DOI:10.3969/j.issn.1003-5060.2024.01.020

基于 2 个不相交子集的 MDS 自对偶码构造

曹宇婷, 朱士信
(合肥工业大学 数学学院,安徽 合肥 230601)

摘 要:最大距离可分(maximum distance separable,MDS)自对偶码是一类最优线性码,在通信、数据存储和区组设计等领域有着广泛的应用,构造 MDS 自对偶码是当前编码理论研究的一个热点问题。文章基于有限域及其乘法群的 2 个不相交子集,利用广义 Reed-Solomon(RS)码构造了几类新的 MDS 自对偶码;得到的 MDS 自对偶码具有灵活的长度。

关键词:最大距离可分(MDS)自对偶码;广义 Reed-Solomon(RS)码;有限域
中图分类号:O157.4 **文献标志码**:A **文章编号**:1003-5060(2024)01-0132-05

New MDS self-dual codes based on two disjoint subsets

CAO Yuting, ZHU Shixin
(School of Mathematics, Hefei University of Technology, Hefei 230601, China)

Abstract: Maximum distance separable(MDS) self-dual codes are a class of optimal linear codes, which can be extensively applied in many fields such as communications, data storage and block designs. It has become a hot topic to construct MDS self-dual codes in coding theory. In this paper, several new classes of MDS self-dual codes are constructed from generalized Reed-Solomon(RS) codes based on two disjoint subsets of the multiplicative subgroup of a finite field. The resulting MDS self-dual codes have flexible lengths.

Key words: maximum distance separable(MDS) self-dual code; generalized Reed-Solomon(RS) code; finite field

0 引 言

最大距离可分(maximum distance separable,MDS)码是代数编码领域中极其重要的一类码,具有良好的特性。MDS 码的构造是代数编码领域中的一个重要问题,特别是在码长不太长的情况下,其性能非常接近理论值。自对偶码是一类十分重要的线性码,在密码学[1]和组合学[2]中有广泛的应用。考虑这 2 类码的交集即 MDS 自对偶码是十分必要的。MDS 自对偶码和密码学、量子通信以及组合设计等领域有着密切的联系,因此构造参数最优的 MDS 自对偶码是当前编码理论的一个重要研究内容。目前,构造 MDS 自对偶码应用的数学工具主要有:① 基于经典码的构造,如代数几何码、经典自对偶线性码和广义(Reed-Solomon,RS)码等;② 基于组合的结构;③ 基于代数的构造。本文在广义 RS 码的基础上,结合编码理论和有限域,给出在一定条件下具有新参数的 MDS 自对偶码。

设 F_q 是有 q 个元素的有限域,其中 q 是素数幂。F_q 上的线性码 C 表示为 $[n,k,d]_q$,它是 F_{q^n} 的线性子空间,其中:k 为维数;d 为最小距离。当 $d=n-k+1$ 时,称 C 为 MDS 码。对线性码 C,$C^{\perp}$ 表示 C 的欧几里得对偶码。若 $C=C^{\perp}$,则

收稿日期:2023-02-20;**修回日期**:2023-03-03
基金项目:国家自然科学基金资助项目(12171134);国家自然科学基金联合基金资助项目(U21A20428)
作者简介:曹宇婷(1997—),女,安徽黄山人,合肥工业大学硕士生;
朱士信(1962—),男,安徽枞阳人,博士,合肥工业大学教授,博士生导师,通信作者,E-mail:zhushixin@hfut.edu.cn.

