广义 Reed-Solomon 码的深洞

张俊^{①*}, 符方伟^①, 廖群英^②^① 南开大学陈省身数学研究所, 天津 300071;^② 四川师范大学数学与软件科学学院, 成都 610066

E-mail: zhangjun04@mail.nankai.edu.cn, fwfu@nankai.edu.cn, qunyingliao@sicnu.edu.cn

收稿日期: 2012-01-09; 接受日期: 2013-01-22; * 通信作者

国家重点基础研究发展计划 (973) (批准号: 2013CB834204)、国家自然科学基金 (批准号: 10990011, 61171082, 10990011 和 60872025) 和四川省杰出青年学术技术带头人培育计划 (批准号: 2011JQ0037) 资助项目

摘要 深洞在广义 Reed-Solomon 码的译码中发挥重要的作用. 最近, Wu 和 Hong 通过循环码对于标准 Reed-Solomon 码发现了一类新的深洞. 本文给出一个简洁的方法, 对于一般广义 Reed-Solomon 码给出新的一类深洞. 特别地, 对于标准 Reed-Solomon 码, 我们得到了 Wu 和 Hong 给出的深洞. 对于广义 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$, Li 和 Wan 研究和刻画了 $k+1$ 次多项式定义的深洞, 并且指出这个问题归结为在有限域中的子集和问题. 在偶特征的情形下, 利用他们的方法, 我们对于一些特殊的 Reed-Solomon 码得到了更多一类新的深洞. 此外, 我们研究扩展 Reed-Solomon 码 (即赋值集合为 $D = \mathbb{F}_q$) $k+2$ 次多项式定义的深洞, 并且证明没有 $k+2$ 次多项式定义的深洞.

关键词 编码理论 Reed-Solomon 码 译码 深洞 乘法特征 二次方程**MSC (2010) 主题分类** 94B35, 11C08

1 引言

设 $\mathbb{F}_q$ 是具有 q 个元素的有限域 (特征为 p). 固定子集 $D = \{x_1, x_2, \dots, x_n\} \subseteq \mathbb{F}_q$, 称作赋值集合. 有限域 $\mathbb{F}_q$ 上长度为 n , 维数为 k 的 (广义) Reed-Solomon 码 $C = \text{GRS}_k(\mathbb{F}_q, D)$ 定义如下:

$$\text{GRS}_k(\mathbb{F}_q, D) = \{(f(x_1), \dots, f(x_n)) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \leq k-1\}.$$

C 中的每个元素称为码字. 两种最常见的 Reed-Solomon 码是 $D = \mathbb{F}_q^*$ 或者 $\mathbb{F}_q$. 对于前者 $D = \mathbb{F}_q^*$, 我们称为标准 Reed-Solomon 码. 对于后者 $D = \mathbb{F}_q$, 我们称为扩展 Reed-Solomon 码.

对于每一个向量 (又称为字) $u \in \mathbb{F}_q^n$, 利用 Lagrange 插值公式, 存在次数不高于 $n-1$ 的多项式 $f \in \mathbb{F}_q[x]$ 满足

$$u = u_f = (f(x_1), f(x_2), \dots, f(x_n)).$$

显然, $u_f \in \text{GRS}_k(\mathbb{F}_q, D)$ 当且仅当 $\deg(f) \leq k-1$. 方便起见, 我们记 u_f 为多项式 $f(x)$ 定义的字.

令 C 为有限域 $\mathbb{F}_q$ 上参数为 $[n, k, d]$ 的线性码. 字 $u \in \mathbb{F}_q^n$ 到 C 的错误距离定义为

$$d(u, C) = \min\{d(u, v) \mid v \in C\},$$

其中

$$d(u, v) = \#\{i \mid u_i \neq v_i, 1 \leq i \leq n\}$$

是字 u 与 v 的 Hamming 距离. 错误距离在 Reed-Solomon 的列表译码中有很重要的作用. 对于接收向量 $u \in \mathbb{F}_q^n$, 当错误距离满足 $d(u, C) \leq n - \sqrt{nk}$ 时, Sudan 列表算法^[1] 和 Guruswami-Sudan 列表算法^[2] 分别给出了 u 的多项式时间译码算法. 随着错误距离的增加, 列表译码将变得很复杂.

极大似然译码是编码理论中最重要的译码方法之一: 对于接收向量 $u \in \mathbb{F}_q^n$, 寻找码字 $v \in C$ 使得 $d(u, v) = d(u, C)$. 这个问题的判定本质是计算错误距离 $d(u, C)$. 这是众所周知的 NP- 完全问题^[3]. 对于广义 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$, 我们有引理 1.

引理 1^[4] 对任一多项式 $f \in \mathbb{F}_q[x]$ 满足 $k \leq \deg(f) \leq n - 1$, 我们有

$$n - \deg(f) \leq d(u_f, C) \leq n - k.$$

特别地, 如果 $d(u_f, C) = n - k$, 我们称字 u_f 为一个深洞, 或者称多项式 f 定义了一个深洞. 根据引理 1, 易知 k 次多项式定义的向量都是深洞.

对于扩展 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, \mathbb{F}_q)$, 基于大量的计算结果, Cheng 和 Murray^[5] 猜想 k 次多项式定义的向量为所有的深洞. 理论上, 在 $d = \deg(f) - k$ 很小及 q 与 $d + k$ 相比很大时, 他们对于这些向量 u_f 证明了他们的猜想. 对于低次数多项式 $f(x)$ 定义的向量, Li 和 Wan^[6] 利用 Cheng 和 Wan^[7] 的思想研究了标准 Reed-Solomon 码的错误距离 $d(u_f, C)$. Liao^[8] 推广了 Li 和 Wan^[6] 的结果到更高次数的多项式. 最近, 利用深刻的代数几何, Cafure 等人^[9] 对于 Li 和 Wan^[6] 的结果作了一点改进. Zhu 和 Wan^[10] 对更大一类的向量的纠错距离作出估计, 作为推论得到更多的向量不是深洞.

