四元码链和量子纠错码的构造

马月娜， 王 雷， 赵学军， 冯有前
(空军工程大学 理学院，陕西 西安 710051)

摘 要:研究量子纠错码的构造,并构造出具有较好参数的量子纠错码。首先利用随机搜索的方法,得到一些具有较好参数的短码长自正交码及由这些自正交码所形成的自正交码链;其次根据这些自正交码的对偶码可得到一系列相应参数的L-链;最后通过组合构造方法和得到的这些L-链构造出量子纠错码。得到一些码长 n 满足 $20\leqslant n\leqslant 36$ 和 $n=40,45,50,55,60$ 、对偶距离达到5或6的自正交码,并根据这些自正交码和它们的对偶码分别构造出了相应参数的自正交码链及L-链。构造出具有较好参数的量子纠错码,其中码长在 $20\leqslant n\leqslant 30$ 范围内的量子纠错码的参数达到或超过了已知的量子纠错码,码长在 $31\leqslant n\leqslant 36$ 和 $40\leqslant n\leqslant 64$ 范围内的量子纠错码都是新的。

关键词:自正交码;自正交码链;L-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(2008)03-0083-04

自Shor和Steane创立量子纠错码理论以来,量子纠错码就成为人们研究的热门问题[1-2]。通过Agebraic Gometric码、Reed-Muller码等可构造出很多具有较好的量子纠错码[3-7]。李瑞虎在文献[8]中将对偶码为四元自正交码的一个码具有的特征提取出来,推广到四元码的序列上,引入称为L-链的四元码概念,并用组合和递归的方法研究了以L-链为模块对中等码长 $n(n\leqslant 2\,047)$、距离为5的线性量子纠错码的构造。

本文利用随机搜索方法,得到 F_4 上码长 $20\leqslant n\leqslant 36$ 以及 $n=40,45,50,55,60$ 、对偶距离为5或6的自正交码,从而构造出一系列自正交码链以及L-链,并根据文献[8]中的构造方法和这些L-链再进一步构造出相应参数的量子纠错码。

1 自正交码链和L-链的构造

设 $F_4=\{0,1,\omega,\bar{\omega}\}$ 是四元有限域,其中 $\bar{\omega}=\omega^2=\omega+1,\bar{\omega}^3=\omega^3=1$。$F_4^n$ 的 k 维子空间 C 称为四元 $[n,k]$ 线性码。F_4^n 上的向量 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的Hermite内积为:$(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{X}\bar{\boldsymbol{Y}}^{\mathrm{T}}=x_1\bar{y}_1+x_2\bar{y}_2+\cdots+x_n\bar{y}_n$,若 $(\boldsymbol{X},\boldsymbol{Y})=0$,则称 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ Hermite正交。若 C 是一个四元 $[n,k]$ 线性码,C 的Hermite对偶码记为 $C^{\perp}=\{\boldsymbol{X}\mid(\boldsymbol{X},\boldsymbol{Y})=0,\forall\boldsymbol{Y}\in C\}$,若 $C\subseteq C^{\perp}$,称 C 为自正交码。

定义1 先给出文献[8]中L-链概念。设 $C_i=[n,k_i,d_i],1\leqslant i\leqslant m$ 为四元码。若 $C_i\subset C_{i+1}\subset C_{i+1}^{\perp}$ 且 $k_i\leqslant k_{i+1}+1$,则称码的序列 $C_1\subset C_2\subset\cdots\subset C_{m-1}\subset C_m$ 为自正交码链;若 $C_{i+1}^{\perp}\subset C_{i+1}\subset C_i$ 且 $k_i\geqslant k_{i+1}+1$,则称码的序列 $C_m\subset C_{m-1}\subset\cdots\subset C_2\subset C_1$ 为L-链。