称 C 为自对偶码。

文献[3-4]基于正交设计构造 MDS 自对偶码,通过构造小域上的生成矩阵得到大的有限域上的 MDS 自对偶码;文献[5]使用循环码和负循环码构造 MDS 自对偶码。广义 RS 码是近年来最常用的 MDS 自对偶编码方式之一。文献[6]发现了具有任意参数的偶特征有限域上的 MDS 自对偶码;文献[7]使用广义 RS 码和扩展广义 RS 码构建了新的 MDS 自对偶码,并将该方法推广到具有一般长度的广义 RS 码;文献[8]基于分圆集合提出了 MDS 欧几里得自对偶码的若干新构造;文献[9]使用 F_q^* 及其 2 个不相交的乘法子群构建了 1 个新的 MDS 自对偶码族;文献[10]通过有理函数域给出了欧几里得 MDS 自对偶码的一些显式组合。

本文沿用文献[11]的方法,在 2 个不相交乘法子集的基础上,通过广义 RS 码构造 MDS 自对偶码。本文的结论推广了文献[8-9,11]的结果,得到了更多新的 MDS 自对偶码类。

1　预备知识

本节将回顾广义 RS 码的基本知识,引用相关的计算公式。

设 F_q 为有限域,q 为素数幂;$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$,$a_i(i=1,2,\cdots,n)$是 F_q 的非零元素,$\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$,$v_i(i=1,2,\cdots,n)$是 F_q 中彼此互异的元素。定义:

$$C_{\mathrm{GRS}_k}(\boldsymbol{a},\boldsymbol{v})=\{(v_1f(a_1),\cdots,v_nf(a_n)):$$
$$f(x)\in F_q[x],\ \deg(f(x))\leqslant k-1\}。$$

$C_{\mathrm{GRS}_k}(\boldsymbol{a},\boldsymbol{v})$和它的对偶码分别是 q 元$[n,k,n-k+1]$和$[n,n-k,k+1]$MDS 码。

设 $\eta(x)$是 F_q^* 的二次特征,Q_q 是 F_q^* 中所有平方数的集合。当 x 是 F_q^* 的平方数时,$\eta(x)=1$;当 x 是非平方数时,$\eta(x)=-1$,即

$$\eta(x)=\begin{cases}1, & x\in Q_q;\\ -1, & x\notin Q_q。\end{cases}$$

对任意 $A\subseteq F_q$,在 F_q 上将多项式表示为 $f_A(x)$,即 $f_A(x)=\prod\limits_{a\in A}(x-a)$。

对任意元素 $a\in A$,定义:

$$\delta_A(a)=\prod_{a'\in A,a'\neq a}(a-a')。$$

引理 1[12]　设 A 是 F_q 的含有 n 个元素的子集,n 是偶数,若对任意$a\in A$,$\eta(\delta_A(a))$的值都相等,则存在一个长度为 n 的 q 元 MDS 自对偶码。

引理 2[9]　1) 设 A 为 F_q 的子集,则对任意 $a\in A$,都有 $\delta_A(a)=f_A'(a)$,其中 $f_A'(a)$是 $f_A(x)$在 $x=a$ 处的导数。

2) 设 A_1 和 A_2 为 F_q 的 2 个不相交子集,$A=A_1\cup A_2$。对任意 $a\in A$,

$$\delta_A(a)=\begin{cases}\delta_{A_1}(a)f_{A_2}(a), & a\in A_1;\\ \delta_{A_2}(a)f_{A_1}(a), & a\in A_2。\end{cases}$$

引理 3[7]　设 $a\in F_q$ 是 n 次本原单位根,n 和 q 是整数且满足 $n\mid(q-1)$,则有:

1) $\prod\limits_{j=1,\,i\neq j}^{n}(g^i-g^j)=g^{i(n-1)}n=g^{-i}n$;

2) 对任意 $\gamma\in F_q$,有

$$x^n-\gamma^n=\prod_{1\leqslant i\leqslant n}(x-\gamma g^i)。$$

2　MDS 自对偶码的构造

设 $q=r^2$,r 是奇素数幂,利用 F_q^* 的 2 个互不相交的乘法子集 A 和 B 构造 1 个新的集合 D,得到 q 元 MDS 自对偶码的新长度。设 a 为满足 $a\mid(q-1)$的整数,记 $a=b_1b_2$,$b_1=\gcd(a,r+1)$,$b_2=a/\gcd(a,r+1)$,则 $b_2\mid[(r-1)(r+1)/b_1]$。又因为 $\gcd\left(b_2,(r+1)/b_1\right)=\gcd\left(a/b_1,(r+1)/b_1\right)=1$,所以 $b_1\mid(r+1)$,$b_2\mid(r-1)$。

