基于自对偶码的S-链构造

赵全习[1,2]， 郭罗斌[3]， 贺筱军[3] ，秋党庆[4]
(1. 空军工程大学 电讯工程学院，陕西 西安 710077;2. 空军工程大学 导弹学院，陕西 三原 713800;3. 空军工程大学 理学院，陕西 西安 710051;4. 空军司令部，北京 100843)

摘 要:研究具有某种最优性质的码的存在性、结构和构造是编码研究的中心问题,为构造量子纠错码开始研究具有特定对偶距离的二元自正交码。研究了码长 n 满足 $12\leqslant n\leqslant 20$ 的二元不可分解自对偶码 B_{12}、D_{14}、E_{16}、F_{16}、H_{18}、I_{18}、J_{20}、K_{20}、L_{20}、M_{20}和 S_{20}的两类子码,即对偶距离最优或对偶距离拟最优的子码,以及相应的S-链的构造。依据不可分解自对偶码的生成矩阵,利用组合方法构造出对偶距离为2、3和4的对偶距离最优或拟最优的子码生成矩阵。在此基础上研究了这些子码构成的子码链,以及由它们的对偶构成的S-链。最后,利用得到的S-链构造出好的量子纠错码,这些量子码都是给定码长和维数时距离达到最大值的量子码。

关键词:自正交码;码链;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)03-0071-05

研究具有某种最优性质的码的存在性、结构和构造是编码研究的中心问题。近年来,人们为构造量子纠错码开始研究具有特定对偶距离的二元SO码[1-3]。1999年,Steane确立了构造量子纠错码的Steane构造法[4],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。李瑞虎将满足Steane构造法的两个二元自正交码的对偶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,将构造量子纠错码的问题转化为构造S-链[5];他和李学良[6]研究了 $n\geqslant 12$ 且 $t\leqslant\lceil\log_2(n+18)\rceil+1$ 时参数为 $[n,n-t,4]\subset[n,n-1,2]$ 的S-链的构造,并用所得到的S-链构造出距离为3和4的量子纠错码。

要构造某些参数的S-链,首先要解决这样的问题:对于给定的码长 N 和极小距离 D ,是否存在SO码 $C=[n,k]$,使得其对偶距离为 d ? 如果 $d_1>d_2$, C_1 是对偶距离为 d_1 的二元SO码, C_1 是否有对偶距离为 d_2 的子码 C_2? 本文对码长 n 满足 $12\leqslant n\leqslant 20$ 的二元自对偶码的情况进行了研究。

1 概念和定理

设 $F_2=\{0,1\}$ 为二元域, F_2^n 为 F_2 上 n 维行线性空间, 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 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$, $\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)\in F_2^n$, $\boldsymbol{X}\cdot\boldsymbol{Y}=x_1y_1+x_2y_2+\cdots+x_ny_n=\boldsymbol{X}\boldsymbol{Y}^{\mathrm{T}}$称为 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的欧氏(Euclid)内积;若 $\boldsymbol{X}\cdot\boldsymbol{Y}=0$,称 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 正交。$C^{\perp}=\{\boldsymbol{X}:\boldsymbol{X}\cdot\boldsymbol{Y}=\}$,对任意的 $\boldsymbol{Y}\in C$ 叫 C 的对偶码。若 $C=[n,k]$,则 $C^{\perp}$ 为 $[n,n-k]$ 线性码。

若 $C\subseteq C^{\perp}$,称 C 为自正交码,简记为SO码;若自正交码 $C=C^{\perp}$,则称 C 为自对偶码。若不存在SO码 C' 真包含SO码 C ,则称 C 为极大SO码。当码长 n 为偶数时,极大SO码为自对偶码;当码长 n 为奇数时,极大SO码为 $[n,\frac{n-1}{2}]$ SO码。

收稿日期:2007-03-06
基金项目:国家自然科学基金资助项目(60573040)
作者简介:赵全习(1965-),男,陕西凤翔人,副教授,博士生,主要从事代数编码及密码研究.
E-mail:zhaoqx@163.com

定理 1(Steane 构造法) 设 C 和 C' 分别是参数为 $[n,k,d]$ 和 $[n,k_1,d_1]$ 的二元码。如果 $C^{\perp}\subset C\subset C'$，且 $k_1\geqslant k+2$，则可构造出参数为 $[[n,k+k_1-n,\min\{d,\lceil\frac{3}{2}d_1\rceil\}]]$ 的量子码[4]。

