加强的量子汉明限*

邢莉娟 李 卓† 张武军

(西安电子科技大学,综合业务网国家重点实验室,西安 710071)

(2010 年 5 月 14 日收到;2010 年 9 月 29 日收到修改稿)

通过研究具有相同重量的算子集合的性质,找到了任意维数纯量子稳定子码参数的新的解析上限. 与目前所知最优的解析上限——著名的量子汉明限相比,本文提出的码限强于量子汉明限.

关键词: 量子汉明限, 量子稳定子码, 量子纠错码, 量子信息

PACS: 03.67.Pp, 03.67.Hk, 03.67.Lx

1. 引 言

量子计算技术因其强大的计算能力,近十几年来,引起了人们极大的兴趣. 当某个装置处理和计算的是量子信息,运行的是量子算法,且遵循量子力学基本规律时,它就是量子计算机. 量子计算机突出的优点有两个,首先是它能够实现量子并行计算,加快计算的速度,提高信息存储能力;其次,它能够模拟量子通信系统,这是经典计算机无法胜任的. 无论量子并行计算还是模拟量子通信系统,本质上都是利用了量子相干性. 然而,在实际环境中,量子计算机的量子比特不是孤立的,它时刻与外部环境发生相互作用,破坏量子比特相干性,导致量子消相干. 因此,要使量子计算机成为现实,一个核心问题就是克服由消相干带来的量子噪声. 此外,源于量子门的不精确性产生的信道噪声也是量子计算机必须克服的另一大障碍.

十几年前建立起来的量子纠错码理论一直以来都被认为是对抗量子消相干效应的主要方法,从而是实现实际量子通信和量子计算必不可少的关键技术[1—10]. 目前来说,量子纠错码领域最大的进展是量子码稳定子框架的建立[11].

在量子纠错码理论中,一个最基本的问题是找出具有给定码长和最小距离的最大的码. 更具体来说就是,令 $B(n,d,m)$ = 码长为 n 最小距离为 d 的 m 元纯量子稳定子码空间的最大维数. 那么确定出 $B(n,d,m)$ 或者找出它的紧的上限就是量子纠错码理论中一个非常重要的问题. 到目前为止,人们已经找到了许多 $B(n,d,m)$ 的上限,比如说量子 Singleton 限和量子汉明限[10,11]. 对于小的码长 n,量子汉明限可以说是最优的,因为达到它的码已经被找到了. 量子汉明限出现之后,人们一直在试图寻找更强的结果. 但是到目前为止,唯一强于量子汉明限的只有量子线性规划限[10],这是利用线性规划技术得到的一类码限. 虽然量子线性规划限更强,但它不是解析的. 这也就是说,一般来说我们必须借助计算机搜索来得到它. 因此,寻找强于量子汉明限的解析上限的问题到现在仍然没有解决. 在本文中,我们将给出第一个这样的解析上限(定理 6).

令 $\mathscr{E}=\{I,E_1,\cdots,E_{m^2-1}\}$ 表示 m 元量子系统的一组优质差错基[12]. 我们用来估计 $B(n,d,m)$ 的方法是研究集合 $\mathscr{E}_n=\mathscr{E}^{\otimes n}$ 中具有相同重量的算子的性质. 为此,我们定义

$A(n,d,w,m)$ = $\mathscr{E}_n$ 中重量为 w 距离至少为 d 的算子的最大个数.

$\mathscr{E}_n$ 中某算子的重量定义为它的非恒等张量因子的个数. $\mathscr{E}_n$ 中两算子的距离定义为它们之间具有不同张量因子的位置的个数.

2. $A(n,d,w,m)$ 的估计

这一节我们来考察 $A(n,d,w,m)$, 即 $\mathscr{E}_n$ 中重量

* 国家自然科学基金(批准号:60902030),陕西省自然科学基金(批准号:2010JQ8025),国家重点基础研究发展计划(973)项目(批准号:2010CB328300),111 工程(批准号:B08038)资助的课题.

† 通讯联系人. E-mail: lizhuo@xidian.edu.cn

为 w 距离至少为 d 的算子的最大个数. 它本身就是一个重要的函数,并且在定理 6 中给出了关于 $B(n,d,m)$ 的新上限. 首先,我们给出关于 $A(n,d,w,m)$ 的一些估计.