定理 1　设 $q=r^2$,r 是奇素数且 $r\equiv1(\bmod 4)$;b_2 和$(r+1)/b_1$ 都是奇数,$b_1\equiv2(\bmod 4)$,则 $a\equiv2(\bmod 4)$。当 s 是偶数、t 是奇数时,可以得到长度为 $n=s(r+1)/b_1+t(r-1)/b_2$ 的一类 q 元 MDS 自对偶码,其中 $1\leqslant s\leqslant(r-1)/b_2$,$1\leqslant t\leqslant(r+1)/b_1$。

证明　设 $n=s(r+1)/b_1+t(r-1)/b_2$,θ 是 F_q^* 的本原元,定义 $\alpha=\theta^{b_1(r-1)}$,$\beta=\theta^{b_2(r+1)}$。

设 A 和 B 是 F_q^* 的 2 个子群,并且 $A=\langle\alpha\rangle$,$B=\langle\beta\rangle$,$\alpha=\theta^{b_1(r-1)}\in Q_q$,$\beta=\theta^{b_2(r+1)}\in Q_q$。因为 $b_1(r-1)$和 $b_2(r+1)$都是偶数且 $a\equiv2(\bmod 4)$,所以 $\alpha=\theta^{b_1(r-1)}\in Q_q$,$\beta=\theta^{b_2(r+1)}\in Q_q$ 和 $\lambda=\theta^{\frac{a}{2}}\notin Q_q$。

定义 $D=(\bigcup\limits_{i=0}^{s-1}\beta^iA)\cup(\bigcup\limits_{j=0}^{t-1}\lambda^{2j+1}B)$,当 $0\leqslant i\leqslant s-1$,$0\leqslant j\leqslant t-1$ 时,$\beta^iA\cap\lambda^{2j+1}B=\varnothing$。于是 D 是 2 个不相交集合$\bigcup\limits_{i=0}^{s-1}\beta^iA$ 和$\bigcup\limits_{j=0}^{t-1}\lambda^{2j+1}B$ 的并集。

首先证明,$\beta^0,\cdots,\beta^{s-1}$是 F_q^* 子集 A 的 s 个不同陪集的代表元。若不是,则对子集 A,存在 $0\leqslant i_1<i_2\leqslant s-1$,使得 $\beta^{i_1}A=\beta^{i_2}A$;即存在 $1\leqslant h\leqslant(r+1)/b_1$,使得 $\beta^{i_1-i_2}=\alpha^h$。于是有:

$$\theta^{b_2(r+1)(i_1-i_2)-b_1(r-1)}h=1\Rightarrow$$
$$(q-1)\mid[b_2(r+1)(i_1-i_2)-b_1(r-1)h]。$$

因为 $b_1(r-1)h<q-1$,所以有:

$$b_1(r-1)\mid b_2(r+1)(i_1-i_2)\Rightarrow$$
$$\frac{r-1}{b_2}\Big|\frac{r+1}{b_1}(i_1-i_2)。$$

又因为 $i_1-i_2\leqslant s-1<(r-1)/b_2$,所以得出矛盾。

类似地,$\lambda^1,\lambda^3,\cdots,\lambda^{2t-1}$ 是 F_q^* 的子集 B 的 t 个不同陪集的代表元。若不是,则对子集 B,存在 $0\leqslant j_1<j_2\leqslant t-1$,使得 $\lambda^{2j_1+1}B=\lambda^{2j_2+1}B$;即存在 $1\leqslant m\leqslant(r-1)/b_2$,使得 $\lambda^{2(j_1-j_2)}=\beta^m$,于是有:

$$\theta^{a(j_1-j_2)-b_2(r+1)m}=1\Rightarrow$$
$$(q-1)\mid[a(j_1-j_2)-b_2(r+1)m]。$$

