最优二元自正交码

王唯良[1,2]， 樊养余[1]， 寇光兴[2]， 闫 龙[2]
(1. 西北工业大学电子信息学院，陕西西安，710072；2. 空军工程大学理学院，陕西西安，710051)

摘要 构造一般二元自正交码是经典纠错码和量子纠错码研究的难点。研究基于并置二元循环矩阵的1-生成子拟循环码结构。以向量移位等价、线性码等价以及二元自正交码码字偶重量特点等为基础，设计特殊二元拟循环码结构，构造了28个最优或已知最优二元拟循环自正交码。提出自正交码截短-删除方法，构造出所获得自正交码的62个衍生码。文中的90个二元自正交码与文献[13]中最优或已知最优线性码比较，分别有67和23个二元自正交码是最优和已知最优。构造结果验证2个方法对一般二元自正交码构造的有效性，同时能较好解决量子纠错码构造中具有尽可能大对偶重量自正交码的设计问题。

关键词 线性码；自正交码；拟循环码；截短-删除构造
DOI 10.3969/j.issn.1009-3516.2015.01.019
中图分类号 TN911.22，O236.2 **文献标志码** A **文章编号** 1009-3516(2015)01-0085-04

Optimal Binary Self-orthogonal Codes

WANG Wei-liang[1,2]，FAN Yang-yu[1]，KOU Guang-xing[2]，YAN Long[2]
(1. School of Electronics and Information，Northwestern Polytechnical University，Xi′an 710072，China；
2.Science College，Air Force Engineering University，Xi′an 710051，China)

Abstract：Designing general binary self-orthogonal codes is a difficult problem in both classical coding theory and quantum coding theory. The structure of one-generator quasi-cyclic codes constructed by concatenating binary circulant matrices is investigated. Twenty-eight optimal or best known binary self-orthogonal codes are built by designing the structure of a special subclass of quasi-cyclic codes，which takes advantage of some restrictions such as the shifting equivalence relation on vector，the equivalence relation on linear codes and even weight property of binary self-orthogonal codes. A puncturing-expurgating construction method for binary self-orthogonal codes is proposed，and sixty-two derived codes from these obtained self-orthogonal codes are constructed. In comparison with Literature (13)，67 and 23 among our ninety self-orthogonal codes are separately optimal and best known. The construction results indicate that these two methods are effective to design general self-orthogonal codes. Furthermore，the ideas can preferably solve the construction problem of self-orthogonal codes with possible larger minimum dual weight，which is the critical infrastructure in designing better quantum codes.

Key words：linear code；self-orthogonal code；quasi-cyclic code；puncturing-expurgating construction

收稿日期：2014-02-25
基金项目：国家自然科学基金资助项目(11471011)
作者简介：王唯良(1976－)，男，陕西宝鸡人，讲师，博士生，主要从事量子编码，图像处理，数据挖掘等研究.E-mail：wlwangkg@gmail.com

引用格式：*王唯良，樊养余，寇光兴，等．最优二元自正交码[J]．空军工程大学学报：自然科学版，2015，16(1)：85-88. WANG Weiliang，FAN Yangyu，KOU Guangxing，et al.Optimal Binary Self-orthogonal Codes[J]. Journal of Air Force Engineering University：Natural Science Edition，2015，16(1)：85-88.*

作为一类特殊的线性码类,自正交码已成为构造量子纠错码的基础[1-4]。当前自正交码研究的热点之一是构造和分类给定码长和维数的自对偶码[5-6],但就如何构造一般自正交码进展缓慢[7]。设计最优自正交码,不但是经典编码领域的重要研究课题,同时也可以为量子纠错码构造提供结构上的借鉴。

拟循环码是循环码的自然推广,现有的许多参数最优或已知最优线性码是拟循环码[8-9]。拟循环码具有优雅的代数结构[10-11]和较为可行的构造方法[8-9],已成为探索好参数码的重要途径之一。尽管将单一的由已知码构造新码的经典构造法应用于自正交码构造,新码参数不太理想或自正交性可能得不到保证[12],但组合使用经典构造法,仍有望克服自正交码构造面临的这 2 个问题。

本文基于一种特殊的二元拟循环结构和截短-删除法构造二元自正交码,与文献[13]中最优或已知最优线性码比较,分别有 67 和 23 个二元自正交码是最优和已知最优。