满足 Steane 构法条件的两个二元码 C 和 C' 具有特征 $C^{\perp}\subset C\subset C'$。将这两个二元码提取出来并推广到二元码的序列上，就是文献[5]引入的 S－链的概念。

定义 1 设 $C_i=[n_i,k_i,d_i]$ 为二元码[5]，$1\leqslant i\leqslant m$。

1)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 S－ 链。

2)若 $k_i\geqslant k_{i+1}+2$，则称(1)中的 S－链为严格 S－链。

定义 2 设自正交码 $C=[n,k]$，$C^{\perp}=[n,n-k,d]$。

1)如果不存在自正交码 $C'=[n,k]$，使得 $C'^{\perp}=[n,n-k>d]$，则称 C 为对偶距离最优 SO 码，简称为 dd 最优 SO 码；如果不存在 SO 码 $C'=[n,k]$，使得 $C'^{\perp}=[n,n-k,d+2]$，则称 C 为对偶距离拟最优 SO 码，简称为 dd 拟最优 SO 码。

2) 如果不存在 SO 码 $C'=[n,k-1]$，使得 $C'^{\perp}=[n,n-k+1,d]$，则称 C 为对偶距离确定时维数最优 SO 码；如果不存在 SO 码 $C'=[n,k-2]$，使得 $C'^{\perp}=[n,n-k+2,d]$，则称 C 为对偶距离确定时维数拟最优 SO 码。

2 自对偶码与 S－链的构造

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，由文献[7]和[8]可知，当 n 为偶数时，每个自正交码必是某个自对偶码的子码；文献[8]给出 $n\leqslant 20$ 时自对偶码的完全分类与记数以及不可分解自对偶码(indecompose self－dual code)的生成矩阵。由文献[8]可知，自对偶码中性质好的是不可分解自对偶码，且 $n\leqslant 12$ 时，自对偶码的子码的结构和性质是平凡的。因此，本文以下仅研究码长 n 满足 $12\leqslant n\leqslant 20$ 的不可分解自对偶码的对偶距离最优和对偶距离拟最优的子码，以及相应的 S－链的构造。

由文献[8]可知，$12\leqslant n\leqslant 20$ 时，不可分解自对偶码共有 12 个，分别为 $B_{12},D_{14},E_{16},F_{16},H_{18},I_{18},J_{20},K_{20},L_{20},M_{20}$ 和 S_{20}。为节省篇幅，将码的生成矩阵中的行向量 $\boldsymbol{x}$ 用 $(\boldsymbol{x}^{\mathrm{T}})^{\mathrm{T}}$ 表示，并将上述这 12 个自对偶码的生成矩阵分别记为

$\boldsymbol{G}_{D_{12}}=(\boldsymbol{a}_1^{\mathrm{T}},\boldsymbol{a}_2^{\mathrm{T}},\boldsymbol{a}_3^{\mathrm{T}},\boldsymbol{a}_4^{\mathrm{T}},\boldsymbol{a}_5^{\mathrm{T}},\boldsymbol{a}_6^{\mathrm{T}},)^{\mathrm{T}}$，$\boldsymbol{G}_{D_{14}}=(\boldsymbol{b}_1^{\mathrm{T}},\boldsymbol{b}_2^{\mathrm{T}},\boldsymbol{b}_3^{\mathrm{T}},\boldsymbol{b}_4^{\mathrm{T}},\boldsymbol{b}_5^{\mathrm{T}},\boldsymbol{b}_6^{\mathrm{T}},\boldsymbol{b}_7^{\mathrm{T}})^{\mathrm{T}}$；

$\boldsymbol{G}_{E_{16}}=(\boldsymbol{e}_1^{\mathrm{T}},\boldsymbol{e}_2^{\mathrm{T}},\boldsymbol{e}_3^{\mathrm{T}},\boldsymbol{e}_4^{\mathrm{T}},\boldsymbol{e}_5^{\mathrm{T}},\boldsymbol{e}_6^{\mathrm{T}},\boldsymbol{e}_7^{\mathrm{T}},\boldsymbol{e}_8^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{G}_{F_{16}}=(\boldsymbol{f}_1^{\mathrm{T}},\boldsymbol{f}_2^{\mathrm{T}},\boldsymbol{f}_3^{\mathrm{T}},\boldsymbol{f}_4^{\mathrm{T}},\boldsymbol{f}_5^{\mathrm{T}},\boldsymbol{f}_6^{\mathrm{T}},\boldsymbol{f}_7^{\mathrm{T}},\boldsymbol{f}_8^{\mathrm{T}})^{\mathrm{T}}$；

