doi: 10.3969/j.issn.0490-6756.2017.05.003

标准 Reed-Solomon 码的错误距离

宋青山[1], 徐小凡[2], 颜丽娟[3]
(1. 四川大学数学学院, 成都 610064; 2. 四川旅游学院, 成都 610100; 3. 78090 部队, 成都 610031)

摘　要: 标准 Reed-Solomon 码的错误距离在其译码过程中发挥着重要作用. 2012 年, Hong 和 Wu 提出了一个著名的错误距离猜想. 本文借助有限域上的二次型理论, 通过计算极大距离可分码的生成矩阵, 推得奇特征有限域 $\boldsymbol{F}_q$ 上一类 $q-4$ 次多项式定义的码字不是标准 Reed-Solomon 码的深洞, 从而部分证明了标准 Reed-Solomon 码的错误距离猜想.

关键词: 标准 Reed-Solomon 码; 错误距离; 二次型; 生成矩阵
中图分类号: O236.2　　**文献标识码**: A　　**文章编号**: 0490-6756(2017)05-0911-06

Error distance of standard Reed-Solomon codes

SONG Qing-Shan[1], *XU Xiao-Fan*[2], *YAN Li-Juan*[3]
(1. College of Mathematics, Sichuan University, Chengdu 610064, China;
2. Sichuan Tourism University, Chengdu 610100, China; 3. 78090 Troops, Chengdu 610031, China)

Abstract: Error distance plays an important role in decoding of the standard Reed-Solomon codes. In 2012, Hong and Wu proposed a famous conjecture of standard Reed-Solomon codes on error distance. In this paper, we show that some polynomials of degree $q-4$ can not define deep holes over finite fields with odd characteristic by using the quadratic form and the generator matrix of maximum distance separable codes. In fact, we partially proved error distance conjecture of standard Reed-Solomon codes.

Keywords: Standard Reed-Solomon codes; Error distance; Quadratic form; Generator matrix
(2010 MSC 11Y16,94B35,94B65)

1　引　言

Reed-Solomon 码是由林肯实验室成员 Reed 和 Solomon 于 1960 年提出的一类重要极大距离可分码. 通常, 基于多项式纠错编码, 采用最大似然译码算法(MLD)译码, 特别是针对标准 Reed-Solomon 码的软件实现高效方便. 在研究中, 一个重要方面是在采用 MLD 算法译码时对于收到的码字 $\boldsymbol{u}$ 如何确定其错误距离 $d(\boldsymbol{u},C)$, 而错误距离问题主要在于确定其界, 达到上界即深洞问题[7], 达到下界即平凡码字问题[8]. 2007 年, Cheng 和 Murry[1] 猜想标准 Reed-Solomon 码的深洞只有码字 $\boldsymbol{u}$ 的拉格朗日插值多项式 $u(x)$ 为 $ax^k+f_{\leqslant k-1}(x)$ 的情形. 2008 年, Li 和 Wan[3] 通过对有限域中子集和的研究分析了 $k+1$ 次多项式对应码字的错误距离. 2012 年, Wu 和 Hong[6] 通过对 Reed-Solomon 码进行离散傅立叶变换, 得到当收到的码字 $\boldsymbol{u}$ 的拉格朗日插值多项式 $u(x)$ 为 $ax^{q-2}+f_{\leqslant k-1}(x)$ 时, $\boldsymbol{u}$ 是标准 Reed-Solomon 码的深洞. 进一步, Wu 和 Hong 猜想, 在特征为奇素数的有限域 $\boldsymbol{F}_q$ 上, 码字 $\boldsymbol{u}$ 为标准 Reed-Solomon 码的深洞当且仅当其拉格朗日插值多项式 $u(x)$ 为 ax^k+

收稿日期: 2017-03-30
基金项目: 四川省教育厅自然科学基金(2016ZB0342)
作者简介: 宋青山 (1984－), 男, 吉林柳河人, 硕士研究生, 主要研究方向为数论与编码理论. E-mail: achisong@163.com
通讯作者: 徐小凡. E-mail: xxfscu@163.com

$f_{\leqslant k-1}(x)$ 或 $ax^{q-2}+f_{\leqslant k-1}(x)$，其中 $a\in \boldsymbol{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\boldsymbol{F}_q$ 上次数不超过 $k-1$ 的多项式. 2016 年，Li 和 Zhu[5] 对 $k+1,k+2$ 次多项式和一类 $q-2,q-3$ 次多项式定义码字的错误距离进行了深入研究，对特征为奇素数和偶素数的有限域进行了全面系统的梳理，其中对 $k+2$ 次多项式情况的研究可以证明在奇特征有限域上 $k+2$ 次多项式对应的码字不是深洞.

本文只讨论特征为奇素数的有限域 $\boldsymbol{F}_q$. 文章是这样组织的. 第 2 节介绍预备知识，第 3 节研究有限域上一类对称二次型的特殊解，第 4 节利用标准 Reed-Solomon 码的生成矩阵证明了在有限域上一类 $q-4$ 次多项式对应的码字不是深洞，即当 $q\geqslant 3^7$，$\lambda\in \boldsymbol{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\boldsymbol{F}_q$ 上次数不超过 $k-1$ 的多项式时，以 $\lambda x^{q-4}+f_{\leqslant k-1}(x)$ 为拉格朗日插值多项式的码字不是有限域 $\boldsymbol{F}_q$ 上标准 Reed-Solomon 码的深洞.

2 预备知识

在本节中，我们给出一些定义和引理.

