文章编号:1671-9352(2025)05-0087-06 DOI:10.6040/j.issn.1671-9352.0.2023.247

三阶扭曲广义 Reed-Solomon 码

张月,闫铭,黄俊松,闫统江*
(中国石油大学(华东)理学院, 山东 青岛 266580)

摘要:构造三阶扭曲广义里德-所罗门(twisted generalized Reed-Solomon, TGRS)码,刻画了这类码是极大距离可分(maximum distance separable, MDS)码的充要条件,给出 MDS 码的新型构造方法,拓展了一阶和二阶 MDS-TGRS 码的研究。
关键词:纠错编码;MDS 码;扭曲广义 Reed-Solomon 码;广义 Reed-Solomon 码;Reed-Solomon 码
中图分类号:O236.2 **文献标志码**:A
引用格式:张月,闫铭,黄俊松,等.三阶扭曲广义 Reed-Solomon 码[J]. 山东大学学报(理学版),2025,60(5):87-92.

Twisted generalized Reed-Solomon codes of order three

ZHANG Yue, YAN Ming, HUANG Junsong, YAN Tongjiang*
(College of Science, China University of Petroleum (East China), Qingdao 266580, Shandong, China)

Abstract: Twisted generalized Reed-Solomon (TGRS) codes of order three are constructed. The necessary and sufficient condition for this class of codes whitch are maximum distance separable(MDS) codes are characteried. A new construction method for MDS codes is provided and the research on MDS-TGRS codes of order one and order two are expanded.
Key words: error correction coding; MDS codes; twisted generalized Reed-Solomon codes; generalized Reed-Solomon codes; Reed-Solomon codes

0 引言

线性纠错码在数据存储、信息安全等领域具有重要应用。构造新的具有良好参数的线性纠错码是编码理论与应用研究的重要课题。本文中,设 p 是一个素数,m、n 是正整数,F_q 是阶为 $q=p^m$ 的有限域,F_q^* 表示 F_q 非零元集合,$\boldsymbol{F}_q^n$ 是 F_q 上 n 维行向量空间。$\boldsymbol{F}_q^n$ 的每个 k 维子空间 C 都被称作一个 q 元$[n,k,d]$线性码,其中 d 为线性码 C 的极小距离[1]。若一个线性码 C 的参数达到 Singleton 界 $d\leqslant n-k+1$, 则称它为极大距离可分(maximum distance separable, MDS)码。因为 MDS 码获得了最大可实现的极小距离,是固定码率条件下具有最大纠错能力的编码,所以被广泛应用于秘密共享方案设计、分布式存储系统和随机错误信道编码。广义里德-所罗门(generalized Reed-Solomon, GRS)码是一类著名的 MDS 码,而扭曲广义里德-所罗门(twisted generalized Reed-Solomon, TGRS)码是 GRS 码的扭曲码,包含 GRS 码,但不一定是 MDS 码,TGRS 码被广泛应用于 McElice 公钥密码体制等领域。因此,研究 TGRS 码满足 MDS 的充分必要条件是一项重要的研究。

扭曲里德-所罗门(twisted Reed-Solomon, TRS)码与 TGRS 码单项式等价[2]。2017 年, Beelen 等[3]首先构造了三类一阶 MDS-TRS 码。接着 Beelen 等[4]通过增加单项式的方法构造了一类新型一阶 TRS 码,并给出了一类 MDS-TRS 码。随后 Liu 等[5]构造了更长码长的新型 MDS-TRS 码,Huang 等[6]给出了一阶 TRS 码是 MDS 码和近极大距离可分(nearest maximum distance separable, NMDS)码的充要条件。2022 年,

收稿日期:2023-06-05; **网络出版时间**:2024-04-08 16:43:30
基金项目:中央高校基本科研业务费专项资金资助(22CX03015A;20CX05012A);山东省自然科学基金资助项目(ZR2022MA061)
第一作者:张月(1998—),女,硕士研究生,研究方向为代数编码学. E-mail:zy1159261554zy@163.com
*通信作者:闫统江(1973—),男,教授,博士生导师,博士,研究方向为代数编码学. E-mail:yantoji@163.com