因为 $b_2(r+1)m\leqslant q-1$,所以有:

$$b_2(r+1)\mid a(j_1-j_2)\Rightarrow\frac{r+1}{b_1}\Big|(j_1-j_2)。$$

又因为 $j_1-j_2\leqslant t-1<(r+1)/b_1$,所以得出矛盾。此时 n 为偶数。

下面计算 $\delta_D(\lambda^{2i+1}\beta^j)$。由引理 2 可知,对任意 $0\leqslant i\leqslant t-1$ 和 $1\leqslant j\leqslant(r-1)/b_2$,有

$$\delta_D(\lambda^{2i+1}\beta^j)=\delta_{\lambda^{2i+1}B}(\lambda^{2i+1}\beta^j)\times$$
$$f_{\beta^hA}(\lambda^{2i+1}\beta^j)=\lambda^{(2i+1)\left(\frac{r-1}{b_2}-1\right)}\beta^{-j}\frac{r-1}{b_2}\times$$
$$\prod_{l=0,l\neq i}^{t-1}\left[\lambda^{(2i+1)\frac{r-1}{b_2}}-\lambda^{(2l+1)\frac{r-1}{b_2}}\right]\times$$
$$\prod_{h=0}^{s-1}\left[(\lambda^{2i+1}\beta^j)^{\frac{r+1}{b_1}}-\beta^{h\frac{r+1}{b_1}}\right]。$$

注意到,$\beta\in Q_q$ 和 $(r-1)/b_2$ 都是偶数,于是有 $\frac{r-1}{b_2}\lambda^{(2i+1)\frac{(r-1)}{b_2}}\beta^{-j}\frac{r-1}{b_2}\in Q_q$。故先讨论 $\prod_{l=0,l\neq i}^{t-1}\left[\lambda^{(2i+1)\frac{r-1}{b_2}}-\lambda^{(2l+1)\frac{r-1}{b_2}}\right]$。

设 $w=\prod_{l=0,l\neq i}^{t-1}\left[\lambda^{(2i+1)\frac{r-1}{b_2}}-\lambda^{(2l+1)\frac{r-1}{b_2}}\right]$,因为

$$\left[\lambda^{(2i+1)\frac{r-1}{b_2}}\right]^{r+1}=\left[\theta^{\frac{(2i+1)b_1}{2}}\right]^{q-1}=1,$$
$$\left[\lambda^{(2i+1)\frac{r-1}{b_2}}\right]^{r}=\lambda^{-(2i+1)\frac{r-1}{b_2}},$$

所以

$$w=\theta^{\frac{r+1}{2}(t-1)-\frac{b_1}{2}[2(t-1)(i+1)+t(t-1)-2i]+k(r+1)}。$$

对任意正整数 k,当 t 是奇数且 $b_1\equiv2\pmod4$ 时,可得 $w\in Q_q$。

对 $\prod_{h=0}^{s-1}\left[(\lambda^{2i+1}\beta^{j\frac{(r+1)}{b_1}}-\beta^{h\frac{(r+1)}{b_1}}\right]$,有

$$\prod_{h=0}^{s-1}\left[\left(\theta^{(2i+1)a/2b_1+jb_2\frac{(r+1)}{b_1}}\right)^{r+1}-\left(\theta^{hb_2\frac{(r+1)}{b_1}}\right)^{r+1}\right]\in F_r^*\subset Q_q。$$