定义 2.1[1] 设 $\boldsymbol{F}_q$ 是特征为奇素数 p 的有限域. 令集合 $\boldsymbol{F}_q^*=\{a_1,\cdots,a_{q-1}\}$，有限域 $\boldsymbol{F}_q$ 上长度为 $q-1$，维数为 k 的标准 Reed-Solomon 码定义为 $RS_q(\boldsymbol{F}_q^*,k):=\{(f(a_1),\cdots,f(a_{q-1}))\in \boldsymbol{F}_q{}^{q-1}\mid f(x)\in \boldsymbol{F}_q[x],\deg f(x)\leqslant k-1\}$，$RS_q(\boldsymbol{F}_q^*,k)$ 中的元素称为码字.

定义 2.2[6] 设 $\boldsymbol{u}=(u_1,\cdots,u_n)\in \boldsymbol{F}_q^n$，$\boldsymbol{v}=(v_1,\cdots,v_n)\in \boldsymbol{F}_q^n$，定义 $d(\boldsymbol{u},\boldsymbol{v})=\sharp\{i\mid u_i\neq v_i,u_i\in \boldsymbol{F}_q,v_i\in \boldsymbol{F}_q\}$ 为码字 $\boldsymbol{u},\boldsymbol{v}$ 的汉明距离.

定义 2.3[6] 有限域 $\boldsymbol{F}_q$ 上的 $[n,k]_q$ 线性码 C，对于接受到的码字 $\boldsymbol{u}\in \boldsymbol{F}_q^n$，定义 $d(\boldsymbol{u},C)=\min\{d(\boldsymbol{u},\boldsymbol{v})\mid \boldsymbol{v}\in C,\boldsymbol{v}\neq 0\}$ 为码字 $\boldsymbol{u}$ 对于码 C 的错误距离. 显然 $d(\boldsymbol{u},C)=0\Leftrightarrow \boldsymbol{u}\in C$.

定义 2.4[6] 有限域 $\boldsymbol{F}_q$ 上的 $[n,k]_q$ 线性码 C，定义 $\rho(C)=\max\{d(\boldsymbol{u},C)\mid \boldsymbol{u}\in \boldsymbol{F}_q^n\}$ 为码 C 的覆盖半径. 特别地，对于 Reed-Solomon 码有 $\rho(C)=n-k$.

对于标准 Reed-Solomon 码，设收到的码字 $\boldsymbol{u}=(u_1,\cdots,u_{q-1})\in \boldsymbol{F}_q^{q-1}$，$\boldsymbol{F}_q$ 上的拉格朗日插值多项式定义为

$$u(x):=\sum_{i=1}^{q-1}u_i\prod_{j=1,j\neq i}^{q-1}\frac{x-x_j}{x_i-x_j},$$

其中 $u(x_i)=u_i$. 由拉格朗日插值多项式的性质知 $\deg u(x)\leqslant q-2$，又 $\boldsymbol{u}\in C\Leftrightarrow \deg u(x)\leqslant k-1\Leftrightarrow d(\boldsymbol{u},C)=0$.

引理 2.5[3] 设 $\boldsymbol{u}\in \boldsymbol{F}_q^{q-1}$，$k\leqslant \deg u(x)\leqslant q-2$，$C$ 为 $\boldsymbol{F}_q$ 上的长度为 n，维数为 k 的 Reed-Solomon 码，则

$$q-1-\deg(u(x))\leqslant d(\boldsymbol{u},C)\leqslant q-1-k.$$

定义 2.6[10] 设 C 为 $\boldsymbol{F}_q$ 上的长度为 $q-1$，维数为 k 的 Reed-Solomon 码，若 $d(\boldsymbol{u},C)=q-1-k$，称码字 $\boldsymbol{u}$ 为 Reed-Solomon 码的深洞，其中 $u(x)$ 为 $\boldsymbol{u}$ 的拉格朗日插值多项式.

引理 2.7[2] 设 C 为 $\boldsymbol{F}_q$ 上的维数为 k 的 Reed-Solomon 码，$\boldsymbol{u},\boldsymbol{v}\in \boldsymbol{F}_q^n$，若 $u(x)=\lambda v(x)+f_{\leqslant k-1}(x)$，其中 $\lambda\in \boldsymbol{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\boldsymbol{F}_q$ 上次数不超过 $k-1$ 的多项式，$u(x),v(x)$ 分别为码字 $\boldsymbol{u},\boldsymbol{v}$ 的拉格朗日插值多项式，则

$$d(\boldsymbol{u},C)=d(\boldsymbol{v},C).$$

引理 2.8[9] 设 $\boldsymbol{F}_q$ 为特征为 p 的有限域，C 为 $\boldsymbol{F}_q$ 上的 $[n,k]$ MDS 码且其覆盖半径 $\rho=n-k$，则码字 $\boldsymbol{u}\in \boldsymbol{F}_q^n$ 为码 C 的深洞当且仅当 $\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{u}\end{pmatrix}$ 为 MDS 码的生成矩阵. 即 $\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{u}\end{pmatrix}$ 的任意 $k+1$ 列线性无关，其中 $\boldsymbol{G}$ 为码 C 的生成矩阵.

引理 2.9[4] 对任意 $\varepsilon>0$，存在 $c_\varepsilon>0$，当 $m<\varepsilon k^{1/2}$，$4\varepsilon^2\ln^2 q<k\leqslant c_\varepsilon q$ 时，对任意的 $(b_1,\cdots b_m)\in \boldsymbol{F}_q^m$，方程

$$\begin{cases}1+b_1t+\cdots+b_mt^m\equiv\prod\limits_{i=1}^{k}(1+x_it)(\mathrm{mod}\ t^{m+1}),\\ x_i\neq x_j(1\leqslant i\neq j\leqslant k)\end{cases}$$

在 $\boldsymbol{F}_q$ 上有解.