定理1 存在如下自正交码链

$[20,4,10]\subset[20,6,10]\subset[20,8,8]\subset[20,9,6]$; $[21,9,8]\subset[21,10,8]$;
$[22,4,10]\subset[22,6,10]\subset[22,8,10]\subset[22,10,8]$; $[23,4,12]\subset[23,6,12]\subset[23,8,10]\subset[23,10,8]$;
$[24,4,12]\subset[24,6,12]\subset[24,8,10]\subset[24,10,8]$; $[25,4,10]\subset[25,6,10]\subset[25,8,10]\subset[25,10,10]$;

收稿日期:2007-06-19
基金项目:国家自然科学基金资助项目(60573040);空军工程大学理学院科研基金资助项目
作者简介:马月娜(1977-),女,陕西西安人,讲师,从事代数编码与密码学研究. E-mail:mayuena2007@yahoo.com.cn

[26,5,12]⊂[26,9,12]⊂[26,10,10]; [27,4,14]⊂[27,6,14]⊂[27,9,12]⊂[27,10,10];
[28,5,14]⊂[28,9,10]⊂[28,10,10]; [29,4,16]⊂[29,7,14]⊂[29,9,12]⊂[29,11,10];
[30,5,16]⊂[30,9,12]⊂[30,11,10]; [31,4,18]⊂[31,7,16]⊂[31,9,14]⊂[31,11,10];
[32,5,18]⊂[32,9,14]⊂[32,11,12]; [33,4,18]⊂[33,7,16]⊂[33,9,14]⊂[33,11,12];
[34,5,22]⊂[34,9,16]⊂[34,11,12]; [35,4,20]⊂[35,7,18]⊂[35,9,16]⊂[35,11,14];
[36,5,24]⊂[36,9,16]⊂[36,11,14]; [40,4,24]⊂[40,7,20]⊂[40,10,16]⊂[40,12,16];
[45,4,26]⊂[45,9,22]⊂[45,10,20]⊂[45,12,16]; [50,4,30]⊂[50,8,26]⊂[50,10,24];
[55,4,34]⊂[55,8,28]⊂[55,11,24]; [60,4,38]⊂[60,8,32]⊂[60,11,28]。

证明 从低维自正交码出发,通过逐行添加满足条件的码字来增加码的维数,使每个新生成的码都是自正交码,从而可构造出高维自正交码并构造出自正交码链。根据这种构造自正交码链的方法,利用计算机随机搜索,得到码长 $20\leqslant n\leqslant 36$ 以及 $n=40,45,50,55,60$、对偶距离为 5 或 6 的自正交码,进而构造出定理所包含的这些自正交码链。这里只给出码长 $n=20$ 的自正交码链所包含的自正交码的生成矩阵 $G_{20,k,d}$。

$$G_{20,4,10}=\begin{pmatrix}1&0&0&0&2&3&2&3&0&0&1&1&1&0&3&2&3&2&1&1\\0&1&0&0&1&1&2&3&2&3&1&0&1&1&1&1&2&3&2&3\\0&0&1&0&2&3&1&1&3&2&1&1&0&1&2&3&1&1&3&2\\0&0&0&1&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1\end{pmatrix}$$

$$G_{20,6,10}=\begin{pmatrix}1&0&0&0&0&0&1&0&2&1&0&3&1&2&3&0&3&3&3&3\\0&1&0&0&0&0&2&1&2&0&1&3&2&2&0&1&3&1&1&0\\0&0&1&0&0&0&2&3&1&3&0&3&0&3&2&1&1&0&1&1\\0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&1&1&1&1&1&1&1&0\\0&0&0&0&1&0&3&0&2&3&1&0&2&0&3&2&3&0&0&2\\0&0&0&0&0&1&3&2&2&0&1&3&1&3&2&2&2&2&3&1\end{pmatrix}$$

$$G_{20,8,8}=\begin{pmatrix}1&0&0&0&0&0&0&0&2&0&2&2&0&0&2&1&0&1&0&1\\0&1&0&0&0&0&0&0&0&3&0&2&0&2&1&1&3&1&2&2\\0&0&1&0&0&0&0&0&0&2&2&3&2&1&2&2&3&1&2&1\\0&0&0&1&0&0&0&0&2&1&2&2&1&3&2&3&0&2&2&1\\0&0&0&0&1&0&0&0&2&0&0&3&1&2&0&1&1&1&1&3\\0&0&0&0&0&1&0&0&1&1&3&1&2&2&0&2&2&2&3&2\\0&0&0&0&0&0&1&0&0&1&2&1&1&3&1&1&3&2&2&2\\0&0&0&0&0&0&0&1&2&1&2&3&0&2&3&2&1&3&3&1\end{pmatrix}$$