Beelen 等[7]利用 Schur 积证明了大部分 MDS-TRS 码并不等价于 GRS 码。同年,几类新型一阶 MDS-TRS 码通过改造 TRS 码的生成矩阵被构造[8-12]。Sui 等[11]构造了二阶 TRS 码,并给出它满足 MDS 的充分必要条件。本文构造了三阶 TGRS 码并给出它是 MDS 码的充分必要条件。

1 预备知识

向量空间 $\boldsymbol{F}_q^n$ 任意两个行向量 $\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$ 和 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$ 的 Hamming 距离定义为

$$\mathrm{dist}(\boldsymbol{u},\boldsymbol{v})=\#\{i:u_i\neq v_i,\ 1\leqslant i\leqslant n\},$$

其中#S 表示集合 S 的基数。设 C 是一个 q 元$[n,k,d]$线性码,则 C 的极小距离 $d=\min\{\mathrm{dist}(\boldsymbol{u},\boldsymbol{v}):\boldsymbol{u},\boldsymbol{v}\in C,\boldsymbol{u}\neq\boldsymbol{v}\}$。

令多项式组$\begin{cases}f_1(x)=\eta_{00}x^k+\eta_{01}x^{k+1}+\eta_{02}x^{k+2}\\ f_2(x)=\eta_{10}x^k+\eta_{11}x^{k+1}+\eta_{12}x^{k+2}\end{cases}$, $\boldsymbol{\eta}=\begin{pmatrix}\eta_{00}&\eta_{01}&\eta_{02}\\ \eta_{10}&\eta_{11}&\eta_{12}\end{pmatrix}$,其中 $\eta_{ij}\in F_q$, $i=0,1$, $j=0,1,2$。令向量 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\boldsymbol{F}_q^n$且 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 互不相同,向量 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)\in(\boldsymbol{F}_q^*)^n$。将生成矩阵为

$$\boldsymbol{G}=\begin{pmatrix}v_1&\cdots&v_n\\ v_1\alpha_1&\cdots&v_n\alpha_n\\ \vdots&\ddots&\vdots\\ v_1\alpha_1^{k-3}&\cdots&v_n\alpha_n^{k-3}\\ v_1(\alpha_1^{k-2}+f_1(\alpha_1))&\cdots&v_n(a_n^{k-2}+f_1(\alpha_n))\\ v_1(\alpha_1^{k-1}+f_2(\alpha_1))&\cdots&v_n(\alpha_n^{k-1}+f_2(\alpha_n))\end{pmatrix}_{k\times n}$$

的线性码 $C_k(\boldsymbol{\alpha},\boldsymbol{v},\boldsymbol{\eta})$定义为三阶 TGRS 码。若多项式 $f_1(x)$ 和 $f_2(x)$ 的项数的最大值为 1(或 2),将线性码 $C_k(\boldsymbol{\alpha},\boldsymbol{v},\boldsymbol{\eta})$ 称为一阶(或二阶)TGRS 码。此外,若$\begin{cases}f_1(x)=\eta_0x^{k+2}\\ f_2(x)=\eta_1x^k\end{cases}$,将线性码 $C_k(\boldsymbol{\alpha},\boldsymbol{v},\boldsymbol{\eta})$ 称为不连续一阶 TGRS 码;若$\begin{cases}f_1(x)=\eta_{00}x^k+\eta_{01}x^{k+2}\\ f_2(x)=\eta_{10}x^k+\eta_{11}x^{k+2}\end{cases}$,将线性码 $C_k(\boldsymbol{\alpha},\boldsymbol{v},\boldsymbol{\eta})$称为不连续二阶 TGRS 码。特殊地,$C_k(\boldsymbol{\alpha},\boldsymbol{I},\boldsymbol{\eta})$称作 TRS 码,其中 $\boldsymbol{v}=\boldsymbol{I}=(1,1,\cdots,1)$。