最近, Wu 和 Hong^[11] 对于标准 Reed-Solomon 码发现了新的一类深洞. 通过离散 Fourier 变换, 他们将标准 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, \mathbb{F}_q^*)$ 看成以下生成多项式生成的循环码:

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{n-k}),$$

其中 α 是域 $\mathbb{F}_q$ 的一个本原元. 这样, 作为循环码, 他们发现两类深洞, 分别为 $a \frac{g(x)}{x - \alpha} + l(x)g(x)$ 和 $a \frac{g(x)}{x - \alpha^{n-k}} + l(x)g(x)$, 其中 $a \in \mathbb{F}_q^*$ 和 $l(x) \in \mathbb{F}_q[x]$ 满足 $\deg(l(x)) \leq k - 1$. 通过 Fourier 逆变换, 后者定义的深洞恰是 k 次多项式定义的深洞, 但是前者是一类新的深洞. 这一类新的深洞对应于由所有多项式 $ux^{q-2} + l(x)$ 定义的向量, 其中 $u \in \mathbb{F}_q^*$ 和 $l(x) \in \mathbb{F}_q[x]$ 满足 $\deg(l(x)) \leq k - 1$.

本文组织如下: 在第 2 节中, 我们研究广义 Reed-Solomon 码的深洞. 基于一个简单的事实, 对于广义 Reed-Solomon 码 ($D \neq \mathbb{F}_q$) 给出一类新的深洞. 第 3 节利用 Li 和 Wan^[6] 对于子集和给出的公式, 在偶特征有限域的情形下, 对于一些特殊的 Reed-Solomon 码给出不同于以上两类的深洞. 在第 4 节中, 我们集中研究扩展 Reed-Solomon 码的深洞, 刻画出可以定义深洞的所有 $k + 2$ 次多项式, 证明这类深洞的存在等价于一类二次方程在有限域 $\mathbb{F}_q$ 上无解. 进而, 我们证明这类二次方程总是有解, 由此证明了没有 $k + 2$ 次多项式定义出的深洞.

2 广义 Reed-Solomon 码一类新的深洞

本节考虑广义 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$. 在 $D \neq \mathbb{F}_q$ 情形下, 除了由 k 次多项式定义出的平凡的深洞, 本节给出一类新的深洞.

在 $D = \mathbb{F}_q^*$ 的情形下, 即标准 Reed-Solomon 码, Wu 和 Hong 考虑它们作为循环码, 给出一类新的深洞 $f = ax^{q-2} + f_{\leq k-1}(x)$ ($a \neq 0$), 其中 $f_{\leq k-1}(x)$ 表示多项式 f 中次数不超过 $k-1$ 的部分. 但是对于一般的赋值集合 $D \neq \mathbb{F}_q^*$, 广义 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$ 不可以看成循环码, 从而他们的方法不再适用. 本节给出一个简单的方法证明了对于任一 $b \notin D$, $f = a(x-b)^{q-2} + f_{\leq k-1}(x)$ ($a \neq 0$) 定义的向量依然是广义 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$ 的深洞.

首先给出一个很重要的引理.

引理 2 设 $\mathbb{F}_q$ 是 q 元素的有限域, $\mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上的多项式环. 对于任何 $D \subsetneq \mathbb{F}_q$, $b \notin D$, 以及任意多项式 $(x-b)^{q-2} - g(x) \in \mathbb{F}_q[x]$ (其中 $g(x)$ 为 $\deg(g(x)) \leq k-1$ 的任一多项式), 则 $a \in D$ 是 $(x-b)^{q-2} - g(x)$ 的根当且仅当 a 是 $1 - (x-b)g(x)$ 的根. 从而, 多项式 $(x-b)^{q-2} - g(x)$ 在 D 中最多有 k 个根.

证明 注意到当 $b \notin D$ 时, 多项式 $(x-b)^{q-2} - g(x)$ 与多项式 $(x-b)^2((x-b)^{q-2} - g(x)) = (x-b) - (x-b)^2g(x)$ 在 D 上有同样的根. 而后者与 $1 - (x-b)g(x)$ 在 D 上有同样的根. 所以多项式 $(x-b)^{q-2} - g(x)$ 和 $1 - (x-b)g(x)$ 在 D 上有同样的根. 但是多项式 $1 - (x-b)g(x)$ 的次数不超过 k , 所以上面三个多项式在 D 上的根的个数都不会超过 k . $\square$

由上面的引理, 我们很容易得到 $\text{GRS}_k(\mathbb{F}_q, D)$ 的新的一类深洞.

定理 3 设 $\mathbb{F}_q$ 是 q 个元素的有限域, $\mathbb{F}_q[x]$ 是 $\mathbb{F}_q$ 上的多项式环. 对于广义 Reed-Solomon 码 $C = \text{GRS}_k(\mathbb{F}_q, D)$, 其中 $D \subsetneq \mathbb{F}_q$ 且 $|D| = n$, 则对任一 $b \notin D$, 多项式 $f = a(x-b)^{q-2} + f_{\leq k-1}(x)$ ($a \in \mathbb{F}_q^*$) 定义了 $\text{GRS}_k(\mathbb{F}_q, D)$ 的一个深洞.

