差错基、量子码与群代数*

李卓† 邢莉娟

(西安电子科技大学, 综合业务网理论及关键技术国家重点实验室, 西安 710071)

(2012 年 8 月 8 日收到; 2013 年 2 月 27 日收到修改稿)

本文找到了一种研究优质差错基和量子纠错码的新方法, 即群代数方法, 它为差错基和量子码提供了一种代数表示. 利用这种代数表示, 建立了一系列关于最一般量子纠错码的线性规划限.

关键词: 群代数, 差错基, 量子纠错码, 量子信息

PACS: 03.67.Pp, 03.67.Hk, 03.67.Lx **DOI:** 10.7498/aps.62.130306

1 引 言

搭建一台能够抵抗消相干和量子噪声的实用量子计算机的需求已经极大的刺激了对于量子纠错码研究的兴趣 [1−9]. 虽然任意差错算子都会影响量子态, 但我们总是可以用一组差错算子基来表示它们. 在文献 [10] 中, 引入了一类特别有用的么正差错基, 称为优质差错基. 优质差错基可以说是量子纠错码理论的基石 [11].

在本文中, 我们提出一种研究差错基和量子码的新方法. 我们利用一种代数方法来研究优质差错基, 即群代数. 他给出了关于优质差错基和量子纠错码的代数表示. 这种群代数表示的优点在于使用他能够精确的陈述出关于量子纠错码的各种性质. 首先, 我们将回忆一下优质差错基的性质. 然后给出与阿贝尔差错基相关联的群代数及其特征的定义. 最后, 作为应用, 我们从群代数的重量枚举子得到一系列关于最一般量子纠错码的线性规划限. 除了包含现有的线性规划限 [12−14] 之外, 这些限还给出了更强的结果.

2 预备知识

令 $\mathscr{H}=\mathbb{C}^n$ 是一个 n 维希尔波特空间, 并令 G 是一个单位元为 0 的 n^2 阶加群. $\mathscr{H}$ 的一组优质差错基是 $\mathscr{H}$ 上的一个么正算子集 $\varepsilon=\{E_g|g\in G\}$, 满足

1) E_0 是恒等算子;

2) 对于所有的 $g\in G$, $\mathrm{tr}E_g=n\delta_{g,0}$;

3) 对于所有的 $g,h\in G$, $E_gE_h=\omega_{gh}E_{g+h}$, 其中 ω_{gh} 是模为 1 的复数. 我们称

G 为差错基 ε 的索引群.

引理 1 如果索引群 G 是阿贝尔的, 那么对于任意非零 $h\in G$ 有

$$\sum_{g\in G}\omega_{gh}\bar{\omega}_{hg}=0.$$

证明 由优质差错基的性质 3), 我们有

$$\begin{aligned}E_aE_bE_h&=(\omega_{bh}\bar{\omega}_{hb})E_aE_hE_b\\&=(\omega_{ah}\bar{\omega}_{ha})(\omega_{bh}\bar{\omega}_{hb})E_hE_aE_b\end{aligned}$$

和

$$\begin{aligned}E_aE_bE_h&=\omega_{ab}E_{a+b}E_h\\&=\omega_{ab}(\omega_{(a+b)h}\bar{\omega}_{h(a+b)})E_hE_{a+b}\\&=(\omega_{(a+b)h}\bar{\omega}_{h(a+b)})E_hE_aE_b,\end{aligned}$$

这意味着

$$(\omega_{ah}\bar{\omega}_{ha})(\omega_{bh}\bar{\omega}_{hb})=\omega_{(a+b)h}\bar{\omega}_{h(a+b)}.\tag{1}$$

现在令 $G_h=\{\omega_{gh}\bar{\omega}_{hg}|g\in G\}$. 那么由 (1) 式可知 G_h 是循环群的子群, 这是因为所有 ω_{gh} 生成一个循环

* 国家自然科学基金 (批准号: 61201138, 60902030)、国家重点基础研究发展计划 (973) 项目 (批准号: 2010CB328300) 和 111 工程 (批准号: B08038) 资助的课题.