$$G_{20,9,6}=\begin{pmatrix}1&0&0&0&0&0&0&0&0&1&2&1&0&0&0&1&1&0&1&2\\0&1&0&0&0&0&0&0&0&3&0&2&0&2&1&1&3&1&2&2\\0&0&1&0&0&0&0&0&0&2&2&3&2&1&1&2&3&2&2&1\\0&0&0&1&0&0&0&0&0&2&1&1&3&3&3&1&0&3&2\\0&0&0&0&1&0&0&0&0&1&0&0&1&2&0&1&0&2&0&0\\0&0&0&0&0&1&0&0&0&2&3&3&2&2&1&2&1&1&0&0\\0&0&0&0&0&0&1&0&0&1&2&1&1&3&2&1&3&1&2&2\\0&0&0&0&0&0&0&1&0&0&2&0&0&2&2&2&0&1&2&2\\0&0&0&0&0&0&0&0&1&3&0&2&0&0&3&0&3&1&3&2\end{pmatrix}$$

由于其它码长的自正交码链的构造过程与上述码长 $n=20$ 的自正交码链的构造过程完全类似,这里不再一一叙述。总结上述讨论,则定理得证。

由 L-链的定义和上述定理的结论,可得如下推论。

推论 1 *存在如下 L-链:*

[20,11,6]⊂[20,12,5]⊂[20,14,4]⊂[20,16,3]; [21,11,7]⊂[21,12,5];
[22,12,6]⊂[22,14,5]⊂[22,16,4]⊂[22,18,3]; [23,13,6]⊂[23,15,5]⊂[23,17,4]⊂[23,19,3];
[24,14,6]⊂[24,16,5]⊂[24,18,4]⊂[24,20,3]; [25,15,6]⊂[25,17,5]⊂[25,19,4]⊂[25,21,3];
[26,16,6]⊂[26,17,5]⊂[26,21,4]; [27,17,6]⊂[27,18,5]⊂[27,21,4]⊂[27,23,3];
[28,18,6]⊂[28,19,5]⊂[28,23,4]; [29,18,6]⊂[29,20,5]⊂[29,22,4]⊂[29,25,3];
[30,19,6]⊂[30,21,5]⊂[30,25,4]; [31,20,6]⊂[31,22,5]⊂[31,24,4]⊂[31,27,3];
[32,21,6]⊂[32,23,5]⊂[32,27,4]; [33,22,6]⊂[33,24,5]⊂[33,26,4]⊂[33,29,3];
[34,23,6]⊂[34,25,5]⊂[34,29,4]; [35,24,6]⊂[35,26,5]⊂[35,28,4]⊂[35,31,3];
[36,25,6]⊂[36,27,5]⊂[36,31,4]; [40,28,6]⊂[40,30,5]⊂[40,33,4]⊂[40,36,3];
[50,40,5]⊂[50,42,4]⊂[50,46,3]; [50,33,6]⊂[50,35,5]⊂[50,36,4]⊂[45,41,3];
[55,44,5]⊂[55,47,4]⊂[55,51,3]; [60,49,5]⊂[60,52,4]⊂[60,56,3]。

2 量子纠错码的构造

根据推论 1 构造出的这些 L-链可知,不同的 L-链分别包含着距离为 5 和距离为 3 以及距离为 5 和距

离为2的码,也就是说可以由已知 L-链$[n,n-s-t,5]\subset[n,n-s,3]$和 L- 链$[m,m-u-k,5]\subset[m,m-k,2]$逐步构造新的距离为5的量子纠错码[9-10]。我们的构造基于文献[8]中的引理1。