证明 不失一般性, 假设 $D \subseteq \mathbb{F}_q^*$ 及 $b = 0$, 而且只考虑多项式 $f = x^{q-2}$. 根据引理 2, 对于任何次数 $\deg(g(x)) \leq k-1$ 的多项式 $g(x) \in \mathbb{F}_q[x]$, 多项式 $f - g$ 在 D 中最多有 k 个根. 所以, 错误距离满足不等式

$$d(u_f, C) = n - \max_{g \in \mathbb{F}_q[x], \deg(g) \leq k-1} |\{f - g \text{ 的根}\}| \geq n - k.$$

另一方面, 对于任何 k 个元子集 $S \subseteq D$, 设

$$g_S = \frac{1 - a_S \prod_{\gamma \in S} (x - \gamma)}{x}, \quad \text{其中 } a_S = (-1)^k \prod_{\gamma \in S} \gamma^{-1}.$$

于是, $g_S \in \mathbb{F}_q[x]$ 是一个次数为 $k-1$ 的多项式, 并且

$$1 - xg_S(x) = a_S \prod_{\gamma \in S} (x - \gamma)$$

在 D 中有 k 个根. 从引理 2 的证明中知, $f - g_S = x^{q-2} - g_S$ 在 D 中有 k 个根. 所以, $d(u_f, C)$ 达到下界, 即

$$d(u_f, C) = n - k.$$

换言之, 多项式 $f = x^{q-2}$ 定义了 Reed-Solomon 码 $C = \text{GRS}_k(\mathbb{F}_q, D)$ 的新的深洞. $\square$

特别地, 如果取 $D = \mathbb{F}_q^*$, 根据定理 3, 多项式 $f = ax^{q-2} + f_{\leq k-1}(x)$ ($a \in \mathbb{F}_q^*$) 定义出标准 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, \mathbb{F}_q^*)$ 的由 Wu 和 Hong 给出的新的深洞.

3 一些特殊的 Reed-Solomon 码的新的深洞

本节考虑偶特征的有限域 (即 $q = 2^a$, $a \in \mathbb{N}$) 上的 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$. 在这种情形下,

对于一些特殊的 Reed-Solomon 码, 我们给出不同于前面两种的新的深洞. 首先回忆 Li 和 Wan^[6] 刻画的 $k+1$ 次多项式定义的深洞.

设 $f = x^{k+1} - bx^k + f_{\leq k-1}(x) \in \mathbb{F}_q[x]$. 引理 1 告诉我们 $d(u_f, C)$ 有两种选择: $n-k-1, n-k$. 如果 f 不能定义一个深洞, 即 $d(u_f, C) = n-k-1$, 这等价于存在多项式 $g \in \mathbb{F}_q[x]$, $\deg(g) \leq k-1$ 使得

$$x^{k+1} - bx^k + f_{\leq k-1}(x) - g(x) = \prod_{j=1}^{k+1} (x - a_{i_j})$$

对于某个 $(k+1)$ 元子集 $\{a_{i_1}, \dots, a_{i_{k+1}}\} \subseteq D$ 成立. 也就等价于存在 $(k+1)$ 元子集 $\{a_{i_1}, \dots, a_{i_{k+1}}\} \subseteq D$ 使得

$$a_{i_1} + \dots + a_{i_{k+1}} = b.$$

采用 Li 和 Wan^[4] 的记号, 对于任意子集 $D \subseteq \mathbb{F}_q^*$, 设

$$N(t, b, D) = \#\left\{S \subseteq D \mid \sum_{x \in S} x = b, \#S = t\right\}.$$

于是, 多项式 $f = x^{k+1} - bx^k + f_{\leq k-1}(x)$ 定义一个深洞, 当且仅当

$$N(t, b, D) = 0.$$

取 $D = \mathbb{F}_q^*$ 或者 $D = \mathbb{F}_q^* \setminus \{1\}$, Li 和 Wan 计算出 $N(t, b, D)$ 的具体公式.

命题 4^[4] 设 $\mathbb{F}_q$ 是 q 个元素的有限域.

(i) 如果 $D = \mathbb{F}_q^*$, 则

$$N(t, 0, \mathbb{F}_q^*) = \frac{1}{q} \binom{q-1}{t} + (-1)^{t+\lfloor t/p \rfloor} \frac{q-1}{q} \binom{q/p-1}{\lfloor t/p \rfloor}.$$

(ii) 如果 $D = \mathbb{F}_q^* \setminus \{1\}$, 令

$$R_t = -p(-1)^{\lfloor t/p \rfloor} \binom{q/p-2}{\lfloor t/p \rfloor} + (p-1-\langle t \rangle_p)(-1)^{\lfloor t/p \rfloor} \binom{q/p-1}{\lfloor t/p \rfloor},$$

$$M(t, b) = -(-1)^{\lfloor t/p \rfloor} \binom{q/p-2}{\lfloor t/p \rfloor} + \delta_{b,t}(-1)^{\lfloor t/p \rfloor} \binom{q/p-1}{\lfloor t/p \rfloor},$$

其中 $\langle t \rangle_p$ 表示 t 模 p 所得的最小非负剩余, $\delta_{b,t} = 1$ 如果 $\langle b \rangle_p > \langle t \rangle_p$; $\delta_{b,t} = 0$, 其他情形. 于是

$$N(t, b, D) = \frac{1}{q} \binom{q-2}{t} + \frac{1}{q} R_t - (-1)^t M(t, t-b).$$

根据以上公式, 在特征 $p=2$ 和 $q>4$ 时, 很容易计算出: 若 $D = \mathbb{F}_q^*$ 或者 $D = \mathbb{F}_q^* \setminus \{1\}$, 我们有

$$N(q-3, 0, D) = 0.$$

于是, $d(u_f, C) = n-k$. 所以, 对于 Reed-Solomon 码 $\text{GRS}_{q-4}(\mathbb{F}_q, D)$ 我们得到一类新的深洞.

定理 5 设 $\mathbb{F}_q$ 是特征为 2 的有限域, 子集 $D = \mathbb{F}_q^*$ 或者 $D = \mathbb{F}_q^* \setminus \{1\}$. 如果 $q>4$, 那么多项式 $ax^{q-3} + f_{\leq k-1}(x)$ ($a \in \mathbb{F}_q^*$) 定义的向量是 $\text{GRS}_{q-4}(\mathbb{F}_q, D)$ 的深洞.