1 预备知识

设 $F_2=\{0,1\}$ 为二元域,称 F_2^n 的 k 维子空间 C 是码长为 n 的 k 维二元线性码,记为 $C=[n,k]$。记 $wt(x)$ 为 $x\in F_2^n$ 中非零分量数量,称 $\boldsymbol{d}=\boldsymbol{d}(C)=\min\{wt(c)\mid c\in C,c\neq 0\}$ 为码 $\boldsymbol{C}$ 的最小重量。具有最小重量 $\boldsymbol{d}$ 的 $[n,k]$ 码记为 $\boldsymbol{C}=[n,k,d]$。以码 $\boldsymbol{C}$ 的一组基为行的矩阵 $\boldsymbol{G}$ 称为 $\boldsymbol{C}$ 的生成矩阵。设 $\boldsymbol{G}_1,\boldsymbol{G}_2$ 是线性码 $\boldsymbol{C}_1,\boldsymbol{C}_2$ 的生成矩阵,如果存在置换矩阵 $\boldsymbol{P}$,使得 $\boldsymbol{G}_1=G_2P$,则称 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 置换等价。任意线性码 $\boldsymbol{C}=[n,k]$ 等价于具有生成矩阵 $G=(I_k\mid A_{k\times(n-k)})$ 的系统码。F_2^n 上的 Euclidean 内积为 $(x,y)=\sum_{i=1}^{n}x_iy_i$,式中:$x=(x_1,\cdots,x_n)$;$y=(y_1,\cdots,y_n)\in F_2^n$。称 $[n,n-k]$ 码 $\boldsymbol{C}^{\perp}=\{x\in F_2^n\mid(x,\boldsymbol{C})=0,\boldsymbol{C}\in\boldsymbol{C}\}$ 为码 $\boldsymbol{C}$ 的对偶码。若 $\boldsymbol{C}\subset\boldsymbol{C}^{\perp}$,则称 $\boldsymbol{C}$ 是自正交的;若 $\boldsymbol{C}=\boldsymbol{C}^{\perp}$,则称 $\boldsymbol{C}$ 是自对偶。

定义 1 设最优二元线性码 $\boldsymbol{C}=[n,k,d]$ 和自正交码 $\boldsymbol{C}'=[n,k,d']$,如果 d 为偶数时 $d'=d$,或 d 为奇数时 $d'=d-1$,则称 $\boldsymbol{C}'$ 是最优的。

定义 2 设二元线性码 $\boldsymbol{C}=[n,k,d\sim d_{\text{opt}}]$ 和自正交码 $\boldsymbol{C}'=[n,k,d']$,其中 $\boldsymbol{d}$ 和 d_{opt} 分别为给定码长 n 和维数 k 时码的最小重量已知下界和理论上界。如果 $\boldsymbol{d}$ 为偶数时 $d'=d$,或 $\boldsymbol{d}$ 为奇数时 $d'=d-1$,则称 $\boldsymbol{C}'$ 是已知最优的。

引理 1 若二元线性码 $\boldsymbol{C}=[n,k]$ 是自正交的,则 $k\leqslant\lceil\frac{n-1}{2}\rceil$,且对任意 $c\in C$,$wt(c)$ 为偶数。

2 拟循环二元自正交码

定义 3 设 $\boldsymbol{C}=[n,k]$ 是二元线性码,$\pi_p:F_2^n\to F_2^n$ 为 p 循环移位算子。如果对任意 $\boldsymbol{c}\in\boldsymbol{C}$,有 $\pi_p\boldsymbol{c}\in\boldsymbol{C}$,则称 $\boldsymbol{C}$ 为拟循环码。

定义 4 称矩阵 $\begin{pmatrix}\boldsymbol{g}\\ \pi_1(\boldsymbol{g})\\ \vdots\\ \pi_{k-1}(\boldsymbol{g})\end{pmatrix}$ 为与向量 $\boldsymbol{g}\in F_2^k$ 对应的 F_2 上的循环矩阵,记为 $\langle g\rangle_k$。