† 通讯作者. E-mail: lizhuo@xidian.edu.cn

群 [15]. 因此, 对于任意非零 $h \in G$, G_h 本身是一个非平凡的循环群. 证毕.

在下面的叙述中, 如无特殊声明, 我们将总是假设优质差错基 ε 的索引群 G 是阿贝尔的. 这个假设是合理的, 因为对于任意维数 n, 这样的优质差错基都是存在的 [10].

3 群代数

我们将用关于 $z_1, \cdots, z_l$ 的形式多项式来描述 l 长的差错算子张量积. 一般来说, $E_g = E_{g_1} \otimes \cdots \otimes E_{g_l}$ 将表示为 $z_1^{g_1} z_2^{g_2} \cdots z_l^{g_l}$, 简记为 z^g. 如果我们规定 $z_i^{g_i} z_i^{h_i} = z_i^{g_i+h_i}$, 那么全部 z^g 就构成一个乘群, 记为 Z. 因此 G^l 和 Z 是同构的群, G^l 中的加法

$$\begin{aligned} g+h &= (g_1, \cdots, g_l) + (h_1, \cdots, h_l) \\ &= (g_1+h_1, \cdots, g_l+h_l), \end{aligned}$$

对应于 Z 中的乘法

$$z^g z^h = z_1^{g_1} \cdots z_l^{g_l} \cdot z_1^{h_1} \cdots z_l^{h_l} = z_1^{g_1+h_1} \cdots z_l^{g_l+h_l} = z^{g+h}.$$

定义 2 复数域 $\mathbb{C}$ 上 Z 的群代数 $\mathbb{C}Z$ 包含所有的形式和

$$\sum_{g \in G^l} a_g z^g, \quad a_g \in \mathbb{C}, \quad z^g \in Z.$$

$\mathbb{C}Z$ 元素间的加法和乘法定义为

$$\begin{aligned} &\sum_{g \in G^l} a_g z^g + \sum_{g \in G^l} b_g z^g = \sum_{g \in G^l} (a_g + b_g) z^g, \\ &r \sum_{g \in G^l} a_g z^g = \sum_{g \in G^l} r a_g z^g, \quad r \in \mathbb{C}, \\ &\sum_{g \in G^l} a_g z^g \cdot \sum_{h \in G^l} b_h z^h = \sum_{g,h \in G^l} a_g b_h z^{g+h}. \end{aligned}$$

对于每一个 $h \in G^l$, 我们关联一个从 Z 到复数域的映射 χ_h, 满足

$$\chi_h(z^g) = \mathrm{tr} E_h^\dagger E_g^\dagger E_h E_g / n^l,$$

χ_h 叫做 Z 的特征. χ_h 的作用可以线性扩展到 $\mathbb{C}Z$上:

$$\begin{aligned} \chi_h\Big(\sum_{g \in G^l} a_g z^g\Big) &= \sum_{g \in G^l} a_g \chi_h(z^g) \\ &= \sum_{g \in G^l} a_g \mathrm{tr} E_h^\dagger E_g^\dagger E_h E_g / n^l. \end{aligned}$$

另外, 我们注意到有如下的关系成立:

$$\chi_h(z^g) = \prod_{i=1}^{l} \omega_{h_i g_i} \bar{\omega}_{g_i h_i}. \tag{2}$$

令

$$C = \sum_{g \in G^l} c_g z^g$$

是群代数 $\mathbb{C}Z$ 的任意元素, 满足

$$M = \sum_{g \in G^l} c_g \neq 0.$$

定义 3 C 的变换定义为如下的 $\mathbb{C}Z$ 的元素 C':

$$C' = \frac{1}{M} \sum_{h \in G^l} \chi_h(C) z^h,$$

其中特征 χ 的定义如上.