定理 1

(a) $A(n,d,w,m) = 1, \quad 2w < d.$

(b) $A(n,2\delta,\delta,m) = \left[\frac{n}{\delta}\right].$

(c) $A(n,2\delta+1,\delta+1,m) \leqslant \left[\frac{(m^2-1)n}{\delta+1}\right].$

证明 (a)是显然的,因为如果 $2w < d$,那么任意两个重量为 w 的算子之间的距离都小于 d. 因此,要使距离至少为 d,算子的个数至多为 1. (b)成立是因为两个重量为 δ 的算子之间的距离至多为 2δ,因此要使距离至少为 2δ,算子间必须具有不重叠的非恒等张量因子. (c)成立是因为两个重量为 $\delta+1$ 的算子之间的距离至多为 $2\delta+2$,因此要使距离至少为 $2\delta+1$,则对于算子的每一个位置,算子间该位置上的非恒等张量因子必须都不同. 共有 n 个位置,共有 m^2-1 个不同的非恒等张量因子,每个算子的重量都为 $\delta+1$. 证毕.

下面的定理是比定理 1 更一般的结果.

定理 2

$$A(n,d,w,m) \leqslant \left[\frac{(m^2-1)dn}{m^2w^2-2(m^2-1)wn+(m^2-1)dn}\right], \quad (1)$$

只要分母是正的.

证明 令 $\Psi \subseteq \mathscr{E}_n$ 是一个达到 $A(n,d,w,m)$ 要求的相同重量算子集,满足 $|\Psi| = M = A(n,d,w,m)$. 再令 $X = (x_{ij})$ 是一个以 Ψ 中算子为行构成的 $M \times n$ 矩阵,因此每行的重量都为 w. 定义差错基 $\mathscr{E}$ 中两元素 E 和 F 上的一种运算“ $*$ ”如下:

$$E*F = \begin{cases} 0, & E = I \text{ 或 } F = I, \\ 1, & E \neq I, F \neq I, E \neq F, \\ 2, & E \neq I, F \neq I, E = F. \end{cases}$$

用两种方法计算和式

$$\sum_{i=1}^{M}\sum_{\substack{j=1\\ j\neq i}}^{M}\sum_{v=1}^{n} x_{iv} * x_{jv}.$$

由于任意两行之间的距离至少为 d,我们有 $\sum_{v=1}^{n} x_{iv} * x_{jv}$ 至多为 $2w-d$. 因此这个和式 $\leqslant (2w-d)M(M-1)$.

另一方面,这个和式也可以写为

$$\sum_{v=1}^{n}\sum_{i=1}^{M}\sum_{\substack{j=1\\ j\neq i}}^{M} x_{iv} * x_{jv}.$$

如果用 k_{vu} 来表示 X 的第 v 列中 E_u 的个数,那么这一列对于和式的贡献为

$$\begin{aligned} &\sum_{u=1}^{m^2-1} k_{vu}\Big(2(k_{vu}-1) + \sum_{\substack{s=1\\ s\neq u}}^{m^2-1} k_{vs}\Big) \\ &= \sum_{u=1}^{m^2-1} k_{vu}\Big(k_{vu} - 2 + \sum_{s=1}^{m^2-1} k_{vs}\Big) \\ &= \Big(\sum_{s=1}^{m^2-1} k_{vs}\Big)^2 + \sum_{u=1}^{m^2-1} k_{vu}(k_{vu}-2). \end{aligned}$$

因此我们有

$$\begin{aligned} &\sum_{v=1}^{n}\Big(\Big(\sum_{s=1}^{m^2-1} k_{vs}\Big)^2 + \sum_{u=1}^{m^2-1} k_{vu}(k_{vu}-2)\Big) \\ &\leqslant (2w-d)M(M-1). \end{aligned} \quad (2)$$