注 与程歧老师讨论时, 他注意到此时任意 $q-3$ 个元素之和不会为 0, 因为它们在 $\mathbb{F}_q$ 中余下来的元素之和不为 0.

4 $k+2$ 次多项式定义的深洞

本节考虑扩展 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, \mathbb{F}_q)$, 其中有限域 $\mathbb{F}_q$ ($q > 5$) 具有奇特征. 根据引理 1, 对于 $k+2$ 次多项式 $f = x^{k+2} - ax^{k+1} - bx^k + f_{\leq k-1}(x)$, 我们有 $n - k - 2 \leq d(u_f, C) \leq n - k$. 于是, 要使 $d(u_f, C) \leq n - k - 1$, 换言之, f 不会定义一个深洞, 当且仅当存在次数不超过 $k-1$ 的多项式 $g \in \mathbb{F}_q[x]$, $k+1$ 元子集 $S \subseteq \mathbb{F}_q$ 及 $\gamma \in \mathbb{F}_q$ 使得

$$f - g = (x - \gamma) \prod_{\beta \in S} (x - \beta).$$

这样, 我们得到方程组

$$\begin{cases} a = \gamma + \sum_{\beta \in S} \beta, \\ b = - \sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 - \gamma \sum_{\beta \in S} \beta. \end{cases}$$

于是, 我们有下面的引理.

引理 6 多项式 $f = x^{k+2} - ax^{k+1} - bx^k + f_{\leq k-1}(x) \in \mathbb{F}_q[x]$ 不能定义一个深洞当且仅当存在 $k+1$ 元子集 $S \subseteq \mathbb{F}_q$ 以及 $\gamma \in \mathbb{F}_q$ 满足

$$\begin{cases} a = \gamma + \sum_{\beta \in S} \beta, \\ b = - \sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 - \gamma \sum_{\beta \in S} \beta. \end{cases}$$

从上面两个等式, 我们有

$$b = - \sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 - \left(a - \sum_{\beta \in S} \beta\right) \sum_{\beta \in S} \beta.$$

所以, 为寻找所有不能定义深洞的 $k+2$ 次多项式 f , 我们只需要寻找出所有 $a \in \mathbb{F}_q$ 和 $b \in \mathbb{F}_q$ 使得等式

$$\begin{cases} b = - \sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 - \left(a - \sum_{\beta \in S} \beta\right) \sum_{\beta \in S} \beta, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j, \end{cases}$$

对于 $k+1$ 元子集 $S \in F_q$ 成立, 也就等价于关于 $X_1, \dots, X_{k+1}$ 的方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq k+1} X_i X_j + \sum_{i=1}^{k+1} X_i^2 - a \sum_{i=1}^{k+1} X_i, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中有解.

事实上, 我们可以证明对任何 $a, b \in \mathbb{F}_q$, 上面的方程均有解. 令 $t = k+1$, 我们有定理 7.

定理 7 对于任何 $a, b \in \mathbb{F}_q$ 及 $3 \leq t \leq q-2$, 方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2 - a \sum_{i=1}^t X_i, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 有解.

定理的证明比较复杂, 为使文章清晰易读, 我们将在附录 A 中给出证明.

因为 $\deg(f) = k + 2 \leq n - 1 = q - 1$, 我们只考虑 $k \leq q - 3$, 根据定理 7, 我们可得到本节的主要结果.

定理 8 设 $\mathbb{F}_q$ 是奇特征的 q ($q > 5$) 个元素的有限域, $\text{GRS}_k(\mathbb{F}_q, \mathbb{F}_q)$ 是 $\mathbb{F}_q$ 上扩展 Reed-Solomon 码. 则对于任何 $2 \leq k \leq q - 3$, $k + 2$ 次多项式 $f = ux^{k+2} + ax^{k+1} + bx^k + f_{\leq k-1}(x) \in \mathbb{F}_q[x]$ ($u \in \mathbb{F}_q^*$, $a, b \in \mathbb{F}_q$) 定义的向量都不是深洞.

本节的结果在 $k + 2$ 次多项式的层面上支持了 Cheng 和 Murray^[5] 关于扩展 Reed-Solomon 码的深洞的猜想. 而在第 2 节中我们已经看到当赋值集合 D 变小, 对任何 $a \in \mathbb{F}_q \setminus D$, 存在一类新的深洞. 我们猜想: 当赋值集合 D 变小的时候, 广义 Reed-Solomon 码 $\text{GRS}_k(\mathbb{F}_q, D)$ 会有更多的深洞. 前面的结果都是对奇特征有限域而言, 第 3 节中对于偶特征的有限域上的一些特殊的广义 Reed-Solomon 码, 我们发现不同于前面两类的新的深洞.

致谢 感谢万大庆老师和程歧老师有益的讨论.