引理1　1)设有 L-链$[n,n-s-t,5]\subset[n,n-s,3]$和 L- 链$[m,m-u-k,5]\subset[m,m-k,2]$则有参数为$[n+n,n+n-\max\{t,u\}-s-k,5]$的码 C 满足 $C^{\perp}\subset C$,从而有参数为$[n+n,n+n-2\max\{t,u\}-2s-2k,5]$的量子纠错码;

2)设有 L-链$[n,n-s-t,6]\subset[n,n-s,4]$和 L- 链$[m,m-u-k,6]\subset[m,m-k,2]$,则有参数为$[n+m,n+m-\max\{t,u\}-s-k,6]$的码 C 满足 $C^{\perp}\subset C$,从而有参数为$[n+m,n+m-2\max\{t,u\}-2s-2k,6]$的量子纠错码。

根据推论1中已知的L-链和引理1可以直接得到下面的两个定理。

定理2　1)当 $n=20,22,23,23,25,27,29,31,33,35,40,45$ 时,存在参数为$[[n+20,n-4,5]]$的量子纠错码;

2)当 $n=23,25,29,31,33,35,36,40$ 时,存在参数为$[[n+23,n-1,5]]$的量子纠错码;

3)当 $n=35,40$ 时,存在参数为 $[[n+22,n-2,5]]$的量子纠错码;

特别地,存在量子纠错码$[[61,35,5]],[[64,38,5]]$。

证明　1)根据推论1,当 $n_1=20,22,23,t_1=2;n_2=24,25,t_2=4;n_3=27,29,31,33,35,t_3=5;n_4=40,45,t_4=6$ 时,有 L- 链$[n_i,n_i-t_i-4,5]\subset[n_i,n_i-4,3]$,再利用引理1和 L- 链$[20,20-7-1,5]\subset[20,20-1,2]$,可构造出参数为$[n_i+20,n_i+20-\max\{t_i,7\}-4-1,5]=[n+20,n+8,5]$的线性码 C,其中 C 满足 $C^{\perp}\subset C$。同时构造出参数为$[[n+20,n-4,5]]$的量子纠错码。

同理可证2)、3)结论成立。

定理3　1)当 $n=22,23,24,25,27$ 时,存在参数为$[[n+20,n-10,6]]$的量子纠错码;

2)当 $n=26,28,30,32,34,36$ 时,存在参数为$[[n+20,n-8,6]]$的量子纠错码;

3)当 $n=29,31,33,35,40,45$ 时,存在参数为$[[n+20,n-12,6]]$的量子纠错码。

证明　1)根据推论1,当 $n=22,23,24,25,27$ 时,有 L- 链$[n,n-6-4,6]\subset[n,n-6,4]$,利用引理1和 L- 链$[20,20-8-1,6]\subset[20,20-1,2]$,可构造出参数为$[n+20,n+20-\max\{8,4\}-6-1,6]=[n+20,n+5,6]$的线性码 C,其中 C 满足 $C^{\perp}\subset C$。同时可构造出参数为$[[n+20,n-10,6]]$的量子纠错码。

同理可证2)、3)结论成立。

3　结束语

除了由自正交码[21,9,8]和[25,10,10]构造的量子纠错码[[21,3,5]]和[[25,5,6]]没有达到文献[9]中量子纠错码的参数外,其余的码长在 $20\leqslant n\leqslant 30$ 范围内、距离为5或6的量子纠错码均达到或超过了文献[9]中已知量子纠错码的参数;码长在 $31\leqslant n\leqslant 36$ 和 $40\leqslant n\leqslant 64$ 范围内、距离为5或6的量子纠错码都是新的。

参考文献:

[1] Shor P W. Scheme for Reducing Decoherence in Quantum Computermemory[J]. Phys Rev A, 1995, 52: 493-496.

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

[3] Hao Chen. Some Good Quantum Error-correcting Codes From Algebric Geometric Codes[J]. IEEE Trans Inf Theory, 2001, 47: 2059-2061.

