第 56 卷 第 10 期 2007 年 10 月
1000-3290/2007/56(10)/5602-05
物 理 学 报
ACTA PHYSICA SINICA
Vol.56,No.10,October,2007

一类基于级联结构的量子好码

李 卓† 邢莉娟
(西安电子科技大学综合业务网国家重点实验室,西安 710071)

(2006 年 12 月 12 日收到;2007 年 2 月 2 日收到修改稿)

借助经典级联码的思想,详细阐述了通过适当选择量子码作为外码和内码,构造一般意义量子级联码的过程.在此基础上,通过选择量子 RS 码作为外码,一组特殊结构的量子码作为内码,具体构造出了一类量子级联码,证明了其是量子好码.在量子纠错码领域中,这是首次利用经典坏码构造出量子好码.

关键词:量子好码,量子级联码,量子纠错码,量子信息
PACC:0367,0365,0210

1. 引 言

量子计算[1,2]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.但是,在实际构建量子计算机或者量子通信设备的过程中,不可避免的就会遇到差错问题.存储在设备中的或在信道中传输的量子比特会因为噪声或环境的作用而发生差错,严重时就会导致计算和通信的失败.近年来发展起来的量子纠错编码技术能够比较有效的解决这一难题.它的基本思想是将 k 位量子比特嵌入到 $n(>k)$位量子比特中,以达到对量子信息的保护.迄今为止,许多种量子纠错码以及相关理论已经被发现和提出[3—9],其中以 CSS 码[6,7]和稳定子码[8,9]最为重要和成熟.

就像在经典编码理论中那样,人们总是想要构造出大码距的量子码;更一般地,人们想要得到码距正比于码长的量子好码.Ashikhmin[10]和 Chen[11]等人分别构造出了基于代数几何码的量子好码.后来,Matsumoto[12]对 Ashikhmin[10]的码进行了改进.

在经典编码理论中,码的级联[13—15]是构造经典好码的重要方法,许多著名的经典好码都是级联结构的.本文正是利用经典级联码的思想,构造出一类量子级联码,并证明它是量子好码.

2. 量子稳定子码简介

关于量子稳定子码的理论已经比较成熟和规范.在这里,将只列出一些本文会用到的内容,其中的定理将不给证明.关于稳定子码的详细介绍可以参阅文献[14].

令 $\boldsymbol{F}_q$ 表示 q 阶有限域,$q=p^m$,p 为素数.对于 $\boldsymbol{F}_q^{2n}$ 上的向量$(\boldsymbol{a}|\boldsymbol{b})$,它的辛重量(symplectic weight)定义为

$$\mathrm{swt}((\boldsymbol{a}|\boldsymbol{b}))=|\{k|(a_k,b_k)\neq(0,0)\}|.$$

对于 $C\subseteq\boldsymbol{F}_q^{2n}$,$\mathrm{swt}(C)$表示 C 中所有非零向量的最小辛重量.给定 $\boldsymbol{F}_q^{2n}$ 上的两个向量$(\boldsymbol{a}|\boldsymbol{b})$和$(\boldsymbol{a}'|\boldsymbol{b}')$,它们的迹辛内积(trace-symplectic inner product)定义为

$$\langle(\boldsymbol{a}|\boldsymbol{b})|(\boldsymbol{a}'|\boldsymbol{b}')\rangle_s=tr_{q/p}(\boldsymbol{b}\cdot\boldsymbol{a}'-\boldsymbol{b}'\cdot\boldsymbol{a}).$$

对于 $\boldsymbol{F}_q^{2n}$ 上的加码(additive code,实际上是一个加群)C,令 $C^{\perp_s}$ 表示 C 关于迹辛内积的对偶码.令$[[n,k,d]]_q$表示用 n 位编码 k 位,距离为 d 的稳定子码,其中每一位都是一个 q 维量子系统.关于量子稳定子码与经典码的联系有如下定理:

定理 1 稳定子码$[[n,k,d]]_q$存在,当且仅当存在一个 $\boldsymbol{F}_q^{2n}$ 上的加码 C,其码字个数$|C|=q^{n-k}$,使得 $C\subseteq C^{\perp_s}$ 且 $\mathrm{swt}(C^{\perp_s}\setminus C)=d$.