假设

$$C' = \sum_{h \in G^l} c'_h z^h,$$

则有

$$\begin{aligned} c'_h &= \frac{1}{M} \chi_h(C) \\ &= \frac{1}{M} \sum_{g \in G^l} c_g \mathrm{tr} E_h^\dagger E_g^\dagger E_h E_g / n^l, \quad h \in G^l. \end{aligned} \tag{3}$$

现在, 让我们来描述群代数 $\mathbb{C}Z$ 的几类重量枚举子. 下面, 我们将用 $\alpha_0 = 0, \alpha_1, \cdots, \alpha_{n^2-1}$ 来表示 G 的元素.

首先考虑的重量枚举子通过引入足够多的变量可以完全指定群代数. 一般地, 我们用变量 z_{ij} 来表示向量 g 的第 i 个位置上是 G 的第 j 个元素 α_j. 向量 $g = (\alpha_{a_1}, \alpha_{a_2}, \cdots, \alpha_{a_l})$ 由如下的多项式来描述:

$$f(g) = z_{1a_1} z_{2a_2} \cdots z_{la_l}.$$

因此 $f(g)$ 可以唯一地确定 g. 这总共需要使用 ln^2 个变量 $z_{ij}, 1 \leqslant i \leqslant l, 0 \leqslant j \leqslant n^2-1$.

现在我们可以定义 C 的确切枚举子为如下的形式:

$$\mathfrak{E}_C = \sum_{g \in G^l} c_g f(g).$$

则变换 C' 的确切枚举子为

$$\mathfrak{E}_{C'} = \sum_{h \in G^l} c'_h f(h).$$

定理 4

$$\begin{aligned} &\mathfrak{E}_{C'}(z_{10}, \cdots, z_{ir}, \cdots, z_{l(n^2-1)}) \\ =&\frac{1}{M} \mathfrak{E}_C\Bigg(\sum_{s=0}^{n^2-1} \omega_{\alpha_s \alpha_0} \bar{\omega}_{\alpha_0 \alpha_s} z_{1s}, \cdots, \\ &\sum_{s=0}^{n^2-1} \omega_{\alpha_s \alpha_r} \bar{\omega}_{\alpha_r \alpha_s} z_{is}, \cdots, \sum_{s=0}^{n^2-1} \omega_{\alpha_s \alpha_{n^2-1}} \bar{\omega}_{\alpha_{n^2-1} \alpha_s} z_{ls}\Bigg). \end{aligned}$$

证明 由 (2) 式和 (3) 式可知, 上式的左边等于

$$\begin{aligned}&\sum_{h\in G^l} c'_h f(h)\\
=&\frac{1}{M}\sum_{g\in G^l} c_g \sum_{h\in G^l}\chi_h(z^g) f(h)\\
=&\frac{1}{M}\sum_{g\in G^l} c_g \sum_{s_1=0}^{n^2-1}\sum_{s_2=0}^{n^2-1}\cdots\sum_{s_l=0}^{n^2-1}\prod_{i=1}^{l}\omega_{\alpha_{s_i}g_i}\bar{\omega}_{g_i\alpha_{s_i}} z_{is_i}\\
=&\frac{1}{M}\sum_{g\in G^l} c_g \prod_{i=1}^{l}\sum_{s=0}^{n^2-1}\omega_{\alpha_s g_i}\bar{\omega}_{g_i\alpha_s} z_{is}\end{aligned}$$

等于右边. 证毕.

下面考虑的枚举子将按照每一个群元素 α_i 在 g 中出现的次数来分类 G^l 中的向量 g.