综上所述,可得:

$$\eta(\delta_D(\beta^j\alpha^j))=\eta(\lambda^{-(2i+1)})=-1。$$

当 $0\leqslant i\leqslant s-1$,$1\leqslant j\leqslant(r+1)/b_1$ 时,计算 $\delta_D(\beta^j\alpha^j)$ 的值。由引理 2 得:

$$\delta_D(\beta^j\alpha^j)=\delta_{\beta^jA}(\beta^j\alpha^j)\times$$
$$f_{\lambda^{2h+1}B}(\beta^j\alpha^j)=\beta^{j\left[\frac{(r+1)}{b_1}-1\right]}\alpha^{-j}\frac{r+1}{b_1}\times$$
$$\prod_{l=0,l\neq i}^{s-1}\left[\beta^{i\frac{(r+1)}{b_1}}-\beta^{l\frac{(r+1)}{b_1}}\right]\times$$
$$\prod_{h=0}^{t-1}\left[\alpha^{j\frac{(r-1)}{b_2}}-\lambda^{(2h+1)\frac{(r-1)}{b_2}}\right],$$

其中,$\beta^{j\left[\frac{(r+1)}{b_1}-1\right]}\alpha^{-j}\in Q_q$。

设 $w'=\prod_{h=0}^{t-1}\left[\alpha^{j\frac{(r-1)}{b_2}}-\lambda^{(2h+1)\frac{(r-1)}{b_2}}\right]$,对任意正整数 k,若 $b_1\equiv2\pmod4$,可得 $w'\in Q_q$。

类似地,

$$\prod_{l=0,l\neq i}^{s-1}\left[\beta^{i\frac{(r+1)}{b_1}}-\beta^{l\frac{(r+1)}{b_1}}\right]=$$
$$\prod_{l=0,l\neq i}^{s-1}\left[\left(\theta^{jb_2\frac{(r+1)}{b_1}}\right)^{r+1}-\left(\theta^{jb_2\frac{(r+1)}{b_1}}\right)^{r+1}\right]\in F_r^*\subset Q_q。$$

综上所述,得:

$$\eta(\delta_D(\lambda^{2i+1}\beta^j))=\eta((r+1)/b_1)=-1。$$

由引理 1 知,存在一个长度为 n 的 q 元 MDS 自对偶码。

$r\equiv1\pmod4$ 的情况。定理 1 构造的 MDS 自对偶码与文献[11]中的定理 1 相比,改变 s 和 t 的取值范围,即由 $1\leqslant s\leqslant(r+1)/(2v)$ 和 $1\leqslant t\leqslant(r-1)/(2u)$ 改变为 $1\leqslant s\leqslant(r-1)/b_2$ 和 $1\leqslant t\leqslant(r+1)/b_1$,其中 b_2 为奇数。不难看出,改变分母的取值,得到一类新的长度为 n 的 MDS 自对偶码。

例 1 设 $r=25$,$q=25^2$,取 $b_1=26$,$b_2=3$,$s=2$,$t=1$。由定理 1 可知,存在一个长度 $n=10$ 的 MDS 自对偶码。此时,得到的长度是新的。

定理 2 设 $q=r^2$,其中 r 为奇素数幂且 $r\equiv3\pmod4$。假设 b_1、$(r-1)/b_2$ 都是奇数,$b_2\equiv2\pmod4$,则 $a\equiv2\pmod4$。若 $t\equiv0\pmod4$,则存在一个长度为 $n=s(r+1)/b_1+t(r-1)/b_2$ 的 q 元MDS 自对偶码,其中:$1\leqslant s\leqslant(r-1)/b_2$;$1\leqslant t\leqslant(r+1)/b_1$。

证明 根据上述构造,当 $1\leqslant s\leqslant(r-1)/b_2$ 且 $1\leqslant t\leqslant(r+1)/b_1$ 时,设 $n=s(r+1)/b_1+t(r-$

$1)/b_2$。设 $A=\langle\alpha\rangle$ 和 $B=\langle\beta\rangle$ 是 F_q^* 的子集,$\alpha=\theta^{b_1(r-1)}\in Q_q$,$\beta=\theta^{b_2(r+1)}\in Q_q$ 且 $\zeta=\theta^{q/2}\notin Q_q$。