$\boldsymbol{G}_{H_{18}}=(\boldsymbol{h}_1^{\mathrm{T}},\boldsymbol{h}_2^{\mathrm{T}},\boldsymbol{h}_3^{\mathrm{T}},\boldsymbol{h}_4^{\mathrm{T}},\boldsymbol{h}_5^{\mathrm{T}},\boldsymbol{h}_6^{\mathrm{T}},\boldsymbol{h}_7^{\mathrm{T}},\boldsymbol{h}_8^{\mathrm{T}},\boldsymbol{h}_9^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{G}_{I_{18}}=(\boldsymbol{i}_1^{\mathrm{T}},\boldsymbol{i}_2^{\mathrm{T}},\boldsymbol{i}_3^{\mathrm{T}},\boldsymbol{i}_4^{\mathrm{T}},\boldsymbol{i}_5^{\mathrm{T}},\boldsymbol{i}_6^{\mathrm{T}},\boldsymbol{i}_7^{\mathrm{T}},\boldsymbol{i}_8^{\mathrm{T}},\boldsymbol{i}_9^{\mathrm{T}})^{\mathrm{T}}$；

$\boldsymbol{G}_{J_{20}}=(\boldsymbol{j}_1^{\mathrm{T}},\boldsymbol{j}_2^{\mathrm{T}},\boldsymbol{j}_3^{\mathrm{T}},\boldsymbol{j}_4^{\mathrm{T}},\boldsymbol{j}_5^{\mathrm{T}},\boldsymbol{j}_6^{\mathrm{T}},\boldsymbol{j}_7^{\mathrm{T}},\boldsymbol{j}_8^{\mathrm{T}},\boldsymbol{j}_9^{\mathrm{T}},\boldsymbol{j}_{10}^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{G}_{K_{20}}=(\boldsymbol{k}_1^{\mathrm{T}},\boldsymbol{k}_2^{\mathrm{T}},\boldsymbol{k}_3^{\mathrm{T}},\boldsymbol{k}_4^{\mathrm{T}},\boldsymbol{k}_5^{\mathrm{T}},\boldsymbol{k}_6^{\mathrm{T}},\boldsymbol{k}_7^{\mathrm{T}},\boldsymbol{k}_8^{\mathrm{T}},\boldsymbol{k}_9^{\mathrm{T}},\boldsymbol{k}_{10}^{\mathrm{T}})^{\mathrm{T}}$；

$\boldsymbol{G}_{L_{20}}=(\boldsymbol{l}_1^{\mathrm{T}},\boldsymbol{l}_2^{\mathrm{T}},\boldsymbol{l}_3^{\mathrm{T}},\boldsymbol{l}_4^{\mathrm{T}},\boldsymbol{l}_5^{\mathrm{T}},\boldsymbol{l}_6^{\mathrm{T}},\boldsymbol{l}_7^{\mathrm{T}},\boldsymbol{l}_8^{\mathrm{T}},\boldsymbol{l}_9^{\mathrm{T}},\boldsymbol{l}_{10}^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{G}_{M_{20}}=(\boldsymbol{m}_1^{\mathrm{T}},\boldsymbol{m}_2^{\mathrm{T}},\boldsymbol{m}_3^{\mathrm{T}},\boldsymbol{m}_4^{\mathrm{T}},\boldsymbol{m}_5^{\mathrm{T}},\boldsymbol{m}_6^{\mathrm{T}},\boldsymbol{m}_7^{\mathrm{T}},\boldsymbol{m}_8^{\mathrm{T}},\boldsymbol{m}_9^{\mathrm{T}},\boldsymbol{m}_{10}^{\mathrm{T}})^{\mathrm{T}}$；