定义 5 向量 $g=(g_1,\cdots,g_l)$ 的成分, 表示为 $\mathrm{comp}(g)$, 定义为 $(s_0,s_1,\cdots,s_{n^2-1})$, 其中 $s_i=s_i(g)$ 是等于 α_i 的分量 g_j 的个数. 显然

$$\sum_{i=0}^{n^2-1} s_i = l.$$

我们把集合 $\{A(t)\}$ 叫做 C 的完全重量分布, 其中 $A(t)$ 是满足 $\mathrm{comp}(g)=t=(t_0,\cdots,t_{n^2-1})$ 的 c_g 的和. 这样我们就可以定义 C 的完全重量枚举子为

$$\begin{aligned}\mathscr{W}_C(z_0,\cdots,z_{n^2-1}) &= \sum_t A(t) z_0^{t_0}\cdots z_{n^2-1}^{t_{n^2-1}}\\
&= \sum_{g\in G^l} c_g z_0^{s_0}\cdots z_{n^2-1}^{s_{n^2-1}}.\end{aligned}$$

同时, C' 的完全重量分布为 $\{A'(t)\}$, $A'(t)$ 是满足 $\mathrm{comp}(h)=t=(t_0,\cdots,t_{n^2-1})$ 的 c'_h 的和, 并且 C' 的完全重量枚举子为

$$\mathscr{W}_{C'}(z_0,\cdots,z_{n^2-1}) = \sum_t A'(t) z_0^{t_0}\cdots z_{n^2-1}^{t_{n^2-1}}.$$

定理 6

$$\begin{aligned}&\mathscr{W}_{C'}(z_0,\cdots,z_r,\cdots,z_{n^2-1})\\
=&\frac{1}{M}\mathscr{W}_C\Bigg(\sum_{s=0}^{n^2-1}\omega_{\alpha_s\alpha_0}\bar{\omega}_{\alpha_0\alpha_s} z_s,\cdots,\\
&\sum_{s=0}^{n^2-1}\omega_{\alpha_s\alpha_r}\bar{\omega}_{\alpha_r\alpha_s} z_s,\cdots,\sum_{s=0}^{n^2-1}\omega_{\alpha_s\alpha_{n^2-1}}\bar{\omega}_{\alpha_{n^2-1}\alpha_s} z_s\Bigg).\end{aligned}$$

证明 在定理 4 中令 $z_{ij}=z_j, 1\leqslant i\leqslant l, 0\leqslant j\leqslant n^2-1$ 即得.

通过令完全重量枚举子中的某些变量相等, 我们可以得到李重量枚举子和汉明重量枚举子. 他们给出越来越少关于群代数的信息, 但同时也变得越来越容易处理.

定义 7 假设 $n^2=2\delta+1$ 是奇数, 并令 G 的元素为 $\alpha_0=0,\alpha_1,\cdots,\alpha_\delta,\alpha_{\delta+1},\cdots,\alpha_{n^2-1}$, 使得 $\alpha_{n^2-i}=-\alpha_i, 1\leqslant i\leqslant\delta$. 则向量 $g\in G^l$ 的李成分, 表示为 $\mathrm{Lee}(g)$, 定义为 $(l_0,l_1,\cdots,l_\delta)$, 其中 $l_0=s_0(g)$, $l_i=s_i(g)+s_{n^2-i}(g), 1\leqslant i\leqslant\delta$.

我们把集合 $\{L(t)\}$ 叫做 C 的李重量分布, 其中 $L(t)$ 是满足 $\mathrm{Lee}(g)=t=(t_0,\cdots,t_\delta)$ 的 c_g 的和. 这样我们就可以定义 C 的李重量枚举子为

$$\begin{aligned}\mathscr{L}_C(z_0,\cdots,z_\delta) &= \sum_t L(t) z_0^{t_0} z_1^{t_1}\cdots z_\delta^{t_\delta}\\
&= \sum_{g\in G^l} c_g z_0^{l_0} z_1^{l_1}\cdots z_\delta^{l_\delta}.\end{aligned}$$