2 主要结果

引理 1[11] 线性码 C 是 MDS 码⇔线性码 C 的生成矩阵的任意 k 阶子式不为 0, $0<k<n$。

引理 2[10] 若 $\boldsymbol{A}_t=\begin{pmatrix}c_0&0&\cdots&0\\ c_1&c_0&\cdots&0\\ \vdots&\vdots&\ddots&\vdots\\ c_t&c_{t-1}&\cdots&c_0\end{pmatrix}$, 其中 $c_0=1$, $c_1,c_2,\cdots,c_t\in F_q$, $0\leqslant t\leqslant 2$, 那么 $\boldsymbol{A}_t^{-1}=\begin{pmatrix}e_0&0&\cdots&0\\ e_1&e_0&\cdots&0\\ \vdots&\vdots&\ddots&\vdots\\ e_t&e_{t-1}&\cdots&e_0\end{pmatrix}$, 其中 $e_0=1$, $e_p=-\sum\limits_{q=0}^{p-1}e_qc_{p-q}$, $1\leqslant p\leqslant t$。

引理 3 令 $3\leqslant k<n$,$\alpha_1,\alpha_2,\cdots,\alpha_k$ 是 F_q 中的不同元素, $\prod\limits_{i\in I}(x-\alpha_i)=\sum\limits_{l=0}^{k}c_lx^{k-l}$,其中任意 k-子集 $I\subseteq\{1,2,\cdots,n\}$。令 $e_0=1$, $e_p=-\sum\limits_{q=0}^{p-1}e_qc_{p-q}$, $1\leqslant p\leqslant t$, $0\leqslant t\leqslant 2$。若 $\alpha_i^{k+t}=\sum\limits_{r=0}^{k-1}g_r^{(t)}\alpha_i^r$,则

$$g_{k-j}^{(t)}=-\sum_{s=0}^{\min\{t,k-j\}}e_{t-s}c_{s+j},\quad 1\leqslant j\leqslant 2。$$

证明　为了简便,令 k-子集 $I=\{1,2,\cdots,k\}$, $(g_0^{(t)},g_1^{(t)},\cdots,g_{k-1}^{(t)})$是下列方程组的唯一解:

$$(x_0,x_1,\cdots,x_{k-1})\begin{pmatrix}1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & \cdots & \alpha_k\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_k^{k-1}\end{pmatrix}=(\alpha_1^{k+t},\alpha_2^{k+t},\cdots,\alpha_k^{k+t})。$$

这意味着 $\alpha_i^{k+t}=\sum\limits_{r=0}^{k-1}g_r^{(t)}\alpha_i^r$, $1\leqslant i\leqslant k$, $0\leqslant t\leqslant 2$, 因此,$\alpha_1,\alpha_2,\cdots,\alpha_k$ 是多项式 $m_t(x)=x^{k+t}-\sum\limits_{r=0}^{k-1}g_r^{(t)}x^r$ 的根。另外,假设存在首一多项式 $h_t(x)=\sum\limits_{i=0}^{t}a_i^{(t)}x^i$ 满足

$$m_t(x)=h_t(x)\prod_{i=1}^{k}(x-\alpha_i)=\Big(\sum_{i=0}^{t}a_i^{(t)}x^i\Big)\Big(\sum_{l=0}^{k}c_lx^{k-l}\Big),$$

其中$a_i^{(t)}\in F_q$。比较 $m_t(x)$的 2 种表示中 $x^{k+t},x^{k+t-1},\cdots,x^k,\cdots,x^0$ 的系数可得

$$\begin{cases}(a_0^{(t)},a_1^{(t)},\cdots,a_t^{(t)})\boldsymbol{A}_t=(0,0,\cdots,1), & 0\leqslant t\leqslant 2,\\ g_{k-j}^{(t)}=-\sum\limits_{s=0}^{\min\{t,k-j\}}a_s^{(t)}c_{s+j}, & 1\leqslant j\leqslant 2。\end{cases}$$