$\boldsymbol{G}_{R_{20}}=(\boldsymbol{r}_1^{\mathrm{T}},\boldsymbol{r}_2^{\mathrm{T}},\boldsymbol{r}_3^{\mathrm{T}},\boldsymbol{r}_4^{\mathrm{T}},\boldsymbol{r}_5^{\mathrm{T}},\boldsymbol{r}_6^{\mathrm{T}},\boldsymbol{r}_7^{\mathrm{T}},\boldsymbol{r}_8^{\mathrm{T}},\boldsymbol{r}_9^{\mathrm{T}},\boldsymbol{r}_{10}^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{G}_{S_{20}}=(\boldsymbol{s}_1^{\mathrm{T}},\boldsymbol{s}_2^{\mathrm{T}},\boldsymbol{s}_3^{\mathrm{T}},\boldsymbol{s}_4^{\mathrm{T}},\boldsymbol{s}_5^{\mathrm{T}},\boldsymbol{s}_6^{\mathrm{T}},\boldsymbol{s}_7^{\mathrm{T}},\boldsymbol{s}_8^{\mathrm{T}},\boldsymbol{s}_9^{\mathrm{T}},\boldsymbol{s}_{10}^{\mathrm{T}})^{\mathrm{T}}$。

引理 1 ①不存在[14,5]SO 码 C[9]，使 $d(C^{\perp})=3$；②不存在[14,6]SO 码 D，使 $d(D^{\perp})=4$。

推论 1 不存在参数为[18,5]的自正交码 C，使 $d(C^{\perp})=3$。

证明 设 C 是[18,5] 的自正交码 C 且 $d(C^{\perp})=3$。令 C 的生成矩阵为 $\boldsymbol{G}$，$\boldsymbol{G}$ 的列为 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_{18}$，则 $\boldsymbol{\alpha}_i$ 互不相同且任一 $\boldsymbol{\alpha}_i$ 不为零，从 31 个 5 维非零列向量中删除 $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_{18}$，余下的 13 列构成的矩阵记为 $\boldsymbol{G}_1$，则 $\boldsymbol{G}_1\boldsymbol{G}_1^{\mathrm{T}}=0$，从而 $\boldsymbol{G}_1$ 生成[13,5] 自正交码 C_1 且 $d(C_1^{\perp})=3$。于是 $\boldsymbol{C}_1$ 的扩展码为[14,6] 的自正交码且其对偶距离为 4。矛盾。

引理 2 设 C 是参数为[20,5] 的自正交码且对偶距离为 3，则 C 不包含对偶距离为 2 的 2 维子码[9-10]。

证明 设 C_1 为 C 的 2 维子码，$\boldsymbol{X}_1,\boldsymbol{X}_2$ 为 C_1 的一组基，且 $\omega(\boldsymbol{X}_1)\geqslant\omega(\boldsymbol{X}_2)$。将 $\boldsymbol{X}_1,\boldsymbol{X}_2$ 扩充成 C 的一组基 $\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_5$，则可设 C 的生成矩阵 $\boldsymbol{G}=(\boldsymbol{X}_1^{\mathrm{T}},\boldsymbol{X}_2^{\mathrm{T}},\cdots,\boldsymbol{X}_5^{\mathrm{T}})^{\mathrm{T}}=(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_{20})$，其中 $\boldsymbol{\alpha}_i$ 是 $\boldsymbol{G}$ 的第 i 列。

将 31 个 5 维非零列向量排成如下形式的矩阵

$$\boldsymbol{H}=(\boldsymbol{G}|\boldsymbol{G}_1)=(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_{20}|\boldsymbol{\alpha}_{21},\cdots,\boldsymbol{\alpha}_{31})$$

则 $\boldsymbol{H}$ 是[31,26,3] Hamming 码的校验阵，于是 $\boldsymbol{G}_1$ 生成的码 $C_2=[11,5]$ 自正交且对偶距离为 3，故 C_2 与

$\overline{D}_{11}$等价。由于$\boldsymbol{H}$中每行重量为16，$\boldsymbol{G}_1$中每行重量大于等于4,故$\boldsymbol{G}$中每行重量为小于等于12。

又因为$\boldsymbol{H}$中任意两行之和重量为16，$\boldsymbol{G}_1$中任两行重量之和至少为4,故$\omega(\boldsymbol{X}_1+\boldsymbol{X}_2)\leqslant 12$。由关系式$\omega(\boldsymbol{X}_1+\boldsymbol{X}_2)=\omega(\boldsymbol{X}_1)+\omega(\boldsymbol{X}_2)-2\omega(\boldsymbol{X}_1*\boldsymbol{X}_2)$可得$\omega(\boldsymbol{X}_1*\boldsymbol{X}_2)\geqslant\omega(\boldsymbol{X}_1)+\omega(\boldsymbol{X}_2)-12$。