参考文献

- 1 Sudan M. Decoding of Reed-Solomon codes beyond the error-correction bound. *J Complexity*, 1997, 13: 180–193
- 2 Guruswami V, Sudan M. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans Inform Theory*, 1999, 45: 1757–1767
- 3 Guruswami V, Vardy A. Maximal-likelihood decoding of Reed-Solomon codes is NP-hard. *IEEE Trans Inform Theory*, 2005, 51: 2249–2256
- 4 Li J Y, Wan D Q. On the subset sum problem over finite fields. *Finite Fields Appl*, 2008, 14: 911–929
- 5 Cheng Q, Murray E. On deciding deep holes of Reed-Solomon codes. In: *Lecture Notes in Computer Science*, vol. 4484. Berlin: Springer, 2007, 296–305
- 6 Li J Y, Wan D Q. A new sieve for distinct coordinate counting. *Sci China Math*, 2010, 53: 2351–2362
- 7 Cheng Q, Wan D Q. On the list and bounded distance decodibility of the Reed-Solomon codes. *SIAM J Comput*, 2007, 37: 195–209
- 8 Liao Q Y. On Reed-Solomon codes. *Chin Ann Math Ser B*, 2011, 32: 89–98
- 9 Cafure A, Matera G, Privitelli M. Singularities of symmetric hypersurfaces and an application to Reed-Solomon codes. *ArXiv: 1109.2265v1*, 2012
- 10 Zhu G Z, Wan D Q. Computing error distance of Reed-Solomon codes. In: *Lecture Notes in Comput Sci*, vol. 7287. Berlin: Springer, 2012, 214–224
- 11 Wu R J, Hong S F. On deep holes of standard Reed-Solomon codes. *Sci China Math*, 2012, 55: 2447–2455
- 12 Li J Y, Wan D Q. On error distance of Reed-Solomon codes. *Sci China Ser A*, 2008, 51: 1982–1988

附录

本附录给出定理 7 的证明, 这里只考虑 $q = p > 2$ 为素数且 $q \geq 257$ 的情形. 对于素数 $q < 257$ 时, 可利用计算机直接验证. 而对于一般 q 为素数的方幂情形, 可类似证明. 思路如下.

注意到当有限域 $\mathbb{F}_q$ 的特征 $p \mid (t + 1)$ 时, 引理 A.1 失效. 此时, 将 t 分成三段考虑. 但是当 t 比较小, 比如存在常数 c_1 , 使得 $t < c_1 q$ 时, 类似于引理 A.3 的证明以及定理 7 证明中 (b) 部分的证明仍然有效; 当 t 较大时, 即存在常数 c_2 使 $t > c_2 q$ 时, 由引理 A.2 知, 只需考虑补集合 $\mathbb{F}_q \setminus \{X_1, X_2, \dots, X_t\}$. 最后结合定理 A.7 需要的版本 (取 $c = 1/2$ 以及 [12, 定理 5.3] 中取适当 ϵ), 即可证明定理 7.

首先给出几个引理. 根据下面的引理, 我们把问题化简为 $a = 0$ 的情形.

引理 A.1 对任意 $a, b \in \mathbb{F}_q$, 方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2 - a \sum_{i=1}^t X_i, \\ X_i \neq X_j, \text{ 对所有的 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中有解当且仅当对任意 $\beta \in \mathbb{F}_q$, 方程

$$\begin{cases} \beta = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2, \\ X_i \neq X_j, \text{ 对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中可解.

证明 必要性显然. 只需证明充分性.

对任意给定的 $a, b \in \mathbb{F}_q$, 取 $\beta = \frac{ta^2}{2(t+1)} + b$. 设 $(x_1, x_2, \dots, x_t) \in \mathbb{F}_q^t$ 为方程

$$\begin{cases} \beta = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2, \\ X_i \neq X_j, \text{ 对所有 } i \neq j \end{cases}$$

的解, 取 $c = \frac{a}{t+1}$, 则可得

$$\begin{aligned} & \sum_{1 \leq i < j \leq t} (x_i + c)(x_j + c) + \sum_{i=1}^t (x_i + c)^2 - a \sum_{i=1}^t (x_i + c) \\ &= \sum_{1 \leq i < j \leq t} x_i x_j + \sum_{i=1}^t x_i^2 + ((t+1)c - a) \sum_{i=1}^t x_i - tac + \frac{t(t+1)}{2} c^2 \\ &= b, \end{aligned}$$

即 $(x_1 + c, \dots, x_t + c) \in \mathbb{F}_q^t$ 为方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2 - a \sum_{i=1}^t X_i, \\ X_i \neq X_j, \text{ 对所有 } i \neq j \end{cases}$$

的解. □

引理 A.2 设 $S \subset \mathbb{F}_q$ 且 $2 \leq |S| \leq q-2$, $S' = \mathbb{F}_q \setminus S$, 则

$$\sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 + \sum_{\beta \in S} \beta^2 = \sum_{\{\gamma_1, \gamma_2\} \subset S'} \gamma_1 \gamma_2.$$

证明 注意到

$$0 = \sum_{\{\beta_1, \beta_2\} \subset \mathbb{F}_q} \beta_1 \beta_2 + \sum_{\beta \in \mathbb{F}_q} \beta^2$$

$$\begin{aligned}
&= \left(\sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 + \sum_{\beta \in S} \beta^2 \right) + \left(\sum_{\{\gamma_1, \gamma_2\} \subset S'} \gamma_1 \gamma_2 + \sum_{\gamma \in S'} \gamma^2 \right) + \sum_{\beta \in S, \gamma \in S'} \beta \gamma \\
&= \left(\sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 + \sum_{\beta \in S} \beta^2 \right) + \left(\sum_{\{\gamma_1, \gamma_2\} \subset S'} \gamma_1 \gamma_2 + \sum_{\gamma \in S'} \gamma^2 \right) + \left(\sum_{\gamma \in S'} \gamma \right) \left(- \sum_{\gamma \in S'} \gamma \right) \\
&= \sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 + \sum_{\beta \in S} \beta^2 - \sum_{\{\gamma_1, \gamma_2\} \subset S'} \gamma_1 \gamma_2.
\end{aligned}$$

因此,

$$\sum_{\{\beta_1, \beta_2\} \subset S} \beta_1 \beta_2 + \sum_{\beta \in S} \beta^2 = \sum_{\{\gamma_1, \gamma_2\} \subset S'} \gamma_1 \gamma_2.$$

这就完成了引理 A.2 的证明. □

由引理 A.2, 只需考虑方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

的可解性.