其中 $\boldsymbol{A}_t=\begin{pmatrix}c_0 & 0 & \cdots & 0\\ c_1 & c_0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ c_t & c_{t-1} & \cdots & c_0\end{pmatrix}$。再由引理 2 可知$(a_0^{(t)},a_1^{(t)},\cdots,a_t^{(t)})=(0,0,\cdots,1)\boldsymbol{A}_t^{-1}=(e_t,e_{t-1},\cdots,e_0)$,即 $a_s^{(t)}=e_{t-s}$, 则 $g_{k-j}^{(t)}=-\sum\limits_{s=0}^{\min\{t,k-j\}}e_{t-s}c_{s+j}$, $1\leqslant j\leqslant 2$。

基于以上引理,给出本文的主要结果。

定理 1　设 $3\leqslant k<n$,向量 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\boldsymbol{F}_q^n$且 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 互不相同,向量 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)\in(\boldsymbol{F}_q^*)^n$。那么 TGRS 码 $C_k(\boldsymbol{\alpha},\boldsymbol{v},\boldsymbol{\eta})$是 MDS 码的充分必要条件是

$$\boldsymbol{\eta}=\begin{pmatrix}\eta_{00} & \eta_{01} & \eta_{02}\\ \eta_{10} & \eta_{11} & \eta_{12}\end{pmatrix}\in\Omega,$$

其中

$$\Omega=\left\{\eta\in\boldsymbol{F}_q^{2\times 3}:\text{对任意 }k\text{-子集 }I\subseteq\{1,2,\cdots,n\},\ \begin{vmatrix}1+\sum\limits_{t=0}^{2}\eta_{0t}g_{k-2}^{(t)} & \sum\limits_{t=0}^{2}\eta_{0t}g_{k-1}^{(t)}\\ \sum\limits_{t=0}^{2}\eta_{1t}g_{k-2}^{(t)} & 1+\sum\limits_{t=0}^{2}\eta_{1t}g_{k-1}^{(t)}\end{vmatrix}\neq 0\right\},$$

$$\prod_{i\in I}(x-\alpha_i)=\sum_{l=0}^{k}c_lx^{k-l},\ g_{k-j}^{(t)}=-\sum_{s=0}^{\min\{t,k-j\}}e_{t-s}c_{s+j},\quad 1\leqslant j\leqslant 2,\ 0\leqslant t\leqslant 2。$$

证明　令 k-子集 $I=\{1,2,\cdots,k\}$。由引理 3 可知,若 $\alpha_i^{k+t}=\sum\limits_{r=0}^{k-1}g_r^{(t)}\alpha_i^r$, $1\leqslant i\leqslant k$, $0\leqslant t\leqslant 2$,则 $g_{k-j}^{(t)}=-\sum\limits_{s=0}^{\min\{t,k-j\}}e_{t-s}c_{s+j}$, $1\leqslant j\leqslant 2$,因此由引理 3 可得 k 阶子式

$$|\boldsymbol{G}_I|=\begin{vmatrix}\cdots & v_i & \cdots\\ \cdots & v_i\alpha_i & \cdots\\ \vdots & \vdots & \vdots\\ \cdots & v_i\alpha_i^{k-3} & \cdots\\ \cdots & v_i(\alpha_i^{k-2}+f_1(\alpha_i)) & \cdots\\ \cdots & v_i(\alpha_i^{k-1}+f_2(\alpha_i)) & \cdots\end{vmatrix}$$

$$
=\begin{vmatrix}
\cdots & v_i & \cdots \\
\cdots & v_i\alpha_i & \cdots \\
\vdots & \vdots & \vdots \\
\cdots & v_i\alpha_i^{k-3} & \cdots \\
\cdots & v_i(\alpha_i^{k-2}+\sum_{t=0}^{2}\eta_{0t}\alpha_i^{k+t}) & \cdots \\
\cdots & v_i(\alpha_i^{k-1}+\sum_{t=0}^{2}\eta_{1t}\alpha_i^{k+t}) & \cdots
\end{vmatrix}
$$