令 $\boldsymbol{G}=(I_k,\langle g_1\rangle_k,\cdots,\langle g_{p-1}\rangle_k)$,其中 $\langle g_i\rangle_k$ 为 F_2 上与 $g_i\in F_2^k$,$1\leqslant i\leqslant p-1$ 对应的循环矩阵,则 $\boldsymbol{G}$ 生成特殊拟循环码 $\boldsymbol{C}=[pk,k]$。称向量 $\boldsymbol{g}=(1,g_1,\cdots,g_{p-1})\in F_2^{pk}$ 为拟循环码 $\boldsymbol{C}$ 的生成向量。显然,拟循环码 $\boldsymbol{C}$ 的生成矩阵 $\boldsymbol{G}$ 和生成向量 $\boldsymbol{g}$ 一一对应。此时,这种拟循环码记为 $\boldsymbol{C}=\langle\boldsymbol{g}\rangle=\langle 1,g_1,\cdots,g_{p-1}\rangle$。

直接选择 $g_1,\cdots,g_{p-1}\in F_2^k$ 构造拟循环码 $\boldsymbol{C}=\langle 1,g_1,\cdots,g_{p-1}\rangle$ 面临 2 个困难:①g_i,$1\leqslant i\leqslant p-1$ 数量大,共有 $2^{k(p-1)}$ 种可能。随着 k 和 p 增大,已经超出现有计算能力;②在这些拟循环码中,大量码是等价的。下面围绕这 2 个问题,研究特殊拟循环码 $\boldsymbol{C}=\langle\boldsymbol{g}\rangle=\langle 1,g_1,\cdots,g_{p-1}\rangle$ 生成向量选择和构造策略。

引理 2[8] 设 F_2^k 上二元关系 $\sim$ 为 $g_i\sim g_j$ 当且仅当存在 $l\in Z$,使得 $g_i=\pi_l(g_j)$,则 $\sim$ 是 F_2^k 上等价关系,且 $M_k=|F_2^k/\sim|=\sum_{d\mid k}\sum_{m\mid d}\mu(m)2^{\frac{d}{m}}$,其中 $\mu(\cdot)$ 为默比乌斯函数。当 k 较大时,$M_k\sim 2^k/k$。

定义 F_2^k 上二元关系 $\leqslant$ 为 $g_i\leqslant g_j$ 当且仅当 $D(g_i)\leqslant D(g_j)$,其中 $D(g)$ 为 $g\in F_2^k$ 的十进制表示,则 $\leqslant$ 是 F_2^k 上面的全序关系。令 $\tilde{g}=\operatorname{argmin}\{D(f)\mid f\in[g]\}$,即等价类 $[g]=\{f\in F_2^k\mid f\sim g\}$,$g\in F_2^k$ 中十进制表示最小的代表元素,则 $F_2^k/\sim=\{\tilde{g}_1,\tilde{g}_2,\cdots,\tilde{g}_{M_k}\}$,其中 $\tilde{g}_1,\tilde{g}_2,\cdots,\tilde{g}_{M_k}$ 是不同等价类的十进制表示最小代表元素。

考虑拟循环码

$$\boldsymbol{C}=\langle\tilde{g}\rangle=\langle 1,\tilde{g}_{i_1},\cdots,\tilde{g}_{i_{p-1}}\rangle,\tilde{g}_{i_j}\in F_2^k/\sim,j=1,\cdots,p-1 \tag{1}$$

则式(1)拟循环码生成向量共有 $\boldsymbol{M}_k^{p-1}$ 种可能。对较大的 k 和 p,$\boldsymbol{M}_k^{p-1}\sim\frac{2^{k(p-1)}}{k^{p-1}}\ll 2^{k(p-1)}$。

引理 3 设拟循环码 $\boldsymbol{C}=\langle\tilde{g}\rangle=\langle 1,\tilde{g}_{i_1},\cdots,$

$\tilde{g}_{i_{p-1}}\rangle, \tilde{g}_{i_j} \in F_2^k/\sim, j=1,\cdots,p-1$,则码 $\boldsymbol{C}$ 等价于 $\boldsymbol{C}'=\langle \tilde{g}'\rangle=\langle 1, \tilde{g}_{i'_1},\cdots,\tilde{g}_{i'_{p-1}}\rangle, i'_1,\cdots,i'_{p-1}$ 是 $i_1,\cdots,i_{p-1}$ 的全排列,满足 $D(\tilde{g}_{i'_1})\leqslant\cdots\leqslant D(\tilde{g}_{i'_{p-1}})$。