1)若$\omega(\boldsymbol{X}_1)=\omega(\boldsymbol{X}_2)=12$,由$\boldsymbol{X}_1$与$\boldsymbol{X}_2$正交可知，$\omega(\boldsymbol{X}_1*\boldsymbol{X}_2)\geqslant 6$,此时$\boldsymbol{X}_1$与$\boldsymbol{X}_2$至少有2个分量同时取0,故此时$d(C_1^{\perp})=1$。

2)若$\omega(\boldsymbol{X}_1)=12,\omega(\boldsymbol{X}_2)=10$,由$\boldsymbol{X}_1$与$\boldsymbol{X}_2$正交可知，$\omega(\boldsymbol{X}_1*\boldsymbol{X}_2)\geqslant 6$,从而$\boldsymbol{X}_1$与$\boldsymbol{X}_2$至少有4个分量同时取0,故此时$d(C_1^{\perp})=1$。

3)若$\omega(\boldsymbol{X}_1)=12,\omega(\boldsymbol{X}_2)=8$,仿1)可证$\boldsymbol{X}_1$与$\boldsymbol{X}_2$至少有4个分量同时取0,故此时$d(C_1^{\perp})=1$。

4)若$\omega(\boldsymbol{X}_1)=\omega(\boldsymbol{X}_2)=10$,则$\omega(\boldsymbol{X}_1*\boldsymbol{X}_2)\geqslant 4$，$\boldsymbol{X}_1$与$\boldsymbol{X}_2$至少有4个分量同时取0,故此时$d(C_1^{\perp})=1$。

其它情况下$\omega(\boldsymbol{X}_1)+\omega(\boldsymbol{X}_2)\leqslant 20$,自然有$d(C_1^{\perp})=1$。

定理2　设n为偶数,$12\leqslant n\leqslant 20$。则①存在参数分别为[12,5],[14,6],[18,6],[20,5]的对偶距离为3的dd最优SO码和[16,5]对偶距离为3的dd拟最优SO码;②存在参数分别为[12,6],[14,7],[16,5],[18,7],[20,6]的对偶距离为4的dd最优SO码。

证明　对$12\leqslant n\leqslant 20$每个$n$,从码长为$n$的自对偶码的子码出发,构造出一个对偶距离为3的dd最优SO码或dd拟最优SO码($n=16$)的生成矩阵,这些生成矩阵的前2行生成一个对偶距离为2的2维子码($n=20$除外,此时[20,5]码的前3行生成一个对偶距离为2的3维子码)，从而①成立。

在对偶距离为3的dd最优SO码的生成矩阵中增加全1向量,则可得到对偶距离为4的dd最优SO码的生成矩阵;当$n=16$时,构造出$\boldsymbol{G}^*_{E_{16,5}},\boldsymbol{G}^*_{\tilde{E}_{16,5}}$它们生成对偶距离为4的自正交码,从而②成立。

$$\boldsymbol{G}_{B_{12,5}}=\begin{bmatrix}111111110000\\111100001111\\001111000000\\010101010101\\000000110011\end{bmatrix}=\begin{bmatrix}\boldsymbol{a}_1+\boldsymbol{a}_3\\\boldsymbol{a}_1+\boldsymbol{a}_5\\\boldsymbol{a}_2\\\boldsymbol{a}_6\\\boldsymbol{a}_4+\boldsymbol{a}_5\end{bmatrix}\qquad \boldsymbol{G}_{D_{14,6}}=\begin{bmatrix}110000111111111\\001111011110000\\101010100000000\\111100000000000\\000000000111110\\000000001011011\end{bmatrix}=\begin{bmatrix}\boldsymbol{b}_2+\boldsymbol{b}_7\\\boldsymbol{b}_2+\boldsymbol{b}_4\\\boldsymbol{b}_3\\\boldsymbol{b}_1\\\boldsymbol{b}_5\\\boldsymbol{b}_4+\boldsymbol{b}_6\end{bmatrix}$$

$$\boldsymbol{G}_{E_{16,5}}=\begin{bmatrix}1111000000001111\\0000111111111111\\0011110000111100\\0101010101010101\\0000000011110000\end{bmatrix}=\begin{bmatrix}\boldsymbol{e}_1+\boldsymbol{e}_7\\\boldsymbol{e}_3+\boldsymbol{e}_5+\boldsymbol{e}_7\\\boldsymbol{e}_2+\boldsymbol{e}_6\\\boldsymbol{e}_8\\\boldsymbol{e}_5\end{bmatrix}\qquad \boldsymbol{G}_{E_{16,5}}=\begin{bmatrix}1100110011110000\\1111111100001111\\1111000000111100\\0000111100111100\\0110101010101001\end{bmatrix}=\begin{bmatrix}\boldsymbol{f}_1+\boldsymbol{f}_2+\boldsymbol{f}_4\\\boldsymbol{f}_1+\boldsymbol{f}_3+\boldsymbol{f}_6\\\boldsymbol{f}_1+\boldsymbol{f}_5\\\boldsymbol{f}_3+\boldsymbol{f}_5\\\boldsymbol{f}_7+\boldsymbol{f}_8\end{bmatrix}$$