引理 A.3 设 $b \in \mathbb{F}_q$ 且 $2 \leq t \leq \frac{q-1}{2}$, 则方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中有解.

证明 对 t 作归纳证明. 当 $t = 2, 3$ 时直接验证, 可知结论成立.

现在假设结论对 t ($t \geq 3$) 成立, 则对 $t+1$ 时, 由归纳假设知, 可设方程

$$\sum_{1 \leq i < j \leq t} X_i X_j = b$$

有解 $(x_1, x_2, \dots, x_t) \in \mathbb{F}_q^t$, 其中当 $i \neq j$ 时 $x_i \neq x_j$.

若对所有 $1 \leq i \leq t$, 均有 $x_i \neq 0$, 则 $(0, x_1, x_2, \dots, x_t) \in \mathbb{F}_q^{t+1}$ 为方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t+1} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

的解.

否则, 不失一般性不妨假设 $x_1 = 0$. 只需找到 $x'_t \in \mathbb{F}_q \setminus \{x_1, x_2, \dots, x_t\}$ 以及 $x \in \mathbb{F}_q \setminus \{x_1, x_2, \dots, x_{t-1}, x'_t\}$, 使得 $(x_1, x_2, \dots, x_{t-1}, x'_t, x)$ 为如下方程的解即可,

$$\sum_{1 \leq i < j \leq t+1} X_i X_j = b.$$

记 $a = x_1 + x_2 + \cdots + x_t$. 注意到 $t \geq 3$ 时, $(x_1, x_2, \dots, x_t)$ 的任意置换均为方程的解, 不妨假设 $x_t \neq a$. 从而,

$$\begin{cases} a^2 - 2b = \sum_{i=1}^t x_i^2, \\ a = x_1 + \cdots + x_t. \end{cases}$$

由此可得

$$\begin{cases} a^2 - 2x'_t(x_t - x'_t) - (x_t - x'_t)^2 + x^2 - 2b = \sum_{i=1}^{t-1} x_i^2 + (x'_t)^2 + x^2, \\ a - (x_t - x'_t) + x = x_1 + \cdots + x'_t + x, \end{cases}$$

为方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t+1} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中的解, 只需证明存在 $x'_t \in \mathbb{F}_q \setminus \{x_1, \dots, x_t\}$ 以及 $x \in \mathbb{F}_q \setminus \{x_1, x_2, \dots, x_{t-1}, x'_t\}$, 满足

$$(a - (x_t - x'_t) + x)^2 = a^2 - 2x'_t(x_t - x'_t) - (x_t - x'_t)^2 + x^2,$$

即存在

$$x = \frac{(x_t - x'_t)(x_t - a)}{x_t - x'_t - a} \in \mathbb{F}_q^*$$

满足 $x \in \mathbb{F}_q^* \setminus \{x_2, x_3, \dots, x_{t-1}, x'_t\}$. 由

$$x = \frac{(x_t - x'_t)(x_t - a)}{x_t - x'_t - a} = x_i, \quad \text{对某些 } i = 2, 3, \dots, t-1,$$

可知,

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

而由

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

可知最多只有两个解 c_1 和 c_2 . 如此, 可在

$$\mathbb{F}_q^* \setminus \left\{ x_2, \dots, x_t, \frac{(x_t - x_2)(x_t - a)}{x_t - x_2 - a}, \dots, \frac{(x_t - x_{t-1})(x_t - a)}{x_t - x_{t-1} - a}, c_1, c_2 \right\}$$

中任意选取两个元素. 再由条件

$$q - 1 > t - 1 + t - 2 + 2, \quad \text{即 } t \leq \frac{q-1}{2},$$

知可以取到这样的两个元素, 从而我们构造出方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t+1} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中的解, 完成归纳证明. □

下面计算有限域上一个特殊的二次特征和.

引理 A.4 设 q 为奇素数的幂, $\mathbb{F}_q$ 为 q 元有限域. 则对任意 $c \in \mathbb{F}_q$,

$$\left| \sum_{x \in \mathbb{F}_q} \eta(x^2 + c) \right| = \begin{cases} q-1, & c=0, \\ 3, & \eta(-1) = \eta(c) = -1, \\ 1, & \text{否则}, \end{cases}$$

其中 η 是 $\mathbb{F}_q$ 中的二次特征

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

证明 $c=0$ 时结论显然. 现在假设 $c \neq 0$, 易知二次方程 $x^2 + c = y^2$, 即 $(y-x)(y+x) = c$ 恰有 $(q-1)$ 个解

$$\left\{ \left(\frac{b-c/b}{2}, \frac{b+c/b}{2} \right) \mid b \in \mathbb{F}_q^* \right\}.$$

若 $\eta(-1) = \eta(c) = -1$, 则 $-c$ 为平方元素. 从而方程 $x^2 + c = 0$ 有两个解, 因此,

$$\left| \sum_{x \in \mathbb{F}_q} \eta(x^2 + c) \right| = \left| \frac{q-1-2}{2} - \left(q - \frac{q-1-2}{2} \right) + 0 + 0 \right| = 3.$$

其他情形可类似证明. □

由上述引理, 可以计算有限域中在给定仿射映射下的像仍为平方元素的平方元素的个数. 如此, 有限域中的平方元素占一半, 其中将近一半平方元素在某些仿射下的像仍为平方元素.