3 特殊二次型在有限域的解

本节借助有限域上的二次型理论，分不同情形研究一类对称二次型的特殊解.

定义 3.1 设 $x\in \boldsymbol{F}_q$，有限域 $\boldsymbol{F}_q$ 的二次特征 $\eta(x)$ 为

$$\eta(x)=\begin{cases}1 & x\in \boldsymbol{F}_q^*,x\text{ 是平方数},\\ -1 & x\in \boldsymbol{F}_q^*,x\text{ 不是平方数},\\ 0 & x=0.\end{cases}$$

设 $f(x)\in \boldsymbol{F}_q[x]$，定义 $\Phi^+(f(x))=\sharp\{x\in \boldsymbol{F}_q\mid \eta(f(x))=1\}$，$\Phi^0(f(x))=\sharp\{x\in \boldsymbol{F}_q\mid \eta(f(x))=0\}$，$\Phi^-(f(x))=\sharp\{x\in \boldsymbol{F}_q\mid \eta(f(x))=-1\}$，$\Phi^{\geqslant 0}(f(x))=\Phi^+(f(x))+\Phi^0(f(x))$.

引理 3.2 设 $c\in \boldsymbol{F}_q^*$，则 $\eta(x^2+c)\geqslant 0\Leftrightarrow$ 存在

$b\in \boldsymbol{F}_q^*$，使得 $x=\dfrac{b-c/b}{2}$.

证明　充分性. 若存在 $b\in \boldsymbol{F}_q^*$，使得 $x=\dfrac{b-c/b}{2}$，则 $x^2+c=(\dfrac{b+c/b}{2})^2$，$\eta(x^2+c)\geqslant 0$.

必要性. 考察关于 b 的方程 $b^2-2xb-c=0$，判别式 $\Delta=4x^2+4c$. 若 $\eta(x^2+c)\geqslant 0$，则 $\eta(\Delta)\geqslant 0$. 所以 $b^2-2xb-c=0$ 作为 b 的方程在 $\boldsymbol{F}_q^*$ 中有解，即存在 $b\in \boldsymbol{F}_q^*$，使得 $x=\dfrac{b-c/b}{2}$.

引理 3.3　当 $\deg(f(x))=1$ 时，$\Phi^{\geqslant 0}(f(x))=(q+1)/2$.

证明　显然 $\Phi^{+}(f(x))=\Phi^{-}(f(x))=(q-1)/2$，$\Phi^{0}(f(x))=1$，所以，$\Phi^{\geqslant 0}(f(x))=(q+1)/2$.

引理 3.4　当 $\deg(f(x))=2$ 时，设 $f(x)=ax^2+bx+c$，其中 $a\in \boldsymbol{F}_q^*$，则

$$\Phi^{\geqslant 0}(f(x))\begin{cases}=1 & b^2-4ac=0,\ \text{且}\ \eta(a)=-1,\\ \geqslant (q-1)/2 & \text{其它}.\end{cases}$$

证明　因为 $a\in \boldsymbol{F}_q^*$，所以

$$\begin{cases}\Phi^{+}(ax^2)=q-1,\ \Phi^{0}(ax^2)=1,\\ \quad \Phi^{-}(ax^2)=0 \quad \eta(a)=1,\\ \Phi^{+}(ax^2)=0,\ \Phi^{0}(ax^2)=1,\\ \quad \Phi^{-}(ax^2)=q-1 \quad \eta(a)=-1.\end{cases}$$

对于 $c,b_1,b_2\in \boldsymbol{F}_q^*$，$\dfrac{b_1-c/b_1}{2}=\dfrac{b_2-c/b_2}{2}\Leftrightarrow (b_1-b_2)(b_1b_2+c)=0\Leftrightarrow b_1b_2=-c$. 因为 q 为奇数，所以 $\boldsymbol{F}_q^*$ 上关于 x 的方程 $x^2=-c$，当 $\eta(-c)=1$ 时，有 2 个解；当 $\eta(-c)=-1$ 时，无解. 由引理 3.2 得

$$\begin{cases}\Phi^{+}(x^2+c)=(q-3)/2,\ \Phi^{0}(x^2+c)=2,\\ \quad \Phi^{-}(x^2+c)=(q-1)/2 \quad \eta(-c)=1,\\ \Phi^{+}(x^2+c)=(q-1)/2,\ \Phi^{0}(x^2+c)=0,\\ \quad \Phi^{-}(x^2+c)=(q+1)/2 \quad \eta(-c)=-1.\end{cases}$$

对于 $a,\ c\in \boldsymbol{F}_q^*$，当 $\eta(a)=1$ 时，$\eta(ax^2+c)=\eta((ax)^2+ac)$，从而 $\Phi^{*}(ax^2+c)=\Phi^{*}((ax)^2+ac)=\Phi^{*}(x^2+ac)$，其中 $*$ 可取 $+,-,0$，所以

$$\begin{cases}\Phi^{+}(ax^2+c)=(q-3)/2,\ \Phi^{0}(ax^2+c)=2,\\ \quad \Phi^{-}(ax^2+c)=(q-1)/2 \quad \eta(-c)=1,\\ \Phi^{+}(ax^2+c)=(q-1)/2,\ \Phi^{0}(ax^2+c)=0,\\ \quad \Phi^{-}(ax^2+c)=(q+1)/2 \quad \eta(-c)=-1.\end{cases}$$