但是

$$\sum_{v=1}^{n}\sum_{u=1}^{m^2-1} k_{vu} = wM$$

(X 的总重量),并且当所有的 $k_{vu} = wM/(m^2-1)n$ 时 $\sum_{v=1}^{n}\big(\sum_{s=1}^{m^2-1} k_{vs}\big)^2 + \sum_{v=1}^{n}\sum_{u=1}^{m^2-1} k_{vu}^2$ 最小化,这时

$$\begin{aligned} &\sum_{v=1}^{n}\Big(\sum_{s=1}^{m^2-1} k_{vs}\Big)^2 + \sum_{v=1}^{n}\sum_{u=1}^{m^2-1} k_{vu}^2 \\ &= \frac{w^2M^2}{n} + \frac{w^2M^2}{(m^2-1)n}. \end{aligned}$$

因此,由(2)式可得

$$\begin{aligned} &\frac{w^2M^2}{n} + \frac{w^2M^2}{(m^2-1)n} - 2wM \\ &\leqslant (2w-d)M(M-1). \end{aligned}$$

解出 M 就得到(1)式. 证毕.

既然 k_{vu} 必须为整数,那么上面的结果可以被略微加强.

定理 3 假设 $A(n,d,w,m) = M$,并且定义 k, t 和 r 满足

$$\begin{aligned} wM &= (m^2-1)nk + nt + r, \\ 0 &\leqslant nt + r < (m^2-1)n, \\ 0 &\leqslant r < n. \end{aligned}$$

(这是所有算子的总重量.)那么

$$\begin{aligned} &r((m^2-1)k+t+1)^2 \\ &+ (n-r)((m^2-1)k+t)^2 \\ &+ (nt+r)(k+1)^2 \\ &+ ((m^2-1)n \\ &- (nt+r))k^2 - 2((m^2-1)nk + nt + r) \\ &\leqslant (2w-d)M(M-1). \end{aligned} \quad (3)$$

证明 我们还是来估计 $\sum_{v=1}^{n}\left(\sum_{s=1}^{m^2-1}k_{vs}\right)^2+\sum_{v=1}^{n}\sum_{u=1}^{m^2-1}k_{vu}^2$ 的最小值,但这次是在

$$\sum_{v=1}^{n}\sum_{u=1}^{m^2-1}k_{vu}=wM$$

和 k_{vu} 为整数的约束下. 容易看出,当 $k_{ij}=k+1$ 对于 $1\leqslant i\leqslant n$ 和 $1\leqslant j\leqslant t$, $k_{1(t+1)}=\cdots=k_{r(t+1)}=k+1$, $k_{(r+1)(t+1)}=\cdots=k_{n(t+1)}=k$, $k_{vu}=k$ 对于 $1\leqslant v\leqslant n$ 和 $t+2\leqslant u\leqslant m^2-1$ 时达到最小. 这个最小值为

$$\begin{aligned}&r((m^2-1)k+t+1)^2\\&+(n-r)((m^2-1)k+t)^2\\&+(nt+r)(k+1)^2+((m^2-1)n\\&-(nt+r))k^2,\end{aligned}$$

再由(2)式可知(3)式成立. 证毕.

例子 由定理2可知

$$A(9,8,5,2)\leqslant\left[\frac{216}{100-270+216}\right]=4.$$

但是如果 $A(9,8,5,2)=4$ 的话,那么利用定理3我们有

$$5\cdot 4=27\cdot 0+9\cdot 2+2,$$

因此 $k=0,t=2,r=2$ 并与(3)式矛盾. 因此 $A(9,8,5,2)\leqslant 3$. 实际上算子集 $\{E_1E_1E_1E_1E_1IIII, E_2E_2IIIE_1E_1E_1I, IIE_2E_2IE_2E_2IE_1\}$ 告诉我们 $A(9,8,5,2)=3$.

下面我们给出一个递归关系. 当定理2不适用的时候它是非常有用的.

定理4

$$A(n,d,w,m)\leqslant\left[\frac{(m^2-1)n}{w}A(n-1,d,w-1,m)\right]. \quad (4)$$

证明 考虑这样的算子,它们在第 i 个位置上是 E_j. 如果这个位置被去掉的话,我们得到一个长度为 $n-1$,重量为 $w-1$,距离 $\geqslant d$ 的算子集. 因此,这样的算子的个数 $\leqslant A(n-1,d,w-1,m)$. 因此,原先的算子集的总重量满足

$$\begin{aligned}&wA(n,d,w,m)\\&\leqslant(m^2-1)nA(n-1,d,w-1,m).\end{aligned}$$

证毕.