$$
=\begin{vmatrix}
\cdots & v_i & \cdots \\
\cdots & v_i\alpha_i & \cdots \\
\vdots & \vdots & \vdots \\
\cdots & v_i\alpha_i^{k-3} & \cdots \\
\cdots & v_i(\alpha_i^{k-2}+\sum_{t=0}^{2}\eta_{0t}\sum_{r=0}^{k-1}g_r^{(t)}\alpha_i^{r}) & \cdots \\
\cdots & v_i(\alpha_i^{k-1}+\sum_{t=0}^{2}\eta_{1t}\sum_{r=0}^{k-1}g_r^{(t)}\alpha_i^{r}) & \cdots
\end{vmatrix}
$$

$$
=\begin{vmatrix}
\cdots & v_i & \cdots \\
\cdots & v_i\alpha_i & \cdots \\
\vdots & \vdots & \vdots \\
\cdots & v_i\alpha_i^{k-3} & \cdots \\
\cdots & v_i\left[(1+\sum_{t=0}^{2}\eta_{0t}g_{k-2}^{(t)})\alpha_i^{k-2}+(\sum_{t=0}^{2}\eta_{0t}g_{k-1}^{(t)})\alpha_i^{k-1}\right] & \cdots \\
\cdots & v_i\left[(1+\sum_{t=0}^{2}\eta_{1t}g_{k-1}^{(t)})\alpha_i^{k-1}+(\sum_{t=0}^{2}\eta_{1t}g_{k-2}^{(t)})\alpha_i^{k-2}\right] & \cdots
\end{vmatrix}
$$

$$
=\begin{vmatrix}
\boldsymbol{I}_{k-2} & 0 & 0 \\
0 & 1+\sum_{t=0}^{2}\eta_{0t}g_{k-2}^{(t)} & \sum_{t=0}^{2}\eta_{0t}g_{k-1}^{(t)} \\
0 & \sum_{t=0}^{2}\eta_{1t}g_{k-2}^{(t)} & 1+\sum_{t=0}^{2}\eta_{1t}g_{k-1}^{(t)}
\end{vmatrix}\prod_{i=1}^{k}v_i\prod_{1\leqslant j<i\leqslant k}(\alpha_i-\alpha_j)
$$

$$
=\begin{vmatrix}
1+\sum_{t=0}^{2}\eta_{0t}g_{k-2}^{(t)} & \sum_{t=0}^{2}\eta_{0t}g_{k-1}^{(t)} \\
\sum_{t=0}^{2}\eta_{1t}g_{k-2}^{(t)} & 1+\sum_{t=0}^{2}\eta_{1t}g_{k-1}^{(t)}
\end{vmatrix}\prod_{i=1}^{k}v_i\prod_{1\leqslant j<i\leqslant k}(\alpha_i-\alpha_j) \tag{1}
$$

注意到,式(1)是否为 0 与 k-子集 I 的选取无关。因此,对于一般的 k-子集 I,$|\boldsymbol{G}_I|\neq 0$ 当且仅当 $\boldsymbol{\eta}\in\Omega$。再由引理 1 可知,TGRS 码 $C_k(\boldsymbol{\alpha},\boldsymbol{v},\boldsymbol{\eta})$ 是 MDS 码当且仅当 $\boldsymbol{\eta}\in\Omega$。

注 1 当 $\boldsymbol{v}=\boldsymbol{I}$ 时,定理 1 给出了 TRS 码 $C_k(\boldsymbol{\alpha},\boldsymbol{I},\boldsymbol{\eta})$ 是 MDS 码的充分必要条件。