当 $\eta(a)=-1$ 时，$\eta(ax^2+c)=-\eta((ax)^2+ac)$，从而 $\Phi^{*}(ax^2+c)=-\Phi^{*}((ax)^2+ac)=-\Phi^{*}(x^2+ac)$，其中 $*$ 可取 $+,-,0$，所以

$$\begin{cases}\Phi^{+}(ax^2+c)=(q-1)/2,\ \Phi^{0}(ax^2+c)=2,\\ \quad \Phi^{-}(ax^2+c)=(q-3)/2 \quad \eta(-c)=-1,\\ \Phi^{+}(ax^2+c)=(q+1)/2,\ \Phi^{0}(ax^2+c)=0,\\ \quad \Phi^{-}(ax^2+c)=(q-1)/2 \quad \eta(-c)=1.\end{cases}$$

又因为 $ax^2+bx+c=a(x+b/2a)^2-(b^2-4ac)/4a:=ay^2+\delta$，所以 $a\in \boldsymbol{F}_q^*$ 时，

$$\Phi^{\geqslant 0}(ax^2+bx+c)=\Phi^{\geqslant 0}(ay^2+\delta)\begin{cases}=1 & b^2-4ac=0,\ \text{且}\ \eta(a)=-1,\\ \geqslant (q-1)/2 & \text{其它}.\end{cases}$$

综上所述，对于 $f(x)=ax^2+bx+c$，其中 $a\in \boldsymbol{F}_q^*$，

$$\Phi^{\geqslant 0}(f(x))\begin{cases}=1 & b^2-4ac=0,\ \text{且}\ \eta(a)=-1,\\ \geqslant (q-1)/2 & \text{其它}.\end{cases}$$

引理 3.5　设 p 为一奇素数，$q=p^m$，且 $m\geqslant 1$，$q\geqslant 3^7$，若 $3\leqslant t\leqslant q-4$，则方程组

$$\begin{cases}\sum\limits_{i=1}^{t}x_i^2+\sum\limits_{1\leqslant i<j\leqslant t}x_ix_j=0,\\ x_i\neq x_j(1\leqslant i\neq j\leqslant t)\end{cases}\tag{1}$$

在 $\boldsymbol{F}_q^*$ 上有解.

证明　分为 $3\leqslant t\leqslant (q-3)/6$，$q/7<t\leqslant (q-3)/2$，$(q-1)/2\leqslant t\leqslant q-4$ 三种情形进行证明.

情形 1.　当 $3\leqslant t\leqslant (q-3)/6$ 时.

使用归纳法证明. $t=3$ 时，固定 $x_1\in \boldsymbol{F}_q^*$，若存在 $x_2\in \boldsymbol{F}_q^*\backslash\{x_1\}$，使得关于 x 的方程

$$x^2+(x_1+x_2)x+x_1^2+x_2^2+x_1x_2=0\tag{2}$$

在 $\boldsymbol{F}_q^*\backslash\{x_1,x_2\}$ 有解，则命题真. 而(2)式有解，当且仅当判别式 $\Delta(x_2)=(x_1+x_2)^2-4(x_1^2+x_2^2+x_1x_2)=-3x_2^2-2x_1x_2-3x_1^2$ 为一个平方数，即 $\eta(\Delta(x_2))\geqslant 0$，记 $S_{\eta(\Delta(x_2))\geqslant 0}:=\{x_2\in \boldsymbol{F}_q\mid \eta(\Delta(x_2))\geqslant 0\}$. 当 $p=3$ 时，由引理 3.3，$\Phi^{\geqslant 0}(\Delta(x_2))=(q+1)/2$. 当 $p>3$ 时，由引理 3.4，$(-2x_1)^2-36x_1^2\neq 0$，故 $\Phi^{\geqslant 0}(\Delta(x_2))\geqslant (q-1)/2$. 所以，$\sharp S_{\eta(\Delta(x_2))\geqslant 0}\geqslant (q-1)/2$，在 $\boldsymbol{F}_q$ 中至少有 $(q-1)/2$ 个元素 x_2 使得(2)式有解. 另一方面，当 $x=x_i(i=1,2)$ 时，(2)式作为关于 x_2 的方程最多只有两个解，不妨设为 $x_i^{(1)}$，$x_i^{(2)}(i=1,2)$. 当 $(q-1)/2>7$ 时，$\varnothing\neq S_{\eta(\Delta(x_2))\geqslant 0}\backslash\{0,x_1,x_2,x_1^{(1)},x_1^{(2)},x_2^{(1)},x_2^{(2)}\}$，(2)式在 $\boldsymbol{F}_q^*\backslash\{x_1,x_2\}$ 中有解. 因此，$t=3$，$q>15$ 时命题真.

现在假设结论对 $t\geqslant 3$ 时成立. 不妨设 $(x_1,\cdots,x_t)\in \boldsymbol{F}_q^{*t}$ 为(1)式的解，$a:=\sum\limits_{i=1}^{t}x_i$，则 $-a^2=\sum\limits_{i=1}^{t}x_i^2$.