同时, C' 的李重量分布为 $\{L'(t)\}$, $L'(t)$ 是满足 $\mathrm{Lee}(h)=t=(t_0,\cdots,t_\delta)$ 的 c'_h 的和, 并且 C' 的李重量枚举子为

$$\mathscr{L}_{C'}(z_0,\cdots,z_\delta) = \sum_t L'(t) z_0^{t_0} z_1^{t_1}\cdots z_\delta^{t_\delta}.$$

定理 8 变换 C' 的李枚举子可以通过将 C 的李枚举子中的变量 z_i 替换为

$$z_0+\sum_{s=1}^{\delta}(\omega_{\alpha_s\alpha_i}\bar{\omega}_{\alpha_i\alpha_s}+\bar{\omega}_{\alpha_s\alpha_i}\omega_{\alpha_i\alpha_s}) z_s,$$

然后再除以 M 而得到.

证明 在定理 6 中令 $z_{n^2-i}=z_i, 1\leqslant i\leqslant\delta$ 即得.

向量 $g=(g_1,\cdots,g_l)\in G^l$ 的汉明重量定义为非零分量 g_i 的个数, 表示为 $wt(g)$.

我们把集合 $\{A_i\}$ 叫做 C 的汉明重量分布, 其中 A_i 是满足 $wt(g)=i$ 的 c_g 的和. 这样我们就可以定义 C 的汉明重量枚举子为

$$W_C(x,y)=\sum_{i=0}^{l} A_i x^{l-i} y^i = \sum_{g\in G^l} c_g x^{l-wt(g)} y^{wt(g)}.$$

同时, C' 的汉明重量分布为 $\{A'_i\}$, A'_i 是满足 $\mathrm{wt}(h)=i$ 的 c'_h 的和, 并且 C' 的汉明重量枚举子为

$$W_{C'}(x,y)=\sum_{i=0}^{l} A'_i x^{l-i} y^i.$$

定理 9

$$W_{C'}(x,y)=\frac{1}{M}W_C(x+(n^2-1)y, x-y).$$

证明 在定理 6 中令 $z_0=x$, $z_1=z_2=\cdots=z_{n^2-1}=y$, 再利用引理 1 即得.

4 量子码中的应用

上面得到的关于群代数重量枚举子的结果可

以应用于量子纠错码来建立参数限. 下面我们就来看看这方面的应用.

给定一个量子码 $((l,K,d))_n$, $\{v_i\}$ 是他的一组规范正交基, 令 $\mathscr{P}$ 是向码空间的正交投影. 则我们有

$$\mathscr{P}=\sum_{g\in G^l}\frac{\mathrm{tr}E_g^\dagger\mathscr{P}}{n^l}E_g=\sum_{i=1}^K|v_i\rangle\langle v_i|.$$

现在我们可以从群代数 $\mathbb{C}Z$ 中选出一个元素 $P=\sum_{g\in G^l}p_gz^g$, 满足

$$\begin{aligned}p_g&=\frac{n^{2l}}{K^2}\frac{\mathrm{tr}E_g\mathscr{P}^\dagger}{n^l}\frac{\mathrm{tr}E_g^\dagger\mathscr{P}}{n^l}\\&=\frac{1}{K^2}\left|\sum_{i=1}^K\langle v_i|E_g|v_i\rangle\right|^2.\end{aligned}\tag{4}$$

然后由 (3) 式可得, P 的变换为 $P'=\sum_{h\in G^l}p'_hz^h$, 其中

$$\begin{aligned}p'_h=&\frac{K}{n^l}\sum_{g\in G^l}\frac{n^{2l}}{K^2}\frac{\mathrm{tr}E_g\mathscr{P}^\dagger}{n^l}\\&\times\frac{\mathrm{tr}E_g^\dagger\mathscr{P}}{n^l}\mathrm{tr}E_h^\dagger E_g^\dagger E_hE_g/n^l\\=&\frac{1}{K}\mathrm{tr}E_h^\dagger\mathscr{P}^\dagger E_h\mathscr{P}\\=&\frac{1}{K}\sum_{i=1}^K\sum_{j=1}^K|\langle v_i|E_h|v_j\rangle|^2.\end{aligned}\tag{5}$$