引理 3 表明:如果考虑生成向量十进制表示全序关系,可以消除构造过程中码的等价重复。根据**引理 1、引理 2 和引理 3**,最优或已知最优拟循环自正交码结构如式(2):

$$\begin{aligned}&\boldsymbol{C}=\langle \tilde{g}\rangle=\langle 1,\tilde{g}_{i_1},\cdots,\tilde{g}_{i_{p-1}}\rangle, \tilde{g}_{i_j}\in F_2^k/\sim, j=1,\cdots,p-1\\ &\text{s.t.}\quad D(\tilde{g}_{i_1})\leqslant\cdots\leqslant D(\tilde{g}_{i_{p-1}}),\\ &1+\sum_{j=1}^{p-1} wt(\tilde{g}_{i_j})\equiv 0 \bmod 2\end{aligned}\tag{2}$$

基于式(2),可由已知二元拟循环码(初始为单位矩阵)构造最优或已知最优拟循环自正交码。维数为 12 的二元拟循环自正交码构造过程见图 1,图中 LBC 和 SOC 分别表示线性码和自正交码。例如,二元拟循环自正交码[84,12,34]经由 2 次并置构造而成。与文献[13]中二元线性码比较,自正交码[60,12,24],[36,12,12]和[24,12,8]达到最优线性码的距离界,因此是最优二元自正交码;文献[13]给出线性码[96,12,40-42],[84,12,35-36]和[48,12,17-18],因此自正交码[96,12,40],[84,12,34]和[48,12,16]是已知最优的。

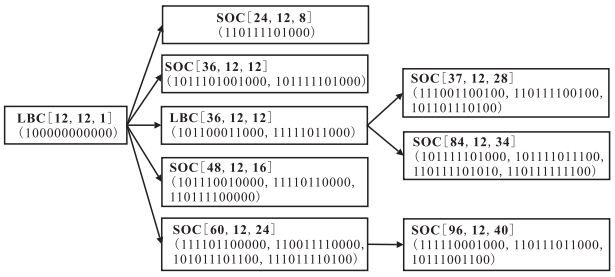

图 1　维数为 12 的二元拟循环自正交码

Fig.1　Binany quasi-cyclic self-orthwgonal codes with dimension 12

定理 1　存在 28 个最优或已知最优二元自正交码。

最优二元自正交码为:[81,9,36],[72,9,32],[63,9,28],[45,9,18];[90,10,40],[50,10,20],[40,10,16],[30,10,10];[77,11,32],[44,11,16],[22,11,6];[60,12,24],[36,12,12],[24,12,8];[39,13,12],[26,13,6];[56,14,20];[45,15,14]。已知最优二元自正交码为:[90,9,40];[60,10,24];[96,12,40],[84,12,34],[48,12,16];[91,13,36],[65,13,24],[52,13,18],[42,14,12];[60,15,20]。

3　自正交码的衍生码

由已知码构造新码的经典线性码构造法可能会破坏自正交码的自正交性,因此许多构造方法,譬如截短法(puncturing method),不能直接用于自正交码构造。但如果结合多种构造法,则有望保持码的自正交性,且新码具有较好参数。基于截短法和删除法(expurgating method),易证**引理 4**。

引理 4　设 $\boldsymbol{G}=(I_k|A_{k\times(n-k)})$ 是二元自正交码 $\boldsymbol{C}=[n,k,d]$ 的生成矩阵,$\boldsymbol{T}=\{i_1,\cdots,i_t\}\subset\{1,\cdots,k\}$,记删除 $\boldsymbol{G}$ 的 (i_j,i_j),$1\leqslant j\leqslant t$ 元素所在的行和列的矩阵为 $\boldsymbol{G}_{\mathrm{T}}$,则 $\boldsymbol{G}_{\mathrm{T}}$ 生成自正交码 $\boldsymbol{C}_T=[n-t,k-t,\geqslant d]$。

例如,考虑拟循环自正交码[56,14,20]。由引理 4 得截短-删除自正交码[56-t,14-t, 20], $1\leqslant t\leqslant 4$。文献[13]给出线性码[55,13,20-21],[54,12,20-22],[53,11,20-22]和[52,10,21-22],易知:[55,13,20]为最优二元自正交码,而[56-t,14-t, 20], $2\leqslant t\leqslant 4$ 为已知最优自正交码。