对于 $t+1$ 时，我们只需要找到 $x_t'\in \boldsymbol{F}_q^*\backslash\{x_1,$

$x_2, \cdots, x_{t-1}\}$,使之满足存在 $x \in \boldsymbol{F}_q^* \setminus \{x_1, \cdots, x_{t-1}, x_t'\}$,使得$(x_1, \cdots, x_{t-1}, x_t', x)$为(1)式在 $t+1$ 时的解.此时

$$-(a-x_t+x_t'+x)^2=\sum_{i=1}^{t-1}x_i^2+x_t'^2+x^2=$$
$$-a^2-x_t^2+x_t'^2+x^2, x^2+x(x_t'-x_t+a)+$$
$$x_t'^2+ax_t'-x_tx_t'-ax_t=0 \tag{3}$$
$$\Delta(x_t')=(x_t'-x_t+a)^2-4(x_t'^2+ax_t'-x_tx_t'-$$
$$ax_t)=-3x_t'^2-2(x_t-a)x_t'+(x_t+a)^2.$$

当 $p=3$, $x_t=a$ 时,此时 $x_t \in \boldsymbol{F}_q^*$,所以 $a \neq 0$. (3)式化简为 $x_2+x_t'x+x_t'^2-a^2=0$,解为 $x=x_t' \pm a$,不妨取 $x=x_t'-a$,当 $x=x_i$ 时,$x_t'=x_i+a$, $(i=1, 2, \cdots, t-1)$,所以在 $\boldsymbol{F}_q^* \setminus \{x_1, \cdots, x_t, x_1+a, \cdots, x_{t-1}+a\}$ 中选取 x_t', $x_t'-a$,则$(x_1, \cdots, x_{t-1}, x_t', x_t'-a)$为(1)式在 $t+1$ 时的解,显然这在 $t<(q-1)/2$ 时,总可以做到.

其它时候,$S_{\eta(\Delta(x_t'))\geqslant 0}:=\{x_t' \in \boldsymbol{F}_q \mid \eta(\Delta(x_t'))\geqslant 0\}$,当 $p=3$, $x_t \neq a$ 时,由引理 3.3, $\Phi^{\geqslant 0}(\Delta(x_t'))=(q+1)/2$. 当 $p>3$ 时,由引理 3.4, $4(x_t-a)^2+12(x_t+a)^2=16(x_t^2+ax_t+a^2):=16\delta$,显然 δ 为对称多项式,将 δ 看作 a 的多项式,则 $\delta=0$ 有解,当且仅当 $-3x_t^2$ 为平方数,即 $\eta(-3)=1$,所以 $\eta(-3)=-1$ 和 $\delta=0$ 不能同时成立,故 $\Phi^{\geqslant 0}(\Delta(x_t'))\geqslant(q-1)/2$.

所以,$\sharp S_{\eta(\Delta(x_t'))\geqslant 0}\geqslant(q-1)/2$ 在 $\boldsymbol{F}_q$ 中至少有 $(q-1)/2$ 个元素 x_t' 使得(3)式有解.取 $x=x_i(i=1, 2, \cdots, t-1)$或 $x=x_t'$ 时,(3)式作为关于 x_t' 的方程最多只有两个解,不妨设为 $x_i^{(1)}$, $x_i^{(2)}(i=1, 2, \cdots, t-1)$, $x_t'^{(1)}$, $x_t'^{(2)}$. 当$(q-1)/2>3t+1$ 时, $\varnothing \neq S_{\eta(\Delta(x_t'))\geqslant 0}\setminus\{0, x_1, \cdots, x_t, x_1^{(1)}, x_1^{(2)}, \cdots, x_{t-1}^{(1)}, x_{t-1}^{(2)}, x_t'^{(1)}, x_t'^{(2)}\}$,即 $t<(q-3)/6$ 时对于 $t+1$ 也成立,因此情形 1 时命题真.

情形 2. 当 $q/7<t\leqslant(q-3)/2$ 时.

设 $f(x)=x^{-\frac{14}{x}}$,则 $f'(x)=\dfrac{14f(x)}{x^2}(\ln x-1)$,当 $x\geqslant 3$ 时,$f'(x)>0$,取 $\varepsilon=\sqrt{2}(q^{-14/q}-1/p-1/2)$,则 ε 关于 p, q 严格单调递增,又因为 $f(x)\to 1(x\to+\infty)$,所以 $\varepsilon=\dfrac{\sqrt{2}}{6}(q\to+\infty, p=3)$, $\varepsilon=\dfrac{\sqrt{2}}{2}(q\to+\infty, p\to+\infty)$.

当 $q/7<t\leqslant(q-1)/2$ 时,$\varepsilon\sqrt{t}>\varepsilon\sqrt{q/7}=\sqrt{2q/7}(q^{-14/q}-1/p-1/2)>\sqrt{2q/7}(q^{-14/q}-5/6)$.

所以,当 $q\geqslant 3^7$ 时,$\sqrt{2q/7}(q^{-14/q}-5/6)>2$, $\varepsilon\sqrt{t}>2$;当 $q\geqslant 5^4$ 时,$4\varepsilon^2\ln^2 q<2\ln^2 q<q/7$, $4\varepsilon^2\ln^2 q<q/7$.

根据引理 2.9,取 $m=2$, $\varepsilon=\sqrt{2}(q^{-14/q}-1/p-1/2)$, $c_\varepsilon=1/2$,当 $q/7<t\leqslant(q-1)/2$, $q\geqslant 3^7$ 时,不等式 $m<\varepsilon t^{1/2}$, $4\varepsilon^2\ln^2 q<t\leqslant c_\varepsilon q$ 总是成立,对任意的 a, $b\in\boldsymbol{F}_q$,方程组

$$\begin{cases} a=\sum\limits_{i=1}^{t}x_i, \\ b=\sum\limits_{1\leqslant i<j\leqslant t}x_ix_j, \\ x_i\neq x_j(1\leqslant i\neq j\leqslant t) \end{cases} \tag{4}$$

在 $\boldsymbol{F}_q^t$ 中有解. 当 $q/7<t\leqslant(q-3)/2$, $q\geqslant 3^7$ 时,取 $a=b=0$,对于 $t+1$ 时设$(x_1, \cdots, x_{t+1})$为(4)式在 $\boldsymbol{F}_q^{t+1}$ 中的一个解,不妨设$(x_1, \cdots, x_t)\in\boldsymbol{F}_q^{*t}$,则

$$\sum_{i=1}^{t}x_i^2+\sum_{1\leqslant i<j\leqslant t}x_ix_j=(\sum_{i=1}^{t}x_i)^2-$$
$$\sum_{1\leqslant i<j\leqslant t}x_ix_j=(-x_{t+1})^2+x_{t+1}\sum_{i=1}^{t}x_i=0.$$

此时无论 x_{t+1} 是否为 0,$(x_1, \cdots, x_t)$为(1)式在 $\boldsymbol{F}_q^{*t}$ 中的解,因此情形 2时命题真.