定理 10-1 如果参数为 $((l,K,d))_n$ 的量子码存在, 那么下面的线性方程组有解:

$$\begin{aligned}&p_0=1,\\&\frac{K}{n^l}\sum_{g\in G^l}\chi_h(z^g)p_g=p_h,\quad 0\leqslant\mathrm{wt}(h)<d,\\&\frac{K}{n^l}\sum_{g\in G^l}\chi_h(z^g)p_g\geqslant p_h,\quad d\leqslant\mathrm{wt}(h)\leqslant l,\\&p_g\geqslant 0,\quad g\in G^l.\end{aligned}$$

证明 由 (4) 式, (5) 式和量子码的性质立即可得.

令 $\{A(t)\}$ 和 $\{A'(t)\}$ 分别为 P 和 P' 的完全重量分布, 其中 $t=(t_0,\cdots,t_{n^2-1})$. 则由定理 6

$$\begin{aligned}&\sum_t A'(t)\prod_{i=0}^{n^2-1}z_i^{t_i}\\&=\frac{K}{n^l}\sum_r A(r)\prod_{j=0}^{n^2-1}\left(\sum_{s=0}^{n^2-1}\omega_{\alpha_s\alpha_j}\bar{\omega}_{\alpha_j\alpha_s}z_s\right)^{r_j}.\end{aligned}\tag{6}$$

如果我们表示

$$\prod_{j=0}^{n^2-1}\left(\sum_{s=0}^{n^2-1}\omega_{\alpha_s\alpha_j}\bar{\omega}_{\alpha_j\alpha_s}z_s\right)^{r_j}=\sum_t a_{\mathrm{tr}}\prod_{i=0}^{n^2-1}z_i^{t_i},$$

则由 (6) 式

$$A'(t)=\frac{K}{n^l}\sum_r a_{tr}A(r).$$

定理 10-2 如果参数为 $((l,K,d))_n$ 的量子码存在, 那么下面的线性方程组有解:

$$\begin{aligned}&A(l,0,\cdots,0)=1,\\&\frac{K}{n^l}\sum_r a_{tr}A(r)=A(t),\quad 0\leqslant l-t_0<d,\\&\frac{K}{n^l}\sum_r a_{tr}A(r)\geqslant A(t),\quad d\leqslant l-t_0\leqslant l,\\&A(t)\geqslant 0.\end{aligned}$$

证明方法基本和定理 10-1 相同, 只是这里需要用到完全重量分布的定义.

在 $n^2=2\delta+1$ 是奇数的情况下, 令 $\{L(t)\}$ 和 $\{L'(t)\}$ 分别为 P 和 P' 的李重量分布, 其中 $t=(t_0,\cdots,t_\delta)$. 则由定理 8

$$\begin{aligned}\sum_t L'(t)\prod_{i=0}^{\delta}z_i^{t_i}=&\frac{K}{n^l}\sum_r L(r)\prod_{j=0}^{\delta}\Bigg(z_0+\sum_{s=1}^{\delta}(\omega_{\alpha_s\alpha_j}\bar{\omega}_{\alpha_j\alpha_s}\\&+\bar{\omega}_{\alpha_s\alpha_j}\omega_{\alpha_j\alpha_s})z_s\Bigg)^{r_j}.\end{aligned}\tag{7}$$

如果我们表示

$$\begin{aligned}&\prod_{j=0}^{\delta}\left(z_0+\sum_{s=1}^{\delta}(\omega_{\alpha_s\alpha_j}\bar{\omega}_{\alpha_j\alpha_s}+\bar{\omega}_{\alpha_s\alpha_j}\omega_{\alpha_j\alpha_s})z_s\right)^{r_j}\\&=\sum_t b_{tr}\prod_{i=0}^{\delta}z_i^{t_i},\end{aligned}$$