下面将利用定理 1 给出 n 较小时构造的 MDS TRS 码。

例 1 令 $\boldsymbol{F}_{17}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$,$\boldsymbol{\alpha}=(1,2,3,5,6,7,8,10)\in\boldsymbol{F}_{17}^{8}$。令 $\boldsymbol{\eta}=\begin{pmatrix}0&0&\eta_{02}\\0&0&\eta_{12}\end{pmatrix}$,其中 $\eta_{ij}\in\boldsymbol{F}_q$,$i=0,1$,$j=0,1,2$。$k\in\{3,4,5,6,7\}$。由引理 2 可知 $\begin{cases}e_1=-c_1\\e_2=c_1^2-c_2\end{cases}$。当 $k=3$ 时,由引理 3 可知

$$\begin{cases} g_{k-2}^{(0)}=-c_2,\ g_{k-2}^{(1)}=-c_3+c_1c_2,\ g_{k-2}^{(2)}=-c_1^2c_2+c_2^2+c_1c_3, \\ g_{k-1}^{(0)}=-c_1,\ g_{k-1}^{(1)}=c_1^2-c_2,\ g_{k-1}^{(2)}=-c_1^3+2c_1c_2-c_3; \end{cases}$$

当 $4\leqslant k\leqslant 7$ 时,由引理 3 可知

$$\begin{cases} g_{k-2}^{(0)}=-c_2,\ g_{k-2}^{(1)}=-c_3+c_1c_2,\ g_{k-2}^{(2)}=-c_1^2c_2+c_2^2+c_1c_3-c_4, \\ g_{k-1}^{(0)}=-c_1,\ g_{k-1}^{(1)}=c_1^2-c_2,\ g_{k-1}^{(2)}=-c_1^3+2c_1c_2-c_3。 \end{cases}$$

利用 Magma 软件计算得到 $n=8$ 时 MDS TRS 码对应的参数 $\boldsymbol{\eta}$ 的个数分布,见表 1。

表 1　F_{17}上参数 $\boldsymbol{\eta}$ 的个数分布表

Table 1　Distribution table of the number of parameters $\boldsymbol{\eta}$ on F_{17}

维数 k	参数 $\boldsymbol{\eta}$ 的个数	MDS 码
3	10	[8,3,6]
4	4	[8,4,5]
5	9	[8,5,4]
6	65	[8,6,3]
7	180	[8,7,2]

仅列出 $k=3$ 时参数 $\boldsymbol{\eta}$ 的所有 10 个取值,

$$\Omega=\left\{\begin{pmatrix}0&0&0\\0&0&0\end{pmatrix},\begin{pmatrix}0&0&1\\0&0&8\end{pmatrix},\begin{pmatrix}0&0&8\\0&0&1\end{pmatrix},\begin{pmatrix}0&0&9\\0&0&7\end{pmatrix},\begin{pmatrix}0&0&12\\0&0&1\end{pmatrix},\begin{pmatrix}0&0&12\\0&0&3\end{pmatrix},\begin{pmatrix}0&0&12\\0&0&13\end{pmatrix},\right.$$
$$\left.\begin{pmatrix}0&0&13\\0&0&15\end{pmatrix},\begin{pmatrix}0&0&15\\0&0&3\end{pmatrix},\begin{pmatrix}0&0&16\\0&0&13\end{pmatrix}\right\}$$

对 $\eta_{ij}(i=0,1,\ j=0,1,2)$赋特殊值可得如下推论。

推论 1　设 $\boldsymbol{\eta}=\begin{pmatrix}0&\eta_2&0\\\eta_1&0&0\end{pmatrix}$,那么 TRS 码 $C_k(\boldsymbol{\alpha},\boldsymbol{I},\boldsymbol{\eta})$是 MDS 码的充分必要条件是 $\boldsymbol{\eta}\in W$,其中 $W=\{(\eta_1,\eta_2):$任意 k-子集 $I\subseteq\{1,2,\cdots,n\}$, $(c_1c_3-c_2^2)\eta_1\eta_2-c_1\eta_1-(c_3-c_1c_2)\eta_2+1\neq 0\}$, $\prod\limits_{i\in I}(x-\alpha_i)=\sum\limits_{l=0}^{k}c_lx^{k-l}$。