这个定理告诉我们,一个量子稳定子码总是与一个经典加码相互对应的.

3. 量子级联码

本节将详细阐述一般意义量子级联码的结构.与经典级联码类似,量子级联码也是由外码和内

† E-mail:lizhuo@xidian.edu.cn

码构成的. 在这里，将仅在以 2 为特征的域上进行说明. 当然，所有结果都可以很直接地推广到任意有限域上.

3.1. 外　码

外码采用稳定子码 $[[N,K,D]]_{2^k}$，与之对应的 $F_{2^k}^{2N}$ 上的加码记为 $\mathscr{O}$，$|\mathscr{O}| = 2^{k(N-K)}$，$\mathscr{O} \subseteq \mathscr{O}^{\perp s}$，$\mathrm{swt}(\mathscr{O}^{\perp s} \setminus \mathscr{O}) = D$.

令 $B = \{\beta_1,\cdots,\beta_k\}$ 表示 F_{2^k}/F_2 的自对偶基. 定义映射 $f_B: F_{2^k} \to F_2^k$，使得 $f_B(a) = (a_1,\cdots,a_k)$，其中 $a = \sum_{i=1}^{k} a_i\beta_i \in F_{2^k}$，$a_i \in F_2$. 由自对偶基的定义易知，对于 F_{2^k} 中的任意两个元素 a 和 a'，有

$$tr_{2^k/2}(aa') = f_B(a) \cdot f_B(a').$$

3.2. 内　码

内码采用稳定子码 $[[n,k,d]]_2$，与之对应的 F_2^{2n} 上的加码记为 $\mathscr{T}$，$|\mathscr{T}| = 2^{n-k}$，$\mathscr{T} \subseteq \mathscr{T}^{\perp s}$，$\mathrm{swt}(\mathscr{T}^{\perp s} \setminus \mathscr{T}) = d$.

由稳定子码理论可知，$\mathscr{T}^{\perp s}$ 的生成矩阵可以表示为 $G^{\perp s}_{(n+k)\times 2n} = \begin{pmatrix} E_{2k\times 2n} \\ G_{(n-k)\times 2n} \end{pmatrix}$，其中，$G_{(n-k)\times 2n}$ 是 $\mathscr{T}$ 的生成矩阵，$E_{2k\times 2n} = \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ z_1 \\ \vdots \\ z_k \end{pmatrix}$，满足 $\langle x_i | x_j \rangle_s = 0$，$\langle z_i | z_j \rangle_s = 0$，$\langle x_i | z_j \rangle_s = \delta_{ij}$，另外，任取 $t, t' \in \mathscr{T}$，有 $\langle t | t' \rangle_s = 0$，$\langle x_i | t \rangle_s = 0$，$\langle z_i | t \rangle_s = 0$，$1 \leqslant i, j \leqslant k$.

3.3. 级联码

利用内码对外码 $\mathscr{O}$ 和 $\mathscr{O}^{\perp s}$ 的每一位进行编码，得到 F_2^{2nN} 上的加码 $\mathscr{C}$ 和 $\mathscr{C}^*$ 如下：

$$\begin{aligned}\mathscr{C} = \{&(c_1\cdots c_N | d_1\cdots d_N) | \\ &(c_i|d_i) = (f_B(a_i)|f_B(b_i))E_{2k\times 2n} \\ &+ t_i, (a_1\cdots a_N | b_1\cdots b_N) \in \mathscr{O}, \\ &t_i \in \mathscr{T}, 1 \leqslant i \leqslant N\}\end{aligned}$$

$$\begin{aligned}\mathscr{C}^* = \{&(c_1^*\cdots c_N^* | d_1^*\cdots d_N^*) | \\ &(c_i^*|d_i^*) = (f_B(a_i^*)|f_B(b_i^*))E_{2k\times 2n} \\ &+ t_i^*, (a_1^*\cdots a_N^* | b_1^*\cdots b_N^*) \in \mathscr{O}^{\perp s}, \\ &t_i^* \in \mathscr{T}, 1 \leqslant i \leqslant N\},\end{aligned}$$