则由 (7) 式

$$L'(t)=\frac{K}{n^l}\sum_r b_{tr}L(r).$$

定理 10-3 如果参数为 $((l,K,d))_n$ 的量子码存在, 那么下面的线性方程组有解:

$$\begin{aligned}&L(l,0,\cdots,0)=1,\\&\frac{K}{n^l}\sum_r b_{tr}L(r)=L(t),\quad 0\leqslant l-t_0<d,\\&\frac{K}{n^l}\sum_r b_{tr}L(r)\geqslant L(t),\quad d\leqslant 1-t_0\leqslant l,\\&L(t)\geqslant 0.\end{aligned}$$

证明方法基本和定理 10-1 相同, 只是这里需要用到李重量分布的定义.

令 $\{A_i\}$ 和 $\{A'_i\}$ 分别为 P 和 P' 的汉明重量分布. 则由定理 9

$$\sum_{i=0}^{l}A'_ix^{l-i}y^i$$

$$=\frac{K}{n^l}\sum_{r=0}^{l}A_r(x+(n^2-1)y)^{l-r}(x-y)^r. \qquad (8)$$

如果我们表示

$$(x+(n^2-1)y)^{l-r}(x-y)^r=\sum_{i=0}^{l}h_{ir}x^{l-i}y^i,$$

则由 (8) 式

$$A_i'=\frac{K}{n^l}\sum_{r=0}^{l}h_{ir}A_r.$$

定理 10-4 如果参数为 $((l,K,d))_n$ 的量子码存在, 那么下面的线性方程组有解:

$$\begin{aligned}&A_0=1,\\&\frac{K}{n^l}\sum_{r=0}^{l}h_{ir}A_r=A_i,\quad 0\leqslant i<d,\\&\frac{K}{n^l}\sum_{r=0}^{l}h_{ir}A_r\geqslant A_i,\quad d\leqslant i\leqslant l,\\&A_i\geqslant 0.\end{aligned}$$

证明方法基本和定理 10-1 相同, 只是这里需要用到汉明重量分布的定义.

实际上,Calderbank 等人在文献 [12] 中首次证明了定理 10-4 对于二元稳定子码成立, 后来 Rains 在文献 [13] 中对其进行了推广. 在文献 [14] 中, Ketkar 等人又证明了定理 10-4 同样适用于非二元稳定子码. 在这里, 我们证明了定理 10-4 其实是普适的, 即对于任何量子码他都是成立的.

最后我们以一个例子来结束这一节. 在定理 10-4 中, 如果我们取 $(l,K,d,n)=(5,2,3,2)$, 则定理 10-4 告诉我们: 如果参数为 $((5,2,3))_2$ 的量子码存在, 那么下面的线性方程组有解:

$$\begin{aligned}&\frac{A_0+A_1+A_2+A_3+A_4+A_5}{16}=A_0=1,\\&\frac{15A_0+11A_1+7A_2+3A_3-A_4-5A_5}{16}=A_1,\\&\frac{45A_0+21A_1+5A_2-3A_3-3A_4+5A_5}{8}=A_2,\\&\frac{135A_0+27A_1-9A_2-5A_3+7A_4-5A_5}{8}\geqslant A_3,\\&\frac{405A_0-27A_1-27A_2+21A_3-11A_4+5A_5}{16}\geqslant A_4,\\&\frac{243A_0-81A_1+27A_2-9A_3+3A_4-A_5}{16}\geqslant A_5,\\&A_i\geqslant 0.\end{aligned}$$

利用线性规划方法, 我们很容易发现以上线性方程组有唯一解 $A_{0\sim 5}=(1,0,0,0,15,0)$. 因此, 如果 $((5,2,3))_2$ 量子码存在的话, 他的重量分布一定是唯一的. 不存在其他类型的 $((5,2,3))_2$ 量子码.