推论 2　设 $\boldsymbol{\eta}=\begin{pmatrix}b_{00}&b_{01}&0\\b_{10}&b_{11}&0\end{pmatrix}$,那么 TRS 码 $C_k(\boldsymbol{\alpha},\boldsymbol{I},\boldsymbol{\eta})$是 MDS 码的充分必要条件是 $\boldsymbol{\eta}\in V$,其中 $V=\left\{\begin{pmatrix}b_{00}&b_{01}\\b_{10}&b_{11}\end{pmatrix}:\right.$任意 k-子集 $I\subseteq\{1,2,\cdots,n\}$, $\left.\begin{vmatrix}1+b_{00}g_{k-2}^{(0)}+b_{01}g_{k-2}^{(1)}&b_{00}g_{k-1}^{(0)}+b_{01}g_{k-1}^{(1)}\\b_{10}g_{k-2}^{(0)}+b_{11}g_{k-2}^{(1)}&1+b_{10}g_{k-1}^{(0)}+b_{11}g_{k-1}^{(1)}\end{vmatrix}\neq 0\right\}$,

$\prod\limits_{i\in I}(x-\alpha_i)=\sum\limits_{l=0}^{k}c_lx^{k-l}$, $g_{k-j}^{(t)}=-\sum\limits_{s=0}^{\min\{t,k-j\}}e_{t-s}c_{s+j}$, $1\leqslant j\leqslant 2$, $0\leqslant t\leqslant 2$。

推论 3　设 $\boldsymbol{\eta}=\begin{pmatrix}b_{00}&0&b_{02}\\b_{10}&0&b_{12}\end{pmatrix}$,那么 TRS 码 $C_k(\boldsymbol{\alpha},\boldsymbol{I},\boldsymbol{\eta})$是 MDS 码的充分必要条件是 $\boldsymbol{\eta}\in E$,其中 $E=\left\{\begin{pmatrix}b_{00}&0&b_{02}\\b_{10}&0&b_{12}\end{pmatrix}:\right.$任意 k-子集 $I\subseteq\{1,2,\cdots,n\}$, $\left.\begin{vmatrix}1+b_{00}g_{k-2}^{(0)}+b_{02}g_{k-2}^{(2)}&b_{00}g_{k-1}^{(0)}+b_{02}g_{k-1}^{(2)}\\b_{10}g_{k-2}^{(0)}+b_{12}g_{k-2}^{(2)}&1+b_{10}g_{k-1}^{(0)}+b_{12}g_{k-1}^{(2)}\end{vmatrix}\neq 0\right\}$, $\prod\limits_{i\in I}(x-\alpha_i)=\sum\limits_{l=0}^{k}c_lx^{k-l}$, $g_{k-j}^{(t)}=-\sum\limits_{s=0}^{\min\{t,k-j\}}e_{t-s}c_{s+j}$, $1\leqslant j\leqslant 2$, $0\leqslant t\leqslant 2$。

注 2　推论 1 即为文献[2]的定理 3.3, 推论 2 即为文献[11]的定理 3.3。

注 3　由推论 3 可知,本文构造的三阶 TGRS 码不仅包含了文献[2]和文献[7-10]中的连续一阶和二阶 TGRS 码,还包含了从未被研究过的不连续一阶和二阶 TGRS 码。

3　结论

依据 TRS 码和 TGRS 码单项式等价的相关原理,构造了一类三阶 TGRS 码,并刻画了该类码是 MDS 码的充分必要条件,给出相应实例进行验证。还可以考虑利用多阶 TGRS 码构造 MDS 码。

参考文献:

[1] 金玲飞,孙中华,滕佳明. LCD-MDS 码的几类构造方法[J]. 中国科学(数学),2021,51(10):1463-1484.
JIN Lingfei, SUN Zhonghua, TENG Jiaming. Several construction methods for LCD-MDS codes[J]. Chinese Science (Mathematics), 2021, 51(10):1463-1484.