这时有

$$\begin{aligned}&\langle (c_1^*\cdots c_N^* | d_1^*\cdots d_N^*) | (c_1\cdots c_N | d_1\cdots d_N) \rangle_s \\ &= \sum_{i=1}^{N} \langle (c_i^* | d_i^*) | (c_i | d_i) \rangle_s \\ &= \sum_{i=1}^{N} \langle (f_B(a_i^*) | f_B(b_i^*))E_{2k\times 2n} \\ &\quad + t_i^* | (f_B(a_i)|f_B(b_i))E_{2k\times 2n} + t_i \rangle_s \\ &= \sum_{i=1}^{N} \langle (f_B(a_i^*)|f_B(b_i^*)) | (f_B(a_i)|f_B(b_i)) \rangle_s \\ &= \sum_{i=1}^{N} \langle (a_i^* | b_i^*) | (a_i | b_i) \rangle_s \\ &= \langle (a_1^*\cdots a_N^* | b_1^*\cdots b_N^*) | (a_1\cdots a_N | b_1\cdots b_N) \rangle_s \\ &= 0\end{aligned}$$

上式说明 $\mathscr{C}^* \subseteq \mathscr{C}^{\perp s}$，又因为 $|\mathscr{C}| = 2^{k(N-K)} 2^{(n-k)N} = 2^{nN-kK}$，$|\mathscr{C}^*| = 2^{k(N+K)} 2^{(n-k)N} = 2^{nN+kK}$，由维数关系易知 $\mathscr{C}^* = \mathscr{C}^{\perp s}$. 考察如下的集合：

$$\begin{aligned}\mathscr{C}^{\perp s} \setminus \mathscr{C} = \{&(c_1\cdots c_N | d_1\cdots d_N) | \\ &(c_i|d_i) = (f_B(a_i)|f_B(b_i))E_{2k\times 2n} \\ &+ t_i, (a_1\cdots a_N | b_1\cdots b_N) \in \mathscr{O}^{\perp s} \setminus \mathscr{O}, \\ &t_i \in \mathscr{T}, 1 \leqslant i \leqslant N\}\end{aligned}$$

因为 $\mathrm{swt}(\mathscr{O}^{\perp s} \setminus \mathscr{O}) = D$，所以在 $(f_B(a_i)|f_B(b_i))$，$1 \leqslant i \leqslant N$ 这 N 个向量中至少有 D 个非零. 对于每一个非零的 $(f_B(a_i)|f_B(b_i))$ 有 $((f_B(a_i)|f_B(b_i)) \times E_{2k\times 2n} + t_i) \in \mathscr{T}^{\perp s} \setminus \mathscr{T}$，从而由 $\mathrm{swt}(\mathscr{T}^{\perp s} \setminus \mathscr{T}) = d$ 可知 $\mathrm{swt}(c_i | d_i) \geqslant d$.

综上所述，存在一个 F_2^{2nN} 上的加码 $\mathscr{C}$，其码字个数 $|\mathscr{C}| = 2^{nN-kK}$，使得 $\mathscr{C} \subseteq \mathscr{C}^{\perp s}$ 且 $\mathrm{swt}(\mathscr{C}^{\perp s} \setminus \mathscr{C}) \geqslant dD$，从而存在一个稳定子码 $[[nN, kK, \geqslant dD]]_2$，称这样得到的码（或类似构造的码）为量子级联码. 当然，在量子级联码中，对于外码的每一位，也可以采用不同的内码进行编码.

