1105
23 Steane A. Multiple-particle interference and quantum error correction. Proc R Soc Lond A, 1996, 452: 2551–2577
24 MacKay D J C, Mitchison G, McFadden P L. Sparse-graph codes for quantum error correction. IEEE Trans Inf Theor, 2004, 50: 2315–2330
25 Markham D, Miyake A, Virmani S. Entanglement and local information access for graph states. New J Phys, 2007, 9: 194
26 Kitaev A Y. Fault-tolerant quantum computation by anyons. Ann Phys, 2003, 303: 2–30
27 Orus R, Wei T C, Buerschaper O, et al. Geometric entanglement in topologically ordered states. New J Phys, 2014, 16: 013015
28 Gottesman D. Class of quantum error-correcting codes saturating the quantum Hamming bound. Phys Rev A, 1996, 54: 1862–1868
29 Li R, Li X. Binary construction of quantum codes of minimum distance three and four. IEEE Trans Inf Theor, 2004, 50: 1331–1335
30 Yu S, Bierbrauer J, Dong Y, et al. All the stabilizer codes of distance 3. IEEE Trans Inf Theor, 2013, 59: 5179–5185
31 Gottesman D. Pasting quantum codes. arXiv: quant-ph/9607027

Entanglement of stabilizer codewords

CHEN XiaoYu*

College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

Quantum communication and quantum computation are two important parts of quantum information science. Quantum algorithm usually uses real equally weighted states, among them are graph states, whose entanglement is well studied. Quantum communication is inevitably connected with quantum error correcting codes (QECC). The most important and frequently used QECCs are quantum stabilizer codes, which can be seen as the combination of graph states with classical error correcting codes. We argue that the complexity of quantum coding is closely related to the entanglement of the code. We prove that entanglement measured by the geometric measure, the robustness and the relative entropy of entanglement are equal for a stabilizer quantum codeword. The entanglement upper and lower bounds are determined from the generators of a quantum code. CSS codes are quantum codes derived from classical codes. We prove that the entanglement of CSS code equals its number of classical generators when the CSS code is dual-containing. We give the entanglement of codewords for Gottesman codes and related codes. An iterative algorithm is developed to calculate the entanglement numerically.

quantum code, multipartite entanglement, entanglement measure

PACS: 03.67.Mn, 03.65.Ud, 03.67.Ac

doi: 10.1360/SSPMA2014-00327