定义 $D=\left(\bigcup_{i=0}^{s-1}\zeta^{2i+1}A\right)\cup\left(\bigcup_{j=0}^{t-1}\alpha^jB\right)$,当 $a\equiv 2(\bmod 4)$时,有 $\zeta^{2i+1}A\cap\alpha^jB=\varnothing$。

一方面,不难证明,当 $1\leqslant s\leqslant(r-1)/b_2$ 时,$\zeta^1,\zeta^3,\cdots,\zeta^{2s-1}$ 是 A 的 s 个不同陪集的代表元。当 $1\leqslant t\leqslant(r+1)/b_1$ 时,$\alpha^0,\cdots,\alpha^{t-1}$ 是 B 的 t 个不同陪集的代表元。

另一方面,当 $0\leqslant i\leqslant t-1$,$1\leqslant j\leqslant(r-1)/b_2$ 时,

$$\delta_D(\alpha^i\beta^j)=\delta_{\alpha^iB}(\alpha^i\beta^j)\times f_{\zeta^{2h+1}A}(\alpha^i\beta^j)=\alpha^{i\lfloor(r-1)/b_2-1\rfloor}\beta^{-j}(r-1)/b_2\times\prod_{l=0,l\neq i}^{t-1}\left[\alpha^{i(r-1)/b_2}-\alpha^{l(r-1)/b_2}\right]\times\prod_{h=0}^{s-1}\left[\beta^{j(r+1)/b_1}-\xi^{(2h+1)(r+1)/b_1}\right]。$$

因为 $\beta,\alpha\in Q_q$,所以 $\alpha^{i\lfloor(r-1)/b_2-1\rfloor}\beta^{-j}\in Q_q$。

对任意正整 k,

$$p=\prod_{l=0,l\neq i}^{t-1}\left[\alpha^{i(r-1)/b_2}-\alpha^{l(r-1)/b_2}\right]=\theta^{(r+1)(t-1)/2-b_1(r-1)\lfloor i(t-2)+t(t-1)/2\rfloor/b_2+k(r+1)}。$$

当 b_1 和 $(r-1)/b_2$ 为奇数且 $t\equiv0(\bmod 4)$时,有 $p\in Q_q$。又因为

$$p'=\prod_{h=0}^{s-1}\left[\beta^{j(r+1)/b_1}-\zeta^{(2h+1)(r+1)/b_1}\right]=\prod_{h=0}^{s-1}\left[(\theta^{jb_2(r+1)/b_1})^{r+1}-(\theta^{b_2(2h+1)/2})^{r+1}\right]\in F_r^*\subset Q_q,$$

所以 $p'\in F_r^*\subset Q_q$。

综上所述,可得:

$$\eta(\delta_D(\alpha^i\beta^j))=\eta((r-1)/b_2)=-1。$$

类似地,当 $0\leqslant i\leqslant s-1$,$1\leqslant j\leqslant(r+1)/b_1$ 时,

$$\delta_D(\zeta^{2i+1}\alpha^j)=\delta_{\zeta^{2i+1}A}(\zeta^{2i+1}\alpha^j)\times f_{\alpha^hB}(\zeta^{2i+1}\alpha^j)=\zeta^{(2i+1)(\frac{r+1}{b_1}-1)}\alpha^{-j}\frac{r+1}{b_1}\times\prod_{l=0,l\neq i}^{s-1}\left[\zeta^{(2i+1)(r+1)/b_1}-\zeta^{(2l+1)(r+1)/b_1}\right]\times\prod_{h=0}^{t-1}\left[(\zeta^{2i+1}\alpha^j)^{(r-1)/b_2}-\alpha^{h(r-1)/b_2}\right]。$$