4. 一类量子好码

在这一节中，将具体构造出一类基于级联结构的量子好码.

4.1. 外　码

选择量子 RS 码 $[[N, N-2K, K+1]]_{2^{2k}}$ 作为外码，其中 $N = 2^{2k} - 1$，$1 \leqslant K \leqslant 2^{2k-1} - 1$. 与之对应的 $F_{2^{2k}}^{2N}$ 上的加码 $\mathscr{O} = \mathscr{R} \times \mathscr{R}$，$\mathscr{O}^{\perp s} = \mathscr{R}^{\perp} \times \mathscr{R}^{\perp}$，其中 $\mathscr{R}$ 是 $F_{2^{2k}}$ 上的经典 RS 码 $[N, K, N-K+1]$，其对偶码

$\mathscr{R}^{\perp}$为 RS 码$[N, N-K, K+1]$,乘积为笛卡儿积.

4.2. 内 码

选择 N 个参数为$[[3k, k]]_2$ 的稳定子码作为内码,分别对外码的 N 位进行编码,对应的加码分别记为 $\mathscr{T}_i$,$1\leqslant i\leqslant N$,使得 $\mathscr{T}_i^{\perp s}$ 的生成矩阵具有如下形式:

$$G_i^{\perp s} = \left(\frac{E_i}{G_i}\right) = \begin{pmatrix} 0_{k\times 2k} & I_{k\times k} & P_i & 0_{k\times k} \\ P_{-i} & 0_{k\times k} & 0_{k\times 2k} & 0_{k\times k} \\ \hline P_{-i} & 0_{k\times k} & Q_i & I_{k\times k} \\ Q_{-i} & I_{k\times k} & 0_{k\times 2k} & 0_{k\times k} \end{pmatrix},$$

其中 I 表示单位阵,0 表示全零阵,$P_i = \begin{pmatrix} f_B(\alpha^i\beta_1) \\ \\ f_B(\alpha^i\beta_k) \end{pmatrix}$,$Q_i = \begin{pmatrix} f_B(\alpha^i\beta_{k+1}) \\ \\ f_B(\alpha^i\beta_{2k}) \end{pmatrix}$,$\alpha$ 是 $F_{2^{2k}}$ 的本原元素,$B=\{\beta_1, \cdots, \beta_{2k}\}$是 $F_{2^{2k}}/F_2$ 的自对偶基.读者可以验证,$G_i^{\perp s}$ 是满足 3.2 节中的要求的.

4.3. 级联码

由以上选择的外码和内码可以得到一类量子级联码,记为 $\mathscr{L}_{N,K}$,$N=2^{2k}-1$,$1\leqslant K\leqslant 2^{2k-1}-1$,$k\geqslant 1$.不过,这里的构造方法有些不同,$\mathscr{L}_{N,K}$对应的经典加码 $\mathscr{C}$和 $\mathscr{C}^{\perp s}$的定义如下:

$$\begin{aligned} \mathscr{C} = \{ & (c_{1l}c_{1r}c_{2l}c_{2r}\cdots c_{Nl}c_{Nr} \mid d_{1l}d_{1r}d_{2l}d_{2r}\cdots d_{Nl}d_{Nr}) \mid \\ & (c_{il}\mid d_{il}) = (e_{il}\mid f_{il})E_i + t_{il}, (c_{ir}\mid d_{ir}) = (e_{ir}\mid f_{ir})E_i + t_{ir}, \\ & (e_{il}e_{ir}\mid f_{il}f_{ir}) = (f_B(a_i)\mid f_B(b_i)), t_{il}, t_{ir}\in \mathscr{T}_i, 1\leqslant i\leqslant N, (a_1\cdots a_N\mid b_1\cdots b_N)\in \mathscr{O}\} \\ \mathscr{C}^{\perp s} = \{ & (c_{1l}c_{1r}c_{2l}c_{2r}\cdots c_{Nl}c_{Nr} \mid d_{1l}d_{1r}d_{2l}d_{2r}\cdots d_{Nl}d_{Nr}) \mid \\ & (c_{il}\mid d_{il}) = (e_{il}\mid f_{il})E_i + t_{il}, (c_{ir}\mid d_{ir}) = (e_{ir}\mid f_{ir})E_i + t_{ir}, \\ & (e_{il}e_{ir}\mid f_{il}f_{ir}) = (f_B(a_i)\mid f_B(b_i)), t_{il}, t_{ir}\in \mathscr{T}_i, 1\leqslant i\leqslant N, (a_1\cdots a_N\mid b_1\cdots b_N)\in \mathscr{O}^{\perp s}\} \end{aligned}$$

因此,$\mathscr{L}_{N,K}$的码参数为$[[6kN, 2k(N-2K), d_k]]_2$.下面考察码距 d_k,进而证明 $\mathscr{L}_{N,K}$是量子好码.

引理 2[15] 给定 F_2 上 M 个不同的非零 L 重,其中 $M=\gamma(2^{\delta L}-1)$,$0<\gamma, \delta<1$,则它们的汉明重量之和至少为 $L\gamma(2^{\delta L}-1)(H_2^{-1}(\delta)-o(L))$,其中 $0<H_2^{-1}(\delta)<0.5$ 为熵函数的逆函数,$o(L)$是 L 的高阶无穷小.

定理 3 量子级联码 $\mathscr{L}_{N,K}$是一类量子好码.

证明:给定 R,$0<R<1/3$.选择 $K=\lfloor N(1-3R)/2\rfloor=\lfloor(2^{2k}-1)(1-3R)/2\rfloor$,则对于任意 $k\geqslant 1$,有 $\mathscr{L}_{N,K}$的码率 $R_k=\dfrac{2k(N-2K)}{6kN}=\dfrac{N-2K}{3N}\geqslant R$.

任取$(c_{1l}c_{1r}\cdots c_{Nl}c_{Nr}\mid d_{1l}d_{1r}\cdots d_{Nl}d_{Nr})\in\mathscr{C}^{\perp s}$,由 $\mathscr{C}^{\perp s}$的定义可知,$(c_{ip}\mid d_{ip})=(e_{ip}\mid f_{ip})E_i+t_{ip}$,$t_{ip}\in\mathscr{T}_i$,$p\in\{l, r\}$,$(e_{il}e_{ir}\mid f_{il}f_{ir})=(f_B(a_i)\mid f_B(b_i))$,$1\leqslant i\leqslant N$,$(a_1\cdots a_N\mid b_1\cdots b_N)\in\mathscr{O}^{\perp s}$.因为 $\mathrm{swt}(\mathscr{O}^{\perp s})=K+1$,所以在$(f_B(a_i)\mid f_B(b_i))$,$1\leqslant i\leqslant N$ 这 N 个向量中至少有 $K+1$ 个非零.对于每一个非零的$(f_B(a_i)\mid f_B(b_i))$,$(e_{il}\mid f_{il})$和$(e_{ir}\mid f_{ir})$中至少有一个非零,选择一个非零的$(e_{ip}\mid f_{ip})$,p 为 l 或者 r,因为 $t_{ip}\in\mathscr{T}_i$,所以存在向量$(g_i\mid h_i)\in F_2^{2k}$,使得 $t_{ip}=(g_i\mid h_i)G_i$,从而有

$$\begin{aligned}(c_{ip}\mid d_{ip}) &= (e_{ip}\mid f_{ip})E_i + t_{ip} \\ &= (e_{ip}\mid f_{ip})E_i + (g_i\mid h_i)G_i \\ &= ((f_{ip}+g_i)P_{-i} + h_iQ_{-i}\mid e_{ip} \\ &\quad + h_i\mid e_{ip}P_i + g_iQ_i\mid g_i)\end{aligned}$$

下面考察一下,对于不同的 i,向量$(c_{ip}\mid d_{ip})$在什么情况下相同.分两种情况进行讨论:

如果 $e_{ip}P_i+g_iQ_i\neq 0$,则对于不同的 i,要使$(c_{ip}\mid d_{ip})$相同,g_i 必须相同,此时,e_{ip} 必须不同,这是因为:由于向量$(e_{ip}\mid g_i)\in F_2^{2k}$,故存在 $w_i\in F_{2k}$,使得 $f_B(w_i)=(e_{ip}\mid g_i)$,则由 P_i和 Q_i 的定义可得 $e_{ip}P_i+g_iQ_i=f_B(\alpha^iw_i)\neq 0$,假设 e_{ip} 也相同,则 w_i 相同,$f_B(\alpha^iw_i)$必不同.因此,要使$(c_{ip}\mid d_{ip})$相同,e_{ip}必须不同,而 k 维向量 e_{ip}至多有 2^k 种不同取值,所以在这种情况下,对于不同的 i,至多有 2^k 个$(c_{ip}\mid d_{ip})$是相同的.

如果 $e_{ip}P_i+g_iQ_i=0$,则有 $e_{ip}=g_i=0$,由于$(e_{ip}\mid f_{ip})$非零,故 f_{ip}一定非零,此时有$(f_{ip}+g_i)P_{-i}+h_iQ_{-i}=f_{ip}P_{-i}+h_iQ_{-i}\neq 0$.要使$(c_{ip}\mid d_{ip})$相同,$h_i$必须相同,则与第一种情况同样的道理可知,此时 f_{ip}必须不同.所以在这种情况下,对于不同的 i,也

是至多有 2^k 个 $(\boldsymbol{c}_{ip}|\boldsymbol{d}_{ip})$ 是相同的.

综上所述，在 $(\boldsymbol{c}_{ip}|\boldsymbol{d}_{ip})$，$1\leqslant i\leqslant N$，$p\in\{l,r\}$ 这 $2N$ 个 $\boldsymbol{F}_2$ 上的 $6k$ 重中，至少有 $\frac{K+1}{2^k}$ 个不同的非零 $6k$ 重. 又由 K 的选择可得 $\frac{K+1}{2^k}\geqslant\frac{2^{2k}-1}{2^k}\frac{1-3R}{2}\geqslant\frac{1-3R}{2}(2^k-1)$，在引理 2 中，令 $L=6k$，$M=\frac{1-3R}{2}\times(2^k-1)$，$\gamma=\frac{1-3R}{2}$，$\delta=1/6$，得到它们的汉明重量之和至少为 $3k(1-3R)(2^k-1)(H_2^{-1}(1/6)-o(k))$，从而有

$$\begin{aligned}&\mathrm{wt}(\boldsymbol{c}_{1l}\boldsymbol{c}_{1r}\cdots\boldsymbol{c}_{Nl}\boldsymbol{c}_{Nr}|\boldsymbol{d}_{1l}\boldsymbol{d}_{1r}\cdots d_{Nl}\boldsymbol{d}_{Nr})\\&\geqslant 2^k3k(1-3R)(2^k-1)(H_2^{-1}(1/6)-o(k))\\&=3k(1-3R)(2^{2k}-2^k)(H_2^{-1}(1/6)-o(k))\end{aligned}$$

其中 wt 表示汉明重量，因子 2^k 是因为在最坏的情况下，每个不同的非零 $6k$ 重都出现了 2^k 次. 另外，对于任意向量 $(\boldsymbol{a}|\boldsymbol{b})$，显然有 $\mathrm{swt}(\boldsymbol{a}|\boldsymbol{b})\geqslant\frac{1}{2}\mathrm{wt}(\boldsymbol{a}|\boldsymbol{b})$，因此有

$$\begin{aligned}&\mathrm{swt}(\boldsymbol{c}_{1l}\boldsymbol{c}_{1r}\cdots\boldsymbol{c}_{Nl}\boldsymbol{c}_{Nr}|d_{1l}\boldsymbol{d}_{1r}\cdots d_{Nl}\boldsymbol{d}_{Nr})\\&\geqslant 3k\frac{1-3R}{2}(2^{2k}-2^k)(H_2^{-1}(1/6)-o(k))\end{aligned}$$

$$\begin{aligned}d_k&\geqslant\mathrm{swt}(\mathscr{C}^{\perp s})\\&\geqslant 3k\frac{1-3R}{2}(2^{2k}-2^k)(H_2^{-1}(1/6)-o(k))\end{aligned}$$

码距与码长之比 $\frac{d_k}{6kN}\geqslant\frac{1-3R}{4}\frac{2^{2k}-2^k}{2^{2k}-1}(H_2^{-1}(1/6)-o(k))\doteq\frac{H_2^{-1}(1/6)}{4}(1-3R)$，当 $k\to\infty$. 这就证明了 $\mathscr{L}_{N,K}$ 是量子好码.

5. 结　　论

本文所做的工作主要有两点：首先借助经典级联码的思想，对一般意义的量子级联码的构造方法进行了详细说明；更重要的是，经过巧妙设计，具体构造出了一类基于级联结构的量子好码. 与前人的工作相比，本文工作的意义在于：虽然在此之前，已经发现了一些其他类型的量子好码，但是这些码或者是由经典好码直接移植过来的[10—12]，或者只是证明了其存在性，并未给出具体构造方法（例如量子 GV 限[9]）. 而本文是首次利用经典坏码具体构造出了量子好码，因此具有重要的理论意义.

[1] Song K H 2005 *Acta Phys. Sin.* **54** 4730 (in Chinese) [宋克慧 2005 物理学报 **54** 4730]

[2] Bennet C H, Divincenzo D P, Smolin J A, Wotters W K 1996 *Phys. Rev.* A **54** 3824

[3] Shor P W 1995 *Phys. Rev.* A **52** 2493

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

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

[6] Calderbank A R, Shor P W 1996 *Phys. Rev.* A **54** 1098

[7] Steane A M 1996 *Proc. Roy. Soc. London Ser.* A **452** 2551

[8] Gottesman D 1996 *Phys. Rev.* A **54** 1862

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

[10] Ashikhmin A, Litsyn S, Tsfasman M 2001 *Phys. Rev.* A **63** 032311

[11] Chen H, Ling S, Xing C 2001 *IEEE Trans. Inform. Theory* **47** 2055

[12] Matsumoto R 2002 *IEEE Trans. Inform. Theory* **48** 2122

[13] Forney G D 1966 *Concatenated Codes* (Cambridge, MA: MIT Press)

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

[15] MacWilliams F J, Sloane N J A 1977 *The Theory of Error-Correcting Codes* (New York: North-Holland) p310

A family of asymptotically good quantum codes based on code concatenation*

Li Zhuo† Xing Li-Juan

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

(Received 12 December 2006; revised manuscript received 2 February 2007)

Abstract

Using the idea of code concatenation in classical coding theory, we make the suggestion of constructing general concatenated quantum codes by choosing certain quantum codes as outer code and inner code. Then by concatenating quantum RS outer codes with a set of special quantum inner codes, one can construct a family of concatenated quantum codes, which is asymptotically good. In the field of quantum error-correcting codes, this is the first time that a family of asymptotically good quantum code is constructed using bad classical codes.

Keywords: asymptotically good quantum codes, concatenated quantum codes, quantum error-correcting codes, quantum information

PACC: 0367, 0365, 0210

† E-mail: lizhuo@xidian.edu.cn