在实际计算 $A(n,d,w,m)$ 时,我们经常是反复使用定理4,直到一个已知的值. 如下面的例子所示.

例子 由(4)式

$$\begin{aligned}&A(20,7,7,2)\\&\leqslant\left[\frac{3\cdot 20}{7}A(19,7,6,2)\right]\\&\leqslant\left[\frac{3\cdot 20}{7}\left[\frac{3\cdot 19}{6}A(18,7,5,2)\right]\right]\\&\leqslant\left[\frac{3\cdot 20}{7}\left[\frac{3\cdot 19}{6}\left[\frac{3\cdot 18}{5}A(17,7,4,2)\right]\right]\right], \quad (5)\end{aligned}$$

然后利用定理1,

$$A(17,7,4,2)\leqslant\left[\frac{3\cdot 17}{4}\right]=12.$$

因此得到

$$\begin{aligned}A(20,7,7,2)&\leqslant\left[\frac{60}{7}\left[\frac{57}{6}\left[\frac{54\cdot 12}{5}\right]\right]\right]\\&=10500. \quad (6)\end{aligned}$$

3. $B(n,d,m)$ 的估计

在这一节中,我们将利用上一节得到的关于 $A(n,d,w,m)$ 的限来估计 $B(n,d,m)$. 在 d 不太大的情况下,下面的结果是非常有用的[11].

定理5 (量子汉明限)

$$B(n,2\delta+1,m)\left(1+(m^2-1)\binom{n}{1}+\cdots+(m^2-1)^{\delta}\binom{n}{\delta}\right)\leqslant m^n.$$

这个定理可以通过函数 $A(n,d,w,m)$ 来加强.

定理6

$$B(n,2\delta+1,m)\left\{1+(m^2-1)\binom{n}{1}+\cdots+(m^2-1)^{\delta}\binom{n}{\delta}+\frac{(m^2-1)^{\delta+1}\binom{n}{\delta+1}-\binom{2\delta+1}{\delta}A(n,2\delta+1,2\delta+1,m)}{A(n,2\delta+1,\delta+1,m)}\right\}\leqslant m^n. \quad (7)$$

证明 令 $\mathscr{C}=((n,K,d))_m$ 是一个纯的量子稳定子码,其中 $K=B(n,d,m), d=2\delta+1$, 并令

$\{|v_i\rangle\}_{i=1}^{K}$ 是它的一组规范正交基. 则由稳定子码的性质可知,对于任意的 $E,F \in \mathrm{E}_n$, 只要 $E^{\dagger}F$ 不属于 C 的规范子,那么 $E|v_i\rangle$ 和 $F|v_j\rangle$ 就是正交的, $1 \leqslant i,j \leqslant K$. 令 S_i 表示 E_n 中所有重量为 i 的算子构成的集合. 则

$$|S_i| = (m^2-1)^i \binom{n}{i}.$$

那么对于 $E \in S_0 \cup S_1 \cup \cdots \cup S_\delta$ 和 $1 \leqslant i \leqslant K$, 所有的状态 $E|v_i\rangle$ 都是相互正交的. 这就证得了量子汉明限(定理 5). 为了得到(7)式,下面我们来考察 $S_{\delta+1}$.

在 C 的规范子中,所有重量为 $d = 2\delta+1$ 的算子构成了一个距离 $\geqslant 2\delta+1$ 的集合. 因此,规范子中重量为 d 的算子个数 $\leqslant A(n,2\delta+1,2\delta+1,m)$.

对应于规范子中每一个重量为 d 的算子 Q, 一共有 $\binom{d}{\delta}$ 个重量为 $\delta+1$ 的算子与 Q 的距离为 δ. 这些算子是互不相同的,构成一个集合表示为 $W_{\delta+1}$. 因此我们有

$$|S_{\delta+1} - W_{\delta+1}| \geqslant (m^2-1)^{\delta+1}\binom{n}{\delta+1} - \binom{d}{\delta}A(n,2\delta+1,2\delta+1,m).$$

对于任意 $E \in S_0 \cup S_1 \cup \cdots \cup S_\delta$ 和 $F \in S_{\delta+1} - W_{\delta+1}$, $E^{\dagger}F$ 一定不属于 C 的规范子. 另外, $S_{\delta+1} - W_{\delta+1}$ 中的一个算子 R 至多与规范子中 $A(n,2\delta+1,\delta+1,m)$ 个算子的距离为 $\delta+1$. 因此(7)式成立. 证毕.