因为 $\beta,\alpha\in Q_q$,所以 $\zeta^{(2i+1)\frac{r+1}{b_1}}\alpha^{-j}\frac{r+1}{b_1}\in Q_q$。对任意正整 k,当 $t\equiv0(\bmod 4)$时,可得 $g'=\theta^M\in F_r^*\subset Q_q$,其中,$M=\frac{(r+1)t}{2}-\frac{b_1(2i+1)t}{2}-jb_1\frac{(r-1)t}{b_2}-b_1\frac{t(t-1)(r-1)}{2b_2}+k(r+1)$。又因为

$$g=\prod_{l=0,l\neq i}^{s-1}\left[\zeta^{(2i+1)(r+1)/b_1}-\zeta^{(2l+1)(r+1)/b_1}\right]=\prod_{l=0,l\neq i}^{s-1}\left[\left(\theta^{(2i+1)b_2/2}\right)^{r+1}-\left(\theta^{(2l+1)b_2/2}\right)^{r+1}\right]\in F_r^*\subset Q_q。$$

综上所述,可得:

$$\eta(\delta_D(\zeta^{2i+1}\alpha^j))=\eta(\zeta^{-(2i+1)})=-1。$$

由引理 1 可知,存在一个长度为 n 的 q 元 MDS 自对偶码。

$r\equiv3(\bmod 4)$的情况。与文献[11]相比,当 $(r+1)bs^2/(2a)$为奇数时,得到一类长度为 n 的 MDS 自对偶码,它的长度是新的。

例 2　设 $r=19$,$q=19^2$,取 $b_1=5$,$b_2=2$,$s=9$,$t=4$。由定理 2 可知,存在一个长度为 $n=72$ 的 MDS 自对偶码。此时,构造的长度是新的。值得注意的是当 $r=19$ 时,获得 61 个的新 MDS 自对偶码。

类似于定理 2,可以得到定理 3。

定理 3　设 $q=r^2$,其中 r 为奇素数幂且 $r\equiv3(\bmod 4)$。假设 b_2 和 $(r+1)/b_1$ 都是奇数,$b_1\equiv0(\bmod 4)$,则 $a\equiv2(\bmod 4)$。当 s 是奇数、t 是偶数时,可以得到长度为 $n=s(q-1)/b_1+t(r-1)$ 的一类 q 元 MDS 自对偶码,其中 $1\leqslant s\leqslant b_1/2$,$1\leqslant t\leqslant(r+1)/b_1$。

例 3　设 $r=19$,$q=19^2$,取 $b_1=4$,$s=1$,$t=4$。由定理 3 可知,存在一个长度为 $n=162$ 的 MDS 自对偶码。此时,得到的长度是新的。值得注意的是,当 $r=19$ 时,可以获得 2 个新的 MDS 自对偶码,长度分别为 $n=126$ 和 $n=162$。

3　结　　论

本文扩展了文献[8-9,11]的构造方法,在 F_q^* 中 2 个不相交的乘法子群和广义 RS 码的基础上,在奇特征有限域上构造了一些新的 MDS 自对偶码。构造的关键是选择适当的相互不相交的子群和特定的参数,使其对应的广义 RS 码为 MDS 自对偶码,并证明通过进一步扩展可以获得其他长度的码。由于自对偶码的参数完全由码长 n 决定,在不同的有限域或有限环上构造不同码长的 MDS 自对偶码是一个值得研究的问题。寻找更多新的自对偶码是今后研究的方向。

[参　考　文　献]

[1]　DOUGHERTY S T, MESNAGER S, SOLE P. Secret-sharing

schemes based on self-dual codes[C]//2008 IEEE Information Theory Workshop. [S. l.]:IEEE,2008:338-342.

[2] MACWILLIAMS F J,SLOANE N J A. The theory of error-correcting codes[M]. Oxford:Elsevier,1977:317-329.

[3] GEORGIOU S,KOUKOUVINOS C. MDS self-dual codes very large prime fields[J]. Finite Fields and Their Applications,2002,8(4):455-470.