[2] SUI Junzhen, YUE Qin, LI Xia, et al. MDS, near-MDS or 2-MDS self-dual codes via twisted generalized Reed-Solomon codes[J]. IEEE Transactions on Information Theory, 2022, 68(12):7832-7841.

[3] BEELEN P, PUCHINGER S, ROSENKILDE J S H. Twisted Reed-Solomon Codes[C]// 2017 IEEE International Symposium on Information Theory (ISIT). Aachen: IEEE, 2017:336-340.

[4] BEELEN P,BOSSERT M, PUCHINGER S, et al. Structural properties of twisted Reed-Solomon codes with applications to cryptography[C]//2018 IEEE International Symposium on Information Theory (ISIT). Vail: IEEE, 2018:946-950.

[5] LIU Hongwei, LIU Shengwei. Constructions of MDS twisted Reed-Solomon codes and LCD-MDS codes[J]. Designs, Codes and Cryptography, 2021, 89(9):2051-2065.

[6] HUANG Daitao, YUE Qin, NIU Yongfeng, et al. MDS or NMDS self-dual codes from twisted generalized Reed-Solomon codes[J]. Designs, Codes and Cryptography, 2021, 89(9):2195-2209.

[7] BEELEN P, PUCHINGER S, ROSENKILDE J. Twisted Reed-Solomon codes[J]. IEEE Transactions on Information Theory, 2022, 68(5):3047-3061.

[8] ZHANG Jun, ZHOU Zhengchun, TANG Chunming. A class of twisted generalized Reed-Solomon codes[J]. Designs, Codes and Cryptography, 2022, 90(7):1649-1658.

[9] SUI Junzhen, ZHU Xiaomeng, SHI Xueying. MDS and near-MDS codes via twisted Reed-Solomon codes[J]. Designs, Codes and Cryptography, 2022, 90(8):1937-1958.

[10] GU Haojie, ZHANG Jun. On twisted generalized Reed-Solomon codes with ℓ twists[J]. IEEE Transactions on Information Theory, 2024, 70(1): 145-153.

[11] SUI Junzhen, YUE Qin, SUN Fuqing. New constructions of self-dual codes via twisted generalized Reed-Solomon codes[J]. Cryptography and Communications, 2023, 15:959-978.

[12] HUFFMAN W, PLESS V. Fundamentals of error correcting codes[M]. Cambridge: Cambridge University Press, 2003.

(编辑:陈丽萍)

(上接第86页)

[10] FU Changjian, GENG Shengfei, LIU Pin. Exchange graphs of cluster algebras have the non-leaving-face property[J]. Bulletin of the London Mathematical Society, 2023, 55(4):2062-2069.

[11] 曹培根. $\mathscr{G}$-系统和丛代数[D]. 杭州:浙江大学, 2019.
CAO Peigen. $\mathscr{G}$-systems and cluster algebras[D]. Hangzhou: Zhejiang University, 2019.

[12] FOMIN S, ZELEVINSKY A. Cluster algebras Ⅳ: coefficients[J]. Compositio Mathematica, 2007, 143(1):112-164.

[13] GROSS M, HACKING P, KEEL S, et al. Canonical bases for cluster algebras[J]. Journal of the American Mathematical Society, 2018, 31(2):497-608.

[14] BRÜSTLE T, YANG Dong. Ordered exchange graphs[C]// Advances in representation theory of algebras, EMS Series of Congress Reports, Zürich: European Mathematical Society, 2013:135-193.

[15] NAKANISHI T, ZELEVINSKY A. On tropical dualities in cluster algebras[J]. Contemporary Mathematics, 2012, 565:217-226.

[16] CAO Peigen, LI Fang. The enough g-pairs property and denominator vectors of cluster algebras[J]. Mathematische Annalen, 2020, 377:1547-1572.

(编辑:陈丽萍)