情形 3. 当$(q-1)/2\leqslant t\leqslant q-4$ 时,设 $\boldsymbol{F}_q^*=<\alpha>$, $S\subset\boldsymbol{F}_q^*$, $2\leqslant\sharp S\leqslant q-3$, $S'=\boldsymbol{F}_q^*\setminus S$,则

$$0=\sum_{i=1}^{q-1}\alpha^i=(\sum_{i=1}^{q-1}\alpha^i)^2=\sum_{i=1}^{q-1}\alpha^{2i}+$$
$$2\sum_{1\leqslant i<j\leqslant q-1}\alpha^i\alpha^j=0+2\sum_{1\leqslant i<j\leqslant q-1}\alpha^i\alpha^j,$$
$$0=\sum_{\substack{\alpha_1\in\boldsymbol{F}_q^*,\ \alpha_2\in\boldsymbol{F}_q^*,\\ \alpha_1\neq\alpha_2}}\alpha_1\alpha_2=\sum_{\substack{\alpha_1\in S,\ \alpha_2\in S,\\ \alpha_1\neq\alpha_2}}\alpha_1\alpha_2+$$
$$\sum_{\substack{\beta_1\in S',\ \beta_2\in S',\\ \beta_1\neq\beta_2}}\beta_1\beta_2+\sum_{\alpha\in S,\ \beta\in S'}\alpha\beta.$$

又因为

$$\sum_{\alpha\in S,\ \beta\in S'}\alpha\beta=\sum_{\alpha\in S}\alpha\sum_{\beta\in S'}\beta=\sum_{\alpha\in S}\alpha(0-\sum_{\alpha\in S}\alpha)=$$
$$-(\sum_{\alpha\in S}\alpha^2+2\sum_{\substack{\alpha_1\in S,\ \alpha_2\in S,\\ \alpha_1\neq\alpha_2}}\alpha_1\alpha_2),$$

所以

$$\sum_{\substack{\alpha_1\in S,\ \alpha_2\in S,\\ \alpha_1\neq\alpha_2}}\alpha_1\alpha_2+\sum_{\alpha\in S}\alpha^2=\sum_{\substack{\beta_1\in S',\ \beta_2\in S',\\ \beta_1\neq\beta_2}}\beta_1\beta_2 \tag{5}$$

下面先证 $3\leqslant t\leqslant(q-3)/2$ 时,方程

$$\begin{cases} \sum\limits_{1\leqslant i<j\leqslant t}x_ix_j=0, \\ x_i\neq x_j(1\leqslant i\neq j\leqslant t) \end{cases} \tag{6}$$

在 $\boldsymbol{F}_q^*$ 上有解.对 t 作归纳法.

$t=3$ 时,固定 $x_1\in\boldsymbol{F}_q^*$,若存在 $x_2\in\boldsymbol{F}_q^*\setminus\{x_1\}$ 使得关于 x 的方程

$$(x_1+x_2)x+x_1x_2=0 \tag{7}$$

在 $\boldsymbol{F}_q^*\setminus\{x_1, x_2\}$ 有解，则命题真. 显然 $x=-\dfrac{x_1x_2}{x_1+x_2}$ 满足(7)式. 再将(7)式看作关于 x_2 的方程，当 $x=x_1$，x_2 时，$x_2=-x_1/2$，$-2x_1$. $x_1+x_2=0$ 时，无解，因此如果在 $\boldsymbol{F}_q^*\{x_1, -x_1/2, -2x_1\}$ 选取 x_2，$-\dfrac{x_1x_2}{x_1+x_2}$，则 $(x_1, x_2, -\dfrac{x_1x_2}{x_1+x_2})$ 为(7)式的解，显然在 $q-1\geqslant 5$ 时可以办到，因此 $t=3$，$q\geqslant 6$ 时命题真.

现在假设结论对 $t\geqslant 3$ 时成立，不妨设 $(x_1, \cdots, x_t)\in \boldsymbol{F}_q^{*t}$ 为(6)式的解，$a:=\sum_{i=1}^{t}x_i$，则 $a^2=\sum_{i=1}^{t}x_i^2$.

对于 $t+1$ 时，只需找到 $x_t'\in\boldsymbol{F}_q^*\{x_1, \cdots, x_{t-1}\}$，使之满足存在 $x\in\boldsymbol{F}_q^*\{x_1, \cdots, x_{t-1}, x_t'\}$，使得 $(x_1, \cdots, x_{t-1}, x_t', x)$ 为(6)式在 $t+1$ 时的解即可. 此时

$$(a-x_t+x_t'+x)^2=\sum_{i=1}^{t-1}x_i^2+x_t'^2+x^2=a^2-x_t^2+x_t'^2+x^2.$$

从而

$$x(x_t'-x_t+a)+x_t^2+ax_t'-x_tx_t'-ax_t=0 \tag{8}$$

$$x=\frac{(x_t-x_t')(x_t-a)}{x_t-x_t'-a}.$$

将(8)式看作关于 x_t' 的方程，当 $x=x_t'$ 时，最多有两个解，不妨记为 c_1，c_2，当 $x=x_i$，$(i=1, 2, \cdots, t-1)$ 时，$x_t'=\dfrac{(x_t-x_i)(x_t-a)}{x_t-x_i-a}$.