推论 A.5 设 q 为奇素数的幂, $\mathbb{F}_q$ 为 q 元有限域. 则对任意 $a, c \in \mathbb{F}_q^*$,

$$A = \#\{x \in \mathbb{F}_q \mid x \text{ 和 } ax + c \text{ 均为 } \mathbb{F}_q \text{ 中的平方元素}\} \geq \frac{q-1}{4}.$$

证明 由引理 A.4 可知,

$$\left| \sum_{x \in \mathbb{F}_q} \eta(ax^2 + c) \right| = \left| \sum_{x \in \mathbb{F}_q} \eta(x^2 + ac) \right| = \begin{cases} 3, & \eta(-1) = \eta(ac) = -1, \\ 1, & \text{否则}. \end{cases}$$

记 $m = \#\{x \in \mathbb{F}_q \mid ax^2 + c \text{ 为 } \mathbb{F}_q \text{ 中的平方元素}\}$, 则

$$\left| \sum_{x \in \mathbb{F}_q} \eta(ax^2 + c) \right| = \begin{cases} |m-2-(q-m)|, & \eta(-ac) = -1, \\ |m-(q-m)|, & \eta(-ac) \neq -1. \end{cases}$$

比较上面两个等式, 可得

$$m \geq \frac{q-1}{2}.$$

再由 $A = \frac{m+(\eta(c)+1)/2}{2} \geq \frac{m}{2}$, 立得推论. □

如果只考虑情形 $\frac{q}{7} < t \leq \frac{q-1}{2}$, 此时在文献 [12, 定理 5.3] 中取 $c = 1/2$ 以及 $\epsilon = \sqrt{2}(\frac{1}{q^{14/q}} - \frac{1}{p} - \frac{1}{2})$, 其中 p 为 $\mathbb{F}_q$ 的特征. 则有如下命题.

命题 A.6 设 $q \geq 257$, $\frac{q}{7} < t \leq \frac{q-1}{2}$. 则对任意 $a, b \in \mathbb{F}_q$, 方程组

$$\begin{cases} a = \sum_{i=1}^t X_i, \\ b = \sum_{1 \leq i < j \leq t} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中可解.

定理 A.7 设 $q \geq 257$, $\frac{q}{7} < t < \frac{6q}{7}$. 则对任意 $a, b \in \mathbb{F}_q$, 方程组

$$\begin{cases} a = \sum_{i=1}^t X_i, \\ b = \sum_{1 \leq i < j \leq t} X_i X_j, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中可解.

证明 等价于证明存在两两不同的 $\alpha_1, \alpha_2, \dots, \alpha_t \in \mathbb{F}_q$, 满足

$$1 + ax + bx^2 \equiv \prod_{j=1}^t (1 - \alpha_j x) \pmod{x^3}.$$

由命题 A.6, 只需证明当 $\frac{q+1}{2} \leq t < \frac{6q}{7}$ 时, 对任意 $a, b \in \mathbb{F}_q$, 均存在两两不同的 $\alpha_1, \alpha_2, \dots, \alpha_t \in \mathbb{F}_q$ 使得

$$1 + ax + bx^2 \equiv \prod_{j=1}^t (1 - \alpha_j x) \pmod{x^3},$$

即

$$\frac{1 - x^{q-1}}{1 + ax + bx^2} \equiv \frac{1 - x^{q-1}}{\prod_{j=1}^t (1 - \alpha_j x)} \pmod{x^3}.$$

令

$$\{\beta_1, \beta_2, \dots, \beta_{q-t}\} = \mathbb{F}_q \setminus \{\alpha_1, \alpha_2, \dots, \alpha_t\}.$$

则问题等价于证明存在两两不同的 $\beta_1, \beta_2, \dots, \beta_{q-t} \in \mathbb{F}_q$, 满足

$$\frac{1 - x^{q-1}}{1 + ax + bx^2} \equiv \prod_{j=1}^{q-t} (1 - \beta_j x) \pmod{x^3}.$$

由命题 A.6, 当 $\frac{q}{7} < q-t \leq \frac{q-1}{2}$ 时, 即 $\frac{q+1}{2} \leq t < \frac{6q}{7}$, 这样的 $\beta_1, \beta_2, \dots, \beta_{q-t}$ 是存在的. $\square$

下面证明定理 7.

定理 7 的证明 (a) 由引理 A.1–A.3, 当 $\frac{q+1}{2} \leq t \leq q-2$ 时, 对任意 $a, b \in \mathbb{F}_q$, 方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2 - a \sum_{i=1}^t X_i, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

在 $\mathbb{F}_q$ 中可解.

(b) 当 $3 \leq t < \frac{q-11}{6}$ 时, 对 t 作归纳证明.

对 $t=3$, 固定一个 $x_1 \in \mathbb{F}_q$ 使得 $2x_1^2 - 3b \neq 0$. 只需找到 $x_2 \in \mathbb{F}_q \setminus \{x_1\}$ 满足: 关于 X 的方程

$$X^2 + (x_1 + x_2)X + x_1^2 + x_2^2 + x_1x_2 - b = 0$$

有解 $x_3 \in \mathbb{F}_q \setminus \{x_1, x_2, -x_1 - x_2\}$.

熟知, 上述关于 X 的方程有解当且仅当判别式

$$\Delta = (x_1 + x_2)^2 - 4(x_1^2 + x_2^2 + x_1x_2 - b) = -3x_2^2 - 2x_1x_2 - 3x_1^2 + 4b$$

为 $\mathbb{F}_q$ 中的平方元素. 注意到特征 $p \neq 3$, 因此, 判别式

$$\Delta = -3 \left(x_2 + \frac{x_1}{3} \right)^2 - \frac{8x_1^2}{3} + 4b.$$

记 $x_2(\Delta) = \{x_2 \in \mathbb{F}_q \setminus \{x_1\} \mid \Delta \text{ 为平方元素}\}$. 由 $x_2 \neq x_1$ 以及推论 A.5 可知,

$$|x_2(\Delta)| \geq \left(2 \left(\frac{q-1}{4} - 1 \right) + 1 \right) - 1 = \frac{q-5}{2}.$$

取 $X = x_i$ ($i=1, 2$) 或者 $X = -x_1 - x_2$, 关于 x_2 的方程

$$X^2 + (x_1 + x_2)X + x_1^2 + x_2^2 + x_1x_2 - b = 0$$

最多只有两个解 $x_i^{(1)}, x_i^{(2)}$ 或者 $c^{(1)}, c^{(2)}$.