例子

$$B(20,7,2) \leqslant \frac{2^{20}}{1+3\binom{20}{1}+3^2\binom{20}{2}+3^3\binom{20}{3}+\left\{3^4\binom{20}{4}-\binom{7}{3}A(20,7,7,2)\right\}/15}.$$

但由(6)式可知 $A(20,7,7,2) \leqslant 10500$. 因此可得 $B(20,7,2) \leqslant 2^4$. 而如果用量子汉明限的话,它给出的结果仅为 $B(20,7,2) \leqslant 2^5$. 因此,我们的结果强于量子汉明限.

4. 结 论

利用定理 6,我们计算了一些本文提出的新的上限的值,并与已知的量子汉明限进行了比较. 最初的几个结果我们列于了表 1 中. 我们发现,新限相对于汉明限的提高程度是不均匀的——有些时候提高的很少,有些时候提高的比较多. 但新的上限一定不会差于量子汉明限. 这里需要指出的是,提高的程度是与(7)式中函数 A 的值有关的. 由于目前只能得到函数 A 的估计值,因此由他计算得出的上限就更加不紧. 如果能够得到关于 A 的精确值的话,那么新的上限的提高程度就会更大. 另外,我们发现表 1 中当 n 为奇数时,新限与汉明限是相同的. 这是否具有一般性. 这些都是将来需要研究的问题.

综上所述,在本文中我们已经建立了关于纯量子稳定子码的一个新的上限. 这个限依赖于一个重要的函数 $A(n,d,w,m)$, 即 E_n 中具有相同重量 w 距离至少为 d 的算子的最大个数. 这可以认为是第一个强于著名的量子汉明限的解析上限.

表 1 汉明限与新上限的对比

n	δ	m	汉明限	新限
5	1	2	2	2
6	1	2	3.4	3.2
7	1	2	5.8	5.8
8	1	2	10.2	9.8
9	1	2	18.3	18.3

[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 and 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.* A **77** 012308

[6] Laflamme R, Miquel C, Paz J P, Zurek W 1996 *Phys. Rev. Lett.* **77** 198

[7] Steane A M 1996 *Phys. Rev. Lett.* **77** 793
[8] Shor P W 1995 *Phys. Rev.* A **52** 2493
[9] Calderbank A R, Rains E M, Shor P W, Sloane N J A 1997 *Phys. Rev. Lett.* **78** 405
[10] Calderbank A R, Rains E M, Shor P W, Sloane N J A 1998 *IEEE Trans. Inform. Theory* **44** 1369
[11] Ketkar A, Klappenecker A, Kumar S, Sarvepalli P K 2006 *IEEE Trans. Inform. Theory* **52** 4892
[12] Ashikhmin A, Knill E 2001 *IEEE Trans. Inform. Theory* **47** 3065

Strengthened quantum Hamming bound*

Xing Li-Juan Li Zhuo† Zhang Wu-Jun
(*State Key Lab of Integrated Services Networks, Xidian University, Xi'an* 710071, *China*)
(Received 14 May 2010; revised manuscript received 29 September 2010)

Abstract

By studying sets of operators with constant weight we present for the first time an analytical upper bound on the pure quantum stabilizer codes whose underlying quantum system can be of arbitrary dimension, which outperforms the so far well-known quantum Hamming bound, the optimal analytical upper bound for small code length.

Keywords: quantum Hamming bound, quantum stabilizer codes, quantum error-correcting codes, quantum information
PACS: 03.67.Pp, 03.67.Hk, 03.67.Lx

* Project supported by the National Natural Science Foundation of China (Grant No. 60902030), the Natural Science Foundation of Shaanxi Province, China (Grant No. 2010JQ8025), 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