对表 1 中拟循环自正交码进行截短-删除,可得最优和已知最优自正交码,见表 2。

定理 2　存在如下 62 个最优或已知最优二元自正交码。

表 1　二元拟循环自正交码的截短-删除衍生码

Tab.1　Punctured-expurgated codes from binary quasi-cyclic self-orthogonal caeles

二元自正交码 $[n, k, d]$	性质
[80,8,36], [55,13,20], [49,9,20], [44,8,18]. [90 −t, 10 −t, 40], [63 −t, 9 −t, 28], [45 −t, 15 −t, 14], [30 −t, 10 −t, 10], t =1, 2. [72 −t, 9 −t, 32], [44 −t, 11 −t, 16], $1\leqslant t\leqslant 3$. [60 −t, 12 −t, 24], [36 −t, 12 −t, 12], [22 −t, 11 −t, 6], $1\leqslant t\leqslant 5$. [40 −t, 10 −t, 16], $1\leqslant t\leqslant 6$; [24 −t, 12 −t, 8], $1\leqslant t\leqslant 10$.	最优
[95,11,40], [64,12,24], [59,14,20], [51,12,18], [42,12,14]. [77 −t, 11 −t, 32], t =1, 2; [39 −t,13 −t, 12], $1\leqslant t\leqslant 3$; [56 −t,14 −t, 20], $2\leqslant t\leqslant 4$.	已知最优

4 结论

构造一般的自正交码,是经典纠错码研究的难点之一,也是好参数量子纠错码设计的基础。本文分析一类特殊拟循环码,提出基于二元循环矩阵并置构造的最优自正交码设计结构。通过引入向量移位等价关系和拟循环码生成向量的全序关系,减小拟循环码生成向量空间的规模;充分考虑二元自正交码码字偶重量特点,尽最大可能减少码重量参数计算次数。这两点保证了拟循环自正交码构造算法的高效性。提出针对自正交码构造的截短-删除法,以所获得的 28 个二元自正交拟循环码为基础,构造了 62 个自正交衍生码。这 90 个自正交码是最优或已知最优的。文中提出的这 2 种构造法,较好解决了一般自正交码,特别是长码长自正交码构造问题。特别地,文中思想和方法,可以用于设计对偶距离尽可能大的自正交码,对构造好参数量子纠错码具有重要的利用价值。

参考文献(References):

[1] Shor P W. Scheme for Reducing Decoherence in Quantum Computer Memory[J].Phys Rev A,1995,52:2493-2496.

[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,1996,54:1098-1105.

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

[5] Bouyuklieva S,Harada M,Munemasa A. Determination of Weight Enumerators of Binary Extremal Self-Dual [42; 21; 8] codes[J]. Finite Fields and Their Applications, 2008,14(1): 177-187.

[6] Bouyuklieva S,Yankov N,Kim J L.Classification of Binary Self-Dual [48; 24; 10] Codes with An Automorphism of Odd Prime Order[J]. Finite Fields and Their Applications, 2012,18(6): 1104-1113.

[7] O'Brien E A. Willems W. On the Automorphism Group of A Binary Self-Dual Doubly-Even [72; 36; 16] code[J]. IEEE Trans Inform Theory, 2011,57(7): 4445 - 4451.

[8] Gulliver T A,Bhargava V K. Some Best Rate 1/p and Rate (p -1)/p Systematic Quasi-Cyclic Codes[J]. IEEE Trans Inform Theory, 1991, 37(3): 552-555.

[9] Chen E Z. New Quasi-Cyclic Codes from Simplex Codes[J]. IEEE Trans Inform Theory, 2007, 53(3): 1193-1196.

[10] Conan J,Séguin S. Structural Properties and Enumeration of Quasi Cyclic Codes[J]. Applicable Algebra in Engineering, Communication and Computing, 1993, 4(1): 25-39.

[11] Lally K, Fitzpatrick P. Algebraic Structure of Quasi-cyclic Codes [J]. Discrete Applied Mathematics, 2001, 111(1-2): 157-175.

[12] La Guardia G G. Asymmetric Quantum Codes: New Codes from Old[J]. Quantum Information Processing, 2013(12): 2771-2790.

[13] Grassl M. Code Tables:Bounds on the Parameters of Various Types of Codes[EB/OL].(2008-10-06)[2014-02-02]http://www.codetables.de/.

(编辑:姚树峰)