$$\boldsymbol{G}_{H_{18,6}}=\begin{bmatrix}1111001111001111100\\001111001111001111\\000000001111111100\\111100000000001111\\101010101010000000\\000000010101010101\end{bmatrix}=\begin{bmatrix}\boldsymbol{h}_1+\boldsymbol{h}_3+\boldsymbol{h}_5\\\boldsymbol{h}_2+\boldsymbol{h}_4+\boldsymbol{h}_6\\\boldsymbol{h}_4+\boldsymbol{h}_5\\\boldsymbol{h}_1+\boldsymbol{h}_6\\\boldsymbol{h}_7\\\boldsymbol{h}_8\end{bmatrix}\qquad \boldsymbol{G}_{J_{20,5}}=\begin{bmatrix}00001111000000001111\\11110000000011111111\\00111100111100111100\\00000011110011110000\\10101010010110101010\end{bmatrix}=\begin{bmatrix}\boldsymbol{j}_3+\boldsymbol{j}_9\\\boldsymbol{j}_1+\boldsymbol{j}_7+\boldsymbol{j}_9\\\boldsymbol{j}_2+\boldsymbol{j}_5+\boldsymbol{j}_8\\\boldsymbol{j}_4+\boldsymbol{j}_7\\\boldsymbol{j}_5+\boldsymbol{j}_{10}\end{bmatrix}$$

$$\boldsymbol{G}^*_{E_{16,5}}=\begin{bmatrix}1111111111111111\\0101010101010101\\0011110000111100\\0000111100001111\\0000000011111111\end{bmatrix}=\begin{bmatrix}\boldsymbol{e}_1+\boldsymbol{e}_3+\boldsymbol{e}_5+\boldsymbol{e}_7\\\boldsymbol{e}_8\\\boldsymbol{e}_2+\boldsymbol{e}_6\\\boldsymbol{e}_3+\boldsymbol{e}_7\\\boldsymbol{e}_5+\boldsymbol{e}_7\end{bmatrix}\qquad \boldsymbol{G}^*_{F_{16,5}}=\begin{bmatrix}1111111111111111\\0101010101010101\\0011110000111100\\0000111100001111\\0000000011111111\end{bmatrix}=\begin{bmatrix}\boldsymbol{f}_1+\boldsymbol{f}_3+\boldsymbol{f}_4+\boldsymbol{f}_6\\\boldsymbol{f}_7+\boldsymbol{f}_8\\\boldsymbol{f}_2+\boldsymbol{f}_5\\\boldsymbol{f}_3+\boldsymbol{f}_6\\\boldsymbol{f}_4+\boldsymbol{f}_6\end{bmatrix}$$

注:上述对偶距离为4的[16,5]的任一个子码的对偶距离为1或2,不能由对偶距离为3的[16,4]码的生成矩阵中增加全1向量得到,故在给出dd拟最优SO码的生成矩阵$\boldsymbol{G}_{E_{16,5}}$和$\boldsymbol{G}_{F_{16,5}}$的同时,给出了dd最优SO码的生成矩阵$\boldsymbol{G}^*_{E_{16,5}}$和$\boldsymbol{G}_{E_{16,5}}$。

定理3 1) 存在由 B_{12} 的子码的对偶码构成的 S－链：

$[12,6,4]\subset[12,7,2]\subset\cdots\subset[12,11,2]$；

$[12,6,4]\subset[12,7,3]\subset[12,8,2]\subset\cdots\subset[12,10,2]$。

2) 存在由 D_{14} 的子码的对偶码构成的 S－链：

$[14,7,4]\subset[14,8,2]\subset[14,9,2]\subset\cdots\subset[14,13,2]$；

$[14,7,4]\subset[14,8,3]\subset[14,9,2]\subset\cdots\subset[14,12,2]$。

3) 存在由 E_{16} 和 F_{16} 的子码的对偶码构成的 S－链：

$[16,8,4]\subset\cdots\subset[16,11,4]\subset[16,12,2]\subset\cdots\subset[16,15,2]$；