[4] Hao Chen, San Ling, Chaoping Xing. Quantum Codes Concatenated From Algebraic Geometric Codes[J]. IEEE Trans Inf Theory, 2005, 51: 2915-2920.

[5] Steane A M. Quantumn Reed-muller codes[J]. IEEE Trans Inf Theory, 1999, 45: 1701-1702.

[6] Thangaraj A, McLaughlin S W. Quantum Codes From Cyclic Codes Over GF(4^m)[J]. IEEE Trans Inf Theory, 2001, 47: 2492-2495.

[7] Ruihu Li, Xueliang Li. Quantum Codes Constructed From Binary Cyclic Codes[J]. Int J Quantum Inf, 2004, 2: 265-272.

[8] Ruihu Li. Research on Additive Quantum Error-Correcting Codes[D]. Xi'an: Northwestern Polytechnical University, 2004.

[9] Calderbank A R, Rains E M, Shor P W. Quantun Error Correction Via Codes Over GF(4)[J]. IEEE Trans Inf Theory, 1998,

44: 1369 - 1387.

[10] Kschischang F R, Pasupathy S. Some Ternary and Quaternary Codes and Associated Sphere Packings[J]. IEEE Trans Inf Theory, 1992, 38: 227 - 246.

(编辑:田新华)

Quaternary Self - orthogonal Code Chains and Construction of Quantum Error - correcting Codes

MA Yue - na, WANG Lei, ZHAO Xue - jun, FENG You - qian
(Science Institute, Air Force Engineering University, Xi'an 710051, China)

Abstract: The method of constructing quantum error - correcting code by the quaternary self - orthogonal sub - code chains and L - chains are investigated in this paper. Random searching method is used to find quaternary self - orthogonal codes and these self - orthogonal codes could form some self - orthogonal code chains. By using combinatorial method, quantum error - correcting codes are constructed in light of L - chains which are constructed by dual of these self - orthogonal codes. The code chains of these self - orthogonal sub - codes and the L - chains which are obtained from the dual of these self - orthogonal sub - codes of length n between 20 and 36 and n = 40, 45, 50, 55, 60 and dual distance five and six are determined. Some quantum codes of distance five and six are constructed by the obtained L - chains, some quantum error - correcting codes are new.

Key words: self - orthogonal code; self - orthogonal code chain; L - chain; quantum error - correcting code

(上接第 49 页)

[10] Zhang X D, Liang Y C. Prefiltering - based ESPRIT for Estimating Parameter of Sinusoids in Non - gaussian Noise[J]. IEEE Trans On Signal Processing, 1995, 43: 349 - 353.

(编辑:田新华,徐楠楠)

Phase Estimation Method of Sinusoidal Signal in Colored Noise

NING Hui[1], SHI Yao - wu[2]
(1. Institute of Aviation Equipment Academy, Beijing 10076, China; 2. College of Communication Engineering, JiLin University, Changchun 130022, Jilin, China)

Abstract: The phase estimation of sinusoidal signal in noise environments is extensively adopted in the field of radar, navigation and DOA estimation, etc. A sinusoidal signal phase estimation method - - - Singular Value Decomposition (SVD), based on cross - high - order cumulant, is proposed. The signal and noise subspace are obtained using SVD of cross - high - order cumulant matrix. The signal subspace is the optimum solution for signal detection and noise suppression. The high - order cumulant matrix of signal is a conjugated symmetric matrix, its left singular vector is identical with the right one, their amplitudes and frequencies are also the same. The cross - high - order cumulant matrix of sinusoidal signals with different phases is a unconjugated symmetric matrix, its left and right singular vector are different because of the phase difference existing among the harmonic signals. A very important theorem is demonstrated in this article, i. e. the phase angle of the left and the right singular vector inner - product of harmonic signal cross - high - order cumulant matrix is equal to the phase difference of sinusoidal signals. Based on this theorem, the method of SVD for phase estimation of sinusoidal signal is deduced. The availability of the method is verified by simulation.

Key words: cross - high - order cumulant; phase estimation; colored noise; SVD