综合上述, 可以在集合 $x_2(\Delta) \setminus \{x_1^{(1)}, x_1^{(2)}, x_2^{(1)}, x_2^{(2)}, c^{(1)}, c^{(2)}\}$ 中任意取一个元素作为 x_2 . 在假设 $6 < \frac{q-5}{2}$ 之下, 即 $q > 17$, 这是可以办到的.

现在假设结论对于 $t \geq 3$ 时成立. 则对于 $t+1$, 由归纳假设, 可设 $(x_1, x_2, \dots, x_t) \in \mathbb{F}_q^t$ 为方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t} X_i X_j + \sum_{i=1}^t X_i^2, \\ X_i \neq X_j, \quad \text{对所有 } i \neq j \end{cases}$$

的解, 并且 $a = \sum_{i=1}^t x_i \neq 0$. 因此,

$$\begin{cases} 2b - a^2 = \sum_{i=1}^t x_i^2, \\ a = \sum_{i=1}^t x_i. \end{cases}$$

类似引理 A.3 的证明, 可知当 $x_i \neq 0$ ($1 \leq i \leq t$) 时, $(x_1, x_2, \dots, x_t, 0) \in \mathbb{F}_q^t$ 为方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t+1} X_i X_j + \sum_{i=1}^{t+1} X_i^2, \\ X_i \neq X_j, \text{ 对所有 } i \neq j \end{cases}$$

的解. 否则, 不妨假设 $x_t = 0$, 此时可以取适当的元素 $x'_t \in \mathbb{F}_q^*$ 替换 x_t , 使之满足存在 $x \in \mathbb{F}_q$, 使得 $(x_1, x_2, \dots, x'_t, x) \in \mathbb{F}_q^{t+1}$ 为方程

$$\begin{cases} b = \sum_{1 \leq i < j \leq t+1} X_i X_j + \sum_{i=1}^{t+1} X_i^2, \\ X_i \neq X_j, \text{ 对所有 } i \neq j \end{cases}$$

的解, 并且

$$\sum_{i=1}^{t-1} x_i + x'_t + x \neq 0.$$

首先, 选取 $x'_t \in \mathbb{F}_q \setminus \{x_1, \dots, x_t\}$ (下面将会确定), 由归纳假设可知,

$$\begin{cases} 2b - a^2 + (x'_t)^2 + x^2 = \sum_{i=1}^{t-1} x_i^2 + (x'_t)^2 + x^2, \\ a + x'_t + x = x_1 + \dots + x'_t + x. \end{cases}$$

需要确定 $x'_t \in \mathbb{F}_q \setminus \{x_1, \dots, x_t, -a\}$ 使关于 x 的方程

$$(a + x'_t + x)^2 = a^2 - (x'_t)^2 - x^2$$

有解 $x \in \mathbb{F}_q \setminus \{x_1, x_2, \dots, x'_t, -(\sum_{i=1}^{t-1} x_i + x'_t)\}$. 从而方程变为

$$x^2 + (a + x'_t)x + x'_t(a + x'_t) = 0.$$

由此, 可以看出需要限制条件 $x'_t \neq -a$. 否则由 $x'_t = -a$, 上述方程变形为 $x^2 = 0$, 其只有零解 $x = 0$. 因此,

$$\sum_{i=1}^{t-1} x_i + x'_t + x = 0,$$

与之前的归纳假设矛盾.

类似 $t = 3$ 时的证明, 上述关于 x 的方程有解当且仅当判别式

$$\Delta = (a + x'_t)^2 - 4x'_t(a + x'_t) = -3(x'_t)^2 - 2ax'_t + a^2$$

为 $\mathbb{F}_q$ 中的平方元素. 注意到特征 $p \neq 3$, 于是

$$\Delta = -3\left(x'_t + \frac{a}{3}\right)^2 + \frac{4a^2}{3}.$$

记

$$x'_t(\Delta) = \{x'_t \in \mathbb{F}_q^* \mid \Delta \text{ 为平方元素}\}.$$

由 $x'_t \neq 0$ 以及推论 A.5, 我们有

$$|x'_t(\Delta)| \geq \left(2\left(\frac{q-1}{4} - 1\right) + 1\right) - 1 = \frac{q-5}{2}.$$

而关于 x'_t 的方程

$$x^2 + (a + x'_t)x + x'_t(a + x'_t) = 0,$$

对每个 $x = x_i$ ($i = 1, 2, \dots, t-1$), 或者 $x = -(\sum_{i=1}^{t-1} x_i + x'_t)$, 或者 $x = x'_t$ 都最多只有两个解, 分别设为 $x_i^{(1)}, x_i^{(2)}, c^{(1)}, c^{(2)}$, 以及 $(x'_t)^{(1)}, (x'_t)^{(2)}$.

综合上述, 可以在集合

$$x'_t(\Delta) \setminus \{x_1, x_2, \dots, x_t, x_1^{(1)}, x_1^{(2)}, \dots, x_{t-1}^{(1)}, x_{t-1}^{(2)}, (x'_t)^{(1)}, (x'_t)^{(2)}, c^{(1)}, c^{(2)}, -a\}$$

任选一个元素作为 x'_t , 从而完成归纳证明. 因为在假设条件

$$3t + 3 < \frac{q-5}{2}, \quad \text{即 } t < \frac{q-11}{6}$$

之下, 这样的 x'_t 总是存在的.

又因为当 $q \geq 257$ 时, $\frac{q}{7} < \frac{q-11}{6}$. 故由 (a), (b) 和定理 A.7, 本文就完成了定理 7 的证明. $\square$

Deep holes of generalized Reed-