5 结 论

在上面的四个定理中, 我们看到, 系数 $\chi_h(z^g)$, a_{tr}, b_{tr} 和 h_{ir} 仅仅依赖于差错基的选择. 因此, 只要给定一组差错基, 我们就可以利用线性规划技术通过这四个定理来获得量子码的码限. 更进一步, 我们还注意到这些定理在一定意义上是单调的. 即从定理 10-4 到定理 10-1, 他们给出了越来越复杂的线性规划问题, 但同时也变得越来越强; 这是由于变量的个数从 l 增加到 n^{2l}, 但同时线性约束的个数也从 l 增加到 n^{2l}.

综上所述, 我们已经在差错基和群代数之间搭起了一座桥梁, 他提供了一条研究量子码的新途径. 例如, 在本文中, 我们就利用他建立了最一般量子码的码限. 我们相信, 群代数方法将成为研究量子纠错码问题的强有力的工具.

[1] Li Z, Xing L J 2008 *Acta Phys. Sin.* **57** 28 (in Chinese) [李卓, 邢莉娟 2008 物理学报 **57** 28]

[2] Li Z, Xing L J 2007 *Acta Phys. Sin.* **56** 5602 (in Chinese) [李卓, 邢莉娟 2007 物理学报 **56** 5602]

[3] Xing L J, Li Z, Bai B M, Wang X M 2008 *Acta Phys. Sin.* **57** 4695 (in Chinese) [邢莉娟, 李卓, 白宝明, 王新梅 2008 物理学报 **57** 4695]

[4] Li Z, Xing L J, Wang X M 2009 *IEEE Trans. Inform. Theory* **55** 3821

[5] Li Z, Xing L J, Wang X M 2008 *Phys. Rev.* **A77** 012308

[6] Li Z, Xing L J 2009 *Phys. Rev.* **A79** 032301

[7] Shor P W 1995 *Phys. Rev.* **A52** 2493

[8] Calderbank A R, Rains E M, Shor P W, Sloane N J A 1997 *Phys. Rev. Lett.* **78** 405

[9] Steane A M 1996 *Phys. Rev. Lett.* **77** 793

[10] Knill E 1996 *Los Alamos Nat. Lab. Rep.* LAUR-96-2717

[11] Ashikhmin A, Knill E 2001 *IEEE Trans. Inform. Theory* **47** 3065

[12] Calderbank A R, Rains E M, Shor P W, Sloane N J A 1998 *IEEE Trans. Inform. Theory* **44** 1369

[13] Rains E M 1999 *IEEE Trans. Inform. Theory* **45** 2361

[14] Ketkar A, Klappenecker A, Kumar S, Sarvepalli P K 2006 *IEEE Trans. Inform. Theory* **52** 4892

[15] Klappenecker A, Rotteler M 2002 *IEEE Trans. Inform. Theory* **48** 2392

Error bases, group algebra and quantum codes*

Li Zhuo† Xing Li-Juan

(*State Key Lab of Integrated Services Networks, Xidian University, Xi'an* 710071, *China*)

(Received 8 August 2012; revised manuscript received 27 February 2013)

Abstract

We find a new approach to study nice error bases and quantum error-correcting codes, namely the group algebra which gives us an algebraic notation for nice error bases and quantum codes. From this algebraic notation we establish a series of linear programming bounds on the most general quantum error-correcting codes.

Keywords: group algebra, error bases, quantum error-correcting codes, quantum information

PACS: 03.67.Pp, 03.67.Hk, 03.67.Lx **DOI:** 10.7498/aps.62.130306

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61201138, 60902030), the National Basic Research Program of China (Grant No. 2010CB328300), and the 111 Project (Grant No. B08038).

† Corresponding author. E-mail: lizhuo@xidian.edu.cn