在 $\boldsymbol{F}_q^*\setminus\{x_1, \cdots, x_t, \dfrac{(x_t-x_1)(x_t-a)}{x_t-x_1-a}, \cdots, \dfrac{(x_t-x_{t-1})(x_t-a)}{x_t-x_{t-1}-a}, c_1, c_2\}$ 中选取 x_t'，$x=\dfrac{(x_t-x_t')(x_t-a)}{x_t-x_t'-a}$，则 $(x_1, \cdots, x_{t-1}, x_t', x)$ 为(6)式在 $t+1$ 时的解. 这在 $q-1\geqslant 2t+1+2$，即 $t\leqslant(q-5)/2$ 时总可以做到. 需注意当 $t=(q-5)/2$ 时，对于 $t+1$ 即 $(q-3)/2$ 的情况也成立. 因此，$3\leqslant t\leqslant(q-3)/2$ 时，(6)式在 $\boldsymbol{F}_q^{*t}$ 中有解. 结合(5)式立即可得在 $(q+1)/2\leqslant t\leqslant q-4$ 时，(1)式在 $\boldsymbol{F}_q^{*t}$ 中有解.

当 $t=(q-1)/2$ 时，取 $x_i=\alpha^{2i}$，$(i=1, 2, \cdots, (q-1)/2)$，因为 $\boldsymbol{F}_q^*=<\alpha>$，所以 $0=\sum_{i=1}^{(q-1)/2}x_i=$

$$\sum_{i=1}^{(q-1)/2}x_i^2=(\sum_{i=1}^{(q-1)/2}x_i)^2=0+2\sum_{1\leqslant i<j\leqslant(q-1)/2}x_ix_j,$$

$$\Rightarrow \sum_{i=1}^{(q-1)/2}x_i^2+\sum_{1\leqslant i<j\leqslant(q-1)/2}x_ix_j=0,$$

$(x_1, \cdots, x_t)$ 为(1)式在 $\boldsymbol{F}_q^{*t}$ 中的解，因此情形 3时，命题真.

综合情形 1～3，引理证毕.

4　主要结果

本节利用标准 Reed-Solomon 码的生成矩阵证明了在奇特征有限域上一类 $q-4$ 次多项式对应的码字不是深洞.

定理 4.1　设 q 为奇数，$q\geqslant 3^7$，$2\leqslant k\leqslant q-6$，$u(x)$ 为码字 $\boldsymbol{u}$ 的拉格朗日插值多项式. 若 $u(x)=\lambda x^{q-4}+f_{\leqslant k-1}(x)$，其中 $\lambda\in\boldsymbol{F}_q^*$，$f_{\leqslant k-1}(x)$ 为 $\boldsymbol{F}_q$ 上次数不超过 $k-1$ 的多项式，则码字 $\boldsymbol{u}$ 不是 $RS_q(\boldsymbol{F}_q^*, k)$ 的深洞.

证明　设 $\boldsymbol{F}_q^*=\{\alpha_1, \cdots, \alpha_{q-1}\}$. 则 $RS_q(\boldsymbol{F}_q^*, k)$ 的生成矩阵为

$$\boldsymbol{G}=\begin{pmatrix}1 & 1 & 1 & \cdots & 1\\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{q-1}\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_{q-1}^2\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_{q-1}^{k-1}\end{pmatrix}.$$

不妨设 $u_{q-4}(x)=x^{q-4}$，则 $\boldsymbol{u}_{q-4}=(\alpha_1^{q-4}, \cdots, \alpha_{q-1}^{q-4})$，取 $\{\beta_1, \cdots, \beta_{k+1}\}\subseteq\boldsymbol{F}_q^*$，下面考虑 $\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{u}_{q-4}\end{pmatrix}$ 的 $k+1$ 阶子方阵

$$\begin{pmatrix}1 & 1 & 1 & \cdots & 1\\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{k+1}\\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \cdots & \beta_{k+1}^2\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ \beta_1^{k-1} & \beta_2^{k-1} & \beta_3^{k-1} & \cdots & \beta_{k+1}^{k-1}\\ \beta_1^{q-4} & \beta_2^{q-4} & \beta_3^{q-4} & \cdots & \beta_{k+1}^{q-4}\end{pmatrix}:=$$

$$(B^0, B^1, \cdots, B^{k-1}, B^{q-4})^T,$$

则

$$\det(B^0, B^1, \cdots, B^{k-1}, B^{q-4})^T=$$

$$\prod_{i=1}^{k+1}\beta_i^{-3}\det(B^3, B^4, \cdots, B^{k+2}, B^0)^T=$$

$$(-1)^k\prod_{i=1}^{k+1}\beta_i^{-3}\det(B^0, B^3, B^4, \cdots, B^{k+2})^T.$$

而

$$\det((B^0, x^0), (B^1, x^1), \cdots, (B^{k+1}, x^{k+1}))^T = \prod_{i=1}^{k+1}(x-\beta_i)\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i) := \sum_{i=0}^{k+1}a_i x^i.$$