[4] HAEADA M,KHAEAGHANI H. Orthogonal designs and MDS self-dual codes[J]. Australasian Journal of Combinatorics,2006,35:57-67.

[5] GUENDA K. New MDS self-dual codes over finite fields [J]. Designs Codes and Cryptography,2012,62(1):31-42.

[6] FANG W J,FU F W. New constructions of MDS Euclidean self-dual codes from GRS codes and extended GRS codes [J]. IEEE Transactions on Information Theory, 2019, 65(9):5574-5579.

[7] YAN H. A note on the constructions of MDS self-dual codes[J]. Cryptography and Communications,2019,11(2): 259-268.

[8] MASSEY J L. Some applications of coding theory in cryptography[M]//Codes and Ciphers:Cryptography and Coding IV. Essex,England:Formara Ltd. ,1995:33-47.

[9] ZHANG A X,FENG K Q. A unified approach to construct MDS self-dual codes via Reed-Solomon codes[J]. IEEE Transactions on Information Theory, 2020, 66(6): 3650-3656.

[10] SOK L. Explicit constructions of MDS self-dual codes[J]. IEEE Transactions on Information Theory,2019,66(6): 3603-3615.

[11] HUANG Z T,FANG W J,FU F W. New constructions of MDS self-dual and self-orthogonal codes via GRS codes[J/OL]. (2021-10-27). https://arxiv.org/pdf/2103.11665.pdf.

[12] JIN L F,XING C P. New MDS self-dual codes from generalized Reed-Solomon codes[J]. IEEE Transactions on Information Theory,2016,63(3):1434-1438.

(责任编辑 朱晓临)

(上接第 111 页)

[19] WOZNIAKIEWICZ A, WIETECHA-POSLUSZNY R, WOZNIAKIEWICZ M,et al. A quick method for determination of psychoactive agents in serum and hair by using capillary electrophoresis and mass spectrometry[J]. Journal of Pharmaceutical and Biomedical Analysis,2015,111: 177-185.

[20] CHEN R, REN C P, LIU M, et al. Early detection of SARS-CoV-2 seroconversion in humans with aggregation-induced near-infrared emission nanoparticle-labeled lateral flow immunoassay[J]. American Chemical Society Nano, 2021,15(5):8996-9004.

[21] ALONSO N,GRIFFA N,MOYANO R D,et al. Development of a lateral flow immunochromatography test for the rapid detection of bovine tuberculosis[J]. Journal of Immunological Methods,2021,491(4):112941.

[22] 吴玉晗,陈伟. 侧向免疫层析快速检测牛乳中四环素和青霉素[J]. 食品科学,2020,41(24):281-286.

[23] 钟友好,赵弟萍,薛峰,等. 基于信号增敏型试纸条三聚氰胺超灵敏检测方法[J]. 食品科学,2014,35(8):289-294.

[24] CHEN W,LI X N,WU Q,et al. Rapid and easy determination of morphine in chafing dish condiments with colloidal gold labeling based lateral flow strips[J]. Food Science and Human Wellness,2019,8(1):40-45.

[25] HASSANTABAR F, ZORRIEHZAHRA M J, FIROUZBAKHSH F, et al. Development and evaluation of colloidal gold immunochromatography test strip for rapid diagnosis of nervous necrosis virus in golden grey mullet (*Chelon aurata*)[J]. Journal of Fish Diseases, 2021, 44(6):783-791.

[26] YANG X D,SUN Z K,TIAN F S,et al. A lateral flow immunochromatographic strip test for rapid detection of hexoestrol in fish samples[J]. Royal Society Open Science, 2018,5(8):180504.

[27] WANG Y L,WANG L M,XUE J J,et al. Signal-amplified lateral flow test strip for visual detection of Cu^{2+}[J]. PLOS ONE,2017,12(1):e0169345.

(责任编辑 张 镅)