$[16,8,4]\subset\cdots\subset[16,10,4]\subset[16,11,3]\subset[16,12,2]\cdots\subset[16,14,2]$。

4) 存在由 H_{18} 和 I_{18} 的子码的对偶码构成的 S－链：

$[18,9,4]\subset\cdots\subset[18,11,4]\subset[18,12,2]\subset\cdots\subset[18,17,2]$；

$[18,9,4]\subset\cdots\subset[18,11,4]\subset[18,12,3]\subset\cdots\subset[18,16,2]$。

5) 存在由 J_{20}、K_{20}、L_{20}、M_{20}、R_{20} 和 S_{20} 的子码的对偶码构成的 S－链：

$[20,10,4]\subset\cdots\subset[20,14,4]\subset[20,15,2]\subset[20,16,2]\subset[20,19,2]$；

$[20,10,4]\subset\cdots\subset[20,14,4]\subset[20,15,3]\subset[20,16,2]\subset[20,17,2]$。

证明 对每个 $12\leqslant n\leqslant 20$，我们构造出一个对偶距离为 3 的最优 SO 码或拟最优 SO 码，以及一个包含全 1 向量且对偶距离为 4 的最优 SO 码，其中 B_{12}、D_{14}、H_{18}、J_{20} 的对偶距离为 3 的 dd 最优子码及 E_{16}、F_{16} 的对偶距离为 3 的 dd 拟最优子码的生成阵见定理 2 的证明，其它自对偶码的对偶距离为 3 的最优子码的生成矩阵见下文。

对定理中这 12 个自对偶码 $[n,n/2]$，令包含全 1 向量的对偶距离为 4 的 dd 最优子码为 $[n,k_1]$，则由自正交码链 $\langle 1_n\rangle\subset\cdots\subset[n,k_1]\subset\cdots\subset[n,n/2]$ 的对偶码得到定理中每种情况下的第 1 个 S－链。

对定理中的 12 个自对偶码 $[n,n/2]$，令所构造的对偶距离为 3 的最优或拟最优 SO 码为 $[n,k_2]$，其前 2 行生成的子码记为 $[n,2]$（$n=20$ 时取其前 3 行生成的子码），则当 $12\leqslant n\leqslant 18$ 时，由自正交码链 $[n,2]\subset\cdots\subset[n,k_2]\subset\cdots\subset[n,n/2]$ 的对偶可得定理中每种情况下的第 2 个 S－ 链。

当 $n=20$ 时，由自正交码链 $[n,3]\subset\cdots\subset[n,k_2]\subset\cdots\subset[n,n/2]$ 的对偶可得到相应的第 2 个 S－链。

$$G_{I_{20,6}}=\begin{bmatrix}1111111111110000111\\00000001111111111\\10101010101000000\\00000111101010101\\10010101011000000\\00001111000110011 0\end{bmatrix}=\begin{bmatrix}i_6+i_9\\i_1+i_3+i_9\\i_5\\i_4+i_8\\i_2+i_4+i_5\\i_3+i_6+i_7\end{bmatrix}\qquad G_{K_{20,5}}=\begin{bmatrix}01010101101011000000\\11110000111100001111\\10101010101011111100\\00111100001110101010\\00000000000011111111\end{bmatrix}=\begin{bmatrix}k_1+k_3+k_9\\k_1+k_5+k_8\\k_7+k_9\\k_2+k_{10}\\k_6+k_8\end{bmatrix}$$

$$G_{L_{20,5}}=\begin{bmatrix}10101010000000110011\\01010100101010111111\\00111101010101001111\\00000001100110001111\\10100101111000101010\end{bmatrix}=\begin{bmatrix}l_3+l_7+l_8\\l_8+l_9\\l_2+l_6+l_8\\l_4+l_5+l_8\\l_1+l_4+l_{10}\end{bmatrix}\qquad G_{M_{20,5}}=\begin{bmatrix}00000000000011111111\\11110011101001011100\\00001111111111110000\\11000000111101100110\\01011010001111110011\end{bmatrix}=\begin{bmatrix}m_4+m_5\\m_1+m_6+m_{10}\\m_2+m_3+m_4\\m_3+m_7\\m_4+m_8+m_9\end{bmatrix}$$

$$G_{R_{20,5}}=\begin{bmatrix}11111100010101101001\\11000011000011111111\\11010110101010000000\\11000000010101010101\\01110000001111100110\end{bmatrix}=\begin{bmatrix}r_1+r_5+r_9\\r_5+r_{10}\\r_1+r_8\\r_9\\r_1+r_4+r_7\end{bmatrix}\qquad G_{S_{20,5}}=\begin{bmatrix}11001111101010101100\\00111100111111110000\\00000000001111001111\\10101010110000000011\\11000000111001111010\end{bmatrix}=\begin{bmatrix}s_3+s_9\\s_2+s_4+s_6\\s_5+s_7\\s_7+s_8\\s_5+s_6+s_{10}\end{bmatrix}$$

3 量子码的构造

利用定理3 中构造的严格 S－链 $[12,7,3]\subset[12,10,2]$、$[14,8,3]\subset[14,12,2]$、$[16,11,3]\subset[16,14,$

2]、[18,12,3]⊂[18,16,2]以及[20,15,3]⊂[20,17,2]可构造出量子码[[12,5,3]]、[[14,6,3]]、[[16,9,3]]、[[18,10,3]]和[[20,12,3]]。这些量子码都是给定n,k时距离达到最大值的量子码,并且[[12,5,3]]、[[14,6,3]]、[[18,10,3]]与文献[6]利用$[n,n-t,4]\subset[n,n-1,2]$形式的S-链所构造的量子码的参数一样。

4　结束语

本文用组合方法研究了码长n满足$12\leqslant n\leqslant 20$的二元自对偶码的对偶距离最优或对偶距离拟最优的子码,确定了包含这些最优或拟最优子码的对偶码的S-链,并构造出了一些好的量子码。

参考文献:

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

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

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

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

[5] 李瑞虎. 加性量子纠错码研究[D]. 西安:西北工业大学,2004.
LI Ruihu. Research on Additive Quantum Codes[D]. Xi'an:Northwestern Polytechnical University,2004. (in Chinese)

[6] Ruihu Li,Xueliang Li, Binary Construction of Quantum Codes of Minimum Distance Three and Four[J]. IEEE Trans Inf Theory,2004,50:1331-1365.

[7] MacWilliams F J,Sloane N J A. The Theory of Error-Correcting Codes[M]. Amsterdam:The Netherlands North-Holland Press,1977.

[8] Pless V. A Classification of Self-Orthogonal Codes Over GF(2)[J]. Discrete Math,1972,3:209-246.

[9] Stefka BouyukLieva. Some Optimal Self-Rthogonal and Self-dual Codes[J]. Discrete Math,2004,18(3):1-10.

[10] Iliya Bouklliеve Patric R. J. Classificaion of Self-Orthogonal Codes. over GF(3)[J]. Discrete Math,2005,19(2):363-370.

(编辑:田新华)

Construction of S-chains From Self-dual Codes

ZHAO Quan-xi[1,2], GUO Luo-bin[3], HE Xiao-jun[3], QIU Dang-qing[4]

(1. Communication Engineering Institute, Air Force Engineering University, Xi'an 710051, China; 2. Missile Institute, Air Force Engineering University, Sanyuan 713800, Shaanxi, China; 3. Science Institute, Air Force Engineering University, Xi'an 710051, China;4. Air Force Command Department, Beijing 100843, China)

Abstract: It is a central problem in the research of coding to study the existence, structure and construction of the certain optimal property codes. In order to construct the quantum error-correcting codes, people have begun to study the self-orthogonal code that has the special self-dual distance. In this paper, two classes of sub-codes, which have optimal dual distance or intended optimal dual distance, of the binary non-decomposable self-dual codes of length n between 12 and 20, such as B_{12}, D_{14}, E_{16}, F_{16}, H_{18}, I_{18}, J_{20}, K_{20}, L_{20}, M_{20} and S_{20}, and the corresponding S-chain construction are studied. Based on the generator matrices of the self-dual codes, optimal sub-codes of dual distance 2, 3 and 4 of these self-dual codes are constructed by using a combinational method. Then code chains of these optimal sub-codes and their dual codes are discussed. Consequently, S-chains are constructed from these sub-codes with optimal dual distance or intended optimal dual distance. Finally, some very good quantum error-correcting codes are constructed from the S-chains obtained. These quantum codes are the ones that the distance reaches the maximum when their n and k are given.

Key Words: self-dual code; S-chain; quantum error-correcting code