考察一次项的系数 a_1 得

$$\det(B^0, B^2, B^3, \cdots, B^{k+1})^T = (-1)^{2+k+2}a_1 = (-1)^{k+4}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\sum_{j=1}^{k+1}\frac{\prod_{i=1}^{k+1}(-\beta_i)}{(-\beta_j)} =$$

$$\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\prod_{j=1}^{k+1}\beta_j\sum_{j=1}^{k+1}\beta_j^{-1}.$$

又因为

$$\det((B^0, x^0), (B^2, x^2), (B^3, x^3), \cdots, (B^{k+2}, x^{k+2}))^T =$$

$$\prod_{i=1}^{k+1}(x-\beta_i)\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\,x\prod_{j=1}^{k+1}\beta_j\Big(\sum_{j=1}^{k+1}\beta_j^{-1}+x^{-1}\Big) := \sum_{i=0}^{k+2}b_i x^i.$$

考察二次项的系数 b_2 得

$$\det(B^0, B^3, B^4, \cdots, B^{k+2})^T = (-1)^{2+k+2}\,b_2 =$$

$$(-1)^{2+k+2}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\prod_{j=1}^{k+1}\beta_j\prod_{j=1}^{k+1}(-\beta_j)\Big(\sum_{1\leqslant i<j\leqslant k+1}\beta_j^{-1}\beta_i^{-1}-\Big(\sum_{j=1}^{k+1}\beta_j^{-1}\Big)^2\Big) =$$

$$\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\prod_{j=1}^{k+1}\beta_j^{\,2}\Big(\sum_{j=1}^{k+1}\beta_j^{-2}+\sum_{1\leqslant i<j\leqslant k+1}\beta_j^{-1}\beta_i^{-1}\Big).$$

所以

$$\det(B^0, B^1, \cdots, B^{k-1}, B^{q-4})^T =$$

$$(-1)^k\prod_{i=1}^{k+1}\beta_i^{-3}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\prod_{j=1}^{k+1}\beta_j^{\,2}\Big(\sum_{j=1}^{k+1}\beta_j^{-2}+\sum_{1\leqslant i<j\leqslant k+1}\beta_j^{-1}\beta_i^{-1}\Big) =$$

$$(-1)^k\prod_{i=1}^{k+1}\beta_i^{-1}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\Big(\sum_{j=1}^{k+1}\beta_j^{-2}+\sum_{1\leqslant i<j\leqslant k+1}\beta_j^{-1}\beta_i^{-1}\Big) :=$$

$$(-1)^k\prod_{i=1}^{k+1}\beta_i^{-1}\prod_{1\leqslant i<j\leqslant k+1}(\beta_j-\beta_i)\Big(\sum_{j=1}^{k+1}\gamma_j^{\,2}+\sum_{1\leqslant i<j\leqslant k+1}\gamma_j\gamma_i\Big).$$

故由引理 3.5 知,当 $q\geqslant 3^7$, $2\leqslant k\leqslant q-6$ 时,存在 $\{\gamma_1, \cdots, \gamma_{k+1}\}\subset \boldsymbol{F}_q^*$ 使得 $\sum_{j=1}^{k+1}\gamma_j^{\,2}+\sum_{1\leqslant i<j\leqslant k+1}\gamma_j\gamma_i=0$,从而有 $\det(B^0, B^1, \cdots, B^{k-1}, B^{q-4})^T=0$,即 $(\boldsymbol{G}\boldsymbol{u}_{q-4})$ 中存在 $k+1$ 列线性相关. 据引理 2.8 知,$\boldsymbol{u}_{q-4}$ 不是 $RS_q(\boldsymbol{F}_q^*, k)$ 的深洞. 又因为 $u(x)=\lambda u_{q-4}(x)+f_{\leqslant k-1}(x)$,从而对于 $1\leqslant i\leqslant q-1$ 有 $u(\alpha_i)=\lambda u_{q-4}(\alpha_i)+f_{\leqslant k-1}(\alpha_i)$,即 $\boldsymbol{u}=\lambda \boldsymbol{u}_{q-4}+f_{\leqslant k-1}$. 由引理 2.7 知,$\boldsymbol{u}$ 不是 $RS_q(\boldsymbol{F}_q^*, k)$ 的深洞. 定理证毕.

参考文献:

[1] Cheng Q, Murray E. On deciding deep holes of Reed-Solomon codes [J]. Mathematics, 2007, 4484: 296.

[2] Hong S, Wu R. On deep holes of generalized Reed-Solomon codes [J]. AIMS Math, 2016, 1: 96.

[3] Li J, Wan D. On the subset sum problem over finite fields [J]. Finite Flelds Th App, 2008, 14: 911.

[4] Li J, Wan D. A new sieve for distinct coordinate counting [J]. Sci China Math, 2010, 53: 2351.

[5] Li Y, Zhu G. On the error distance of extended Reed-Solomon codes [J]. Adv Math Commun, 2016, 10: 413.

[6] Wu R, Hong S. On deep holes of standard Reed-Solomon codes [J]. Sci China Math, 2012, 55: 2447.

[7] 徐小凡, 林宗兵, 许霞. 关于标准 Reed-Solomon 码的深洞猜想的注记[J]. 四川大学学报:自然科学版, 2016, 53: 963.

[8] 徐小凡, 谭千蓉. 关于 Reed-Solomon 码的平凡码字的注记[J]. 四川大学学报:自然科学版, 2014, 51: 7.

[9] Zhuang J, Li J, Cheng Q. On determing deep holes of generalized Reed-Solomon codes [J]. IEEE T Inform Theory, 2016, 62: 199

[10] 郑涛, 吴荣军. 关于 Reed-Solomon 码的深洞的注记[J]. 四川大学学报:自然科学版, 2012, 49: 740.