* 1

自正交码的组合构造与应用

刘乃功[1]，　郭罗斌[1]，　刘　健[2]
(1. 空军工程大学　理学院，陕西　西安　710051；2 空军工程大学　导弹学院，陕西　三原　713800)

摘　要：量子纠错码是量子计算和量子通信可靠运行的保障，构造具有很好参数的量子纠错码是重要的研究问题之一。用二元线性码构造量子码的方法有 CSS(Calderbank－Shor－Steane)方法和 Steane 方法，这两种方法都建立在如何构造给定对偶距离的自正交码上，研究了用组合方法构造二元自正交码问题。由已知对偶距离的二元自正交码链，用组合方法构造对偶距离为 3、4、5 和 6 的二元自正交码，以及对偶距离为 3、4、5 和 6 的二元自正交码构成二元自正交码链的条件。在此基础上，对每个满足 $47\leqslant n\leqslant 70$ 的，构造出参数为 $[n, n-s-t, 5]\subseteq[n, n-s, 3]$ 和 $[n, n-u-v, 6]\subseteq[n, n-v, 4]$ 的 S－链。利用所得到的码链，由 Steane 构造法构造出距离为 5 和 6 的具有很好参数的量子纠错码，改进了前人得到的几个量子纠错码的参数。

关键词：自正交码；S－链；量子纠错码
中图分类号：O157.4　　**文献标识码**：A　　**文章编号**：1009－3516(2009)01－0088－03

自 Shor[1] 和 Steane[2] 创立量子纠错码理论以来，量子纠错码成为数学、计算机科学和物理学的热门研究课题，而构造具有很好参数的量子纠错码则是其中的最重要的研究问题之一。

1996 年，Calderbank 和 Shor[3] 以及 Steane[4] 给出第一个基于二元码构造量子纠错码的方法－CSS 构造法(Calderbank－Shor－Steane Construction)。如果有一个对偶距离为 d 的二元自正交码，利用 CSS 构造法就可得到 $[n, n-2k, d]$ 量子纠错码。1999 年，Steane 在文献[5]中改进了 CSS 构造法，确立了 Steane 构造法。利用 Steane 构造法构造量子纠错码时需要两个具有特定对偶距离的二元自正交码。李瑞虎在文献[6]中将满足 Steane 构造法的 2 个二元码所具有的特性加以抽象概括，引入称为 S－链的二元码链的概念，将构造量子纠错码问题转化为 S－链的构造。

1　预备知识

要构造某些参数的量子纠错码或 S－链，首先要解决对于给定的码长 n 和极小距离 d，如何构造对偶距离为 d 的二元自正交码的问题。如果 $d_1 > d_2$，如何构造对偶距离分别为 d_1 和 d_2 的二元自正交码 C_1 和 C_2，使得他们的对偶距离分别为 d_1 和 d_2，并且 $C_2\subseteq C_1$。为研究这些问题，先对如下概念和定理进行介绍。

设 $\boldsymbol{F}_2$ 为二元域，$\boldsymbol{F}_2^n$ 为 $\boldsymbol{F}_2$ 上 n 维行线性空间，$\boldsymbol{F}_2^n$ 的 k 维子空间 C 叫做码长为 n 的 k 维二元码，并记为 $C=[n,k]$；如果 C 的 Hamming 距离为 d，则简记为 $C=[n,k,d]$。

设 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，$\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)$，$\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的欧氏(Euclid)内积为 $\boldsymbol{X}\cdot\boldsymbol{Y}=x_1y_1+x_2y_2+\cdots+x_ny_n=\boldsymbol{X}\boldsymbol{Y}^{\mathrm{T}}$。若 $\boldsymbol{X}\cdot\boldsymbol{Y}=0$，称 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 正交。若 C 是一个 q 元 $[n,k]$ 线性码，C 的 Euclid 对偶码记为 $C^{\perp}=\{\boldsymbol{X}:\boldsymbol{X}\cdot\boldsymbol{Y}=0$，对任意的 $\boldsymbol{Y}\in C\}$，则 $C^{\perp}$ 为 $[n,n-k]$ 线性码。若 $C\subseteq C^{\perp}$，称 C 为自正交的；若 $C=C^{\perp}$，则称 C 为自对偶的。

定理 1　(Steane 构造法) 如果 $C^{\perp}\subset C\subset C'$，且 $k_1\geqslant k+2$，则可构造出参数为 $[[n,k+k_1-n,\geqslant\min\{d,$

*　**收稿日期**：2008－07－03
基金项目：国家自然科学基金资助项目(60573040)
作者简介：刘乃功(1976－)，男，陕西韩城人，副教授，主要从事函数论、代数编码等领域的研究.
E－mail：haoling@snnu.edu.cn.

$\lceil\frac{3}{2}\rceil d_1\}]]$ 的加性量子码。

满足 Steane 构造法的条件 2 个二元码 C 和 C' 具有特征 $C^{\perp}\subset C\subset C'$。将这 2 个二元码具有的特征提取出来并推广到二元码的序列上,就是文献[6]引入的 S－链的概念。

定义 1　设 $C_i=[n,k_i,d_i]$ 为二元码,$1\leqslant i\leqslant m$。若 $C_{i+1}^{\perp}\subset C_{i+1}\subset C_i$ 且 $k_{i+1}+1$,则称码的序列 $C_m\subset C_{m-1}\subset\cdots\subset C_2\subset C_1$ 为 S－链。

对于 S－ 链 $C_m\subset C_{m-1}\subset\cdots\subset C_2\subset C_1$ 中的每个码 $C_i,C_i^{\perp}$,是自正交码且对偶距离为 d_i. 本文研究如何由已知自正交码链及其对偶所构成的 S－链, 构造出新的对偶距离为 3、4、5 和 6 的自正交码, 以及它们构成的自正交码链和 S－ 链, 再利用构造的 S－ 链构造距离为 5 和 6 的量子纠错码。

2　自正交码和 S－链的构造

本节研究由自正交码链及其对偶所构成的 S－ 链, 如何构造出新的对偶距离为 3、4、5 和 6 的自正交码。为简化叙述, 假设 n 为偶数, 用 $\boldsymbol{1}_n=(1,1,\cdots,1)$ 表示为全 1 向量。

引理 1　设存在 S－ 链$[n,n-s-t-1,6]\subset[n,n-s-1,4]\subset[n,n-1,2]$ 和$[m,m-u-v,5]\subset[m,m-u-v,5]\subset[m,m-u,3]$。记 $a=\max\{s,u\}+1,b=\max\{t,v\}+a$。

1)存在 S－ 链$[m+n,m+n-a-b-t,5]\subset[m+n,m+n-a,3]$;

2)设 m 为偶数, 则有 S－ 链$[m+n,m+n-a-b-t-1,t]\subset[m+n,m+n-a-1,4]\subset[m+n,m+n-1,2]$。

证明　结论(2)的证明见文献[7]的定理 1.2, 这里仅证明结论(1)。

设 S－ 链$[n,n-s-t-1,6]\subset[n,n-s-1,4]\subset[n,n-1,2]$中$[n,n-s-1,4]\subset$ 码的校验矩阵为 $\boldsymbol{H}_1$,$[n,n-s-t-1,6]$,码的校验矩阵为 $\boldsymbol{H}_2$,其中:

$$\boldsymbol{H}_1=\begin{pmatrix}\boldsymbol{1}_n\\ \boldsymbol{X}\end{pmatrix},\ \boldsymbol{H}_2=\begin{pmatrix}\boldsymbol{H}_1\\ \boldsymbol{Y}\end{pmatrix}$$

1)设 S－ 链$[m,m-u-v-,5]\subset[m,m-u,3]$中$[m,m-u,3]$码的校验矩阵为 $\boldsymbol{H}'_1$,$[m,m-u-v,5]$码的校验矩阵为 $\boldsymbol{H}'_2=\begin{pmatrix}\boldsymbol{H}'_1\\ \boldsymbol{Y}'\end{pmatrix}$。假定 $u\geqslant s,v\geqslant t$, 设 $\boldsymbol{X}_0=\begin{pmatrix}\boldsymbol{X}\\ \boldsymbol{0}_{(u-s)\times n}\end{pmatrix},\boldsymbol{Y}_0=\begin{pmatrix}\boldsymbol{Y}\\ \boldsymbol{1}_{(v-t)\times n}\end{pmatrix}$,构造矩阵 $\boldsymbol{H}''_1,\boldsymbol{H}''_2$ 分别为:

$$\boldsymbol{H}''_1=\begin{pmatrix}\boldsymbol{H}'_1 & \boldsymbol{X}_0\\ \boldsymbol{0}_{1\times m} & \boldsymbol{1}_n\end{pmatrix},\boldsymbol{H}''_2=\begin{pmatrix}\boldsymbol{H}'_1 & \boldsymbol{X}_0\\ \boldsymbol{Y}' & \boldsymbol{Y}_0\\ \boldsymbol{1}_{t\times m} & \boldsymbol{X}\\ \boldsymbol{1}_{1\times m} & \boldsymbol{1}_n\end{pmatrix}$$

由已知条件可推出 $\boldsymbol{H}''_1$ 的任意两列线性无关, 所以 $\boldsymbol{H}''_1$ 生成的自正交码的对偶距离为 3; 仿照文献[7]的定理 1.2 可证明 $\boldsymbol{H}''_2$ 生成的自正交码的对偶距离为 5; 由于 $\boldsymbol{H}''_1$ 为 $\boldsymbol{H}''_2$ 的子矩阵, $\boldsymbol{H}''_1$ 生成的自正交码是 $\boldsymbol{H}''_2$ 生成的自正交码的子码, 故此时结论 1)成立。同理可证其他情况下结论 1)正确。

文献[8－9]以及文献[5]研究了码长 $21\leqslant n\leqslant 40$ 的自正交码链和 S－链的构造, 其结果可总结如下:

引理 2　1)存在 S－ 链$[23,12,5]\subset[23,18,3],[24,13,5]\subset[24,19,3],[24,12,6]\subset[24,18,4]\subset[24,23,2],[31,21,5]\subset[31,26,3],[32,21,6]\subset[32,26,4]\subset[32,31,2]$;

2)如果 $25\leqslant n\leqslant 30$,则存在 S－链$[n,n-12,5]\subset[n,n-6,3]$;当 $n=26,28,30$ 时, 还存在 S－链$[n,n-13,6]\subset[n,n-7,4]\subset[n,n-1,2]$;

3)如果 $n=36,38,40$,则存在 S－链$[n,n-13,5]\subset[n,n-6,3]$ 和$[n,n-14,6]\subset[n,n-7,4]\subset[n,n-1,2]$。

利用引理 2 给出的 S－链, 由引理 1,可构造出码长更大的 S－链。

定理 2　1)存在 S－ 链$[47,30,5]\subset[47,41,3],[48,31,5]\subset[48,42,3],[48,30,6]\subset[48,41,4],[55,38,5]\subset[55,49,3],[55,49,3],[56,39,5]\subset[56,50,3],[56,38,6]\subset[56,49,4]$;

2) 设 $49\leqslant n\leqslant 62$ 且 $n\neq 55,56$, 则存在 S－ 链$[n,n-19,5]\subset[n,n-7,3]$, 当 n 为偶数时, 还存在 S－链$[n,n-20,6]\subset[n,n-8,4]\subset[n,n-1,2]$;

3) 设 $63 \leqslant n \leqslant 70$ ，则存在 S - 链 $[n, n-20, 5] \subset [n, n-7, 3]$ ，当 n 为偶数时，还存在 S - 链 $[n, n-21, 6] \subset [n, n-8, 4] \subset [n, n-1, 2]$ 。

证明 利用 S - 链 $[23, 12, 5] \subset [23, 18, 3]$ 和 $[24, 12, 6] \subset [24, 18, 4] \subset [24, 23, 2]$ ，可构造出 $[47, 30, 5] \subset [47, 41, 3]$ 。

依据引理 2，同理可构造出定理中给出的其他 S - 链。

3 量子码的构造

依据 Steane 构造法，利用 S - 链 $[n, n-x, 5] \subset [n, n-y, 3]$ 可构造出参数为 $[n, n-x-y, 5]$ 的量子码，利用 S - 链 $[n, n-x-1, 6] \subset [n, n-y-1, 4]$ 可构造出参数为 $[[n, n-x-y-2, 6]]$ 的量子码。依据定理 2，可得到如下定理 3。

定理 3 1) 存在参数为 $[[47, 24, 5]]$，$[[48, 25, 5]]$，$[[48, 23, 6]]$，$[[55, 32, 5]]$，$[[56, 33, 5]]$，$[[56, 31, 6]]$ 的量子码；

2) 设 $49 \leqslant n \leqslant 62$ 且 $n \neq 55, 56$，则存在参数为 $[[n, n-26, 5]]$ 的量子码，当 n 为偶数时，还存在参数为 $[[n, n-28, 6]]$ 的量子码；

3) 设 $63 \leqslant n \leqslant 70$，则存在参数为 $[[n, n-27, 5]]$ 的量子码，当 n 为偶数时，还存在参数为 $[[n, n-29, 6]]$ 的量子码。

4 结束语

当 $63 \leqslant n \leqslant 70$ 时，定理 3 构造的 $[[n, n-27, 5]]$ 的量子码，以及 n 为偶数时 $[[n, n-29, 6]]$ 的量子码是新的结果。$[[47, 24, 5]]$，$[[48.25.5]]$，$[[48, 23, 6]]$，$[[55, 32, 5]]$，$[[56, 33, 5]]$，$[[56, 31, 6]]$ 比文献[11]的结果好。当 $49 \leqslant n \leqslant 62$ 且 $n \neq 55, 56$，参数为 $[[n, n-26, 5]]$ 的量子码，以及当 n 为偶数时，参数为 $[[n, n-28, 6]]$ 的量子码与文献[10]的结果一致。

参考文献：

[1] Shor P W. Scheme for Reducing Decoherence in Quantum Computer Memory [J]. Phys Rev A, 1995, 52: 2493 - 2396.

[2] Steane A M. Error Correcting Codes in Quantum Theory [J]. Phys Rev Lett, 1996, 77: 793 - 797.

[3] Calderbank A R, Shor P W. Good Quantum Error - correcting Codes Exist [J]. Phys Rev A, 1997, 54: 900 - 911.

[4] Steane A M. Simple Quantum Error Correcting Codes [J]. Phys Rev A, 1996, 77: 793 - 797.

[5] Steane A M. Enlargement of Calderbank - Shor - Steane Quantum Codes [J]. IEEE Trans Inf Theory, 1999, 45: 2492 - 2495.

[6] Li Ruihu. Research on Additive Quantum Codes [D]. Xi'an: PhD Thesis of Northwestern Polytechnical University, 2004.

[7] Ruihu Li, Xueliang Li. Binary Construction of Quantum Codes of Minimum Distances Five and Six [J]. Discrete Math, 2008, 308: 1603 - 1611.

[8] 贺筱军, 赵学军, 李瑞虎. 对偶距离为 5 的极大自正交码及其子码[J]. 计算机工程与应用, 2007, 43(17): 45 - 49.
HE Xiaojun, ZHAO Xuejun, LI Ruihu. Maximal Self - orthogonal Codes of Dual Distance Five and Their Subcodes [J]. Computer Engineering and Appl, 2007, 43(17): 45 - 49. (in Chinese)

[9] 郭罗斌, 贺筱军, 李瑞虎. 距离为 6 的自对偶的子码[J]. 计算机工程与应用, 2008, 44(11): 34 - 36.
GUO Luobin, HE Xiaojun, LI Ruihu. Subcodes of Self - dual Codes of Minimal Distance Six [J]. Computer Engineering and Appl, 2008, 44(11): 34 - 36. (in Chinese)

[10] 马月娜, 王 雷, 赵学军. 四元码链和量子纠错码的构造[J]. 空军工程大学学报: 自然科学版, 2008, 9(3): 83 - 86.
MA Yuena, WANG Lei, ZHAO Xuejun. Quaternary Codes Chain and Construction of Quantum Codes [J]. Journal of Air Force Engineering University: Natural Science Edition, 2008, 9(3): 83 - 86. (in Chinese)

[11] 李瑞虎. 用四元循环码构造的线性量子码[J]. 空军工程大学学报: 自然科学版, 2007, 8(1): 85 - 87.
LI Ruihu. Linear Quantum Codes Constructed From Quaternary Cyclic Codes [J]. Journal of Air Force Engineering University: Natural Science Edition, 2007, 8(1): 85 - 87. (in Chinese)

编辑：徐楠楠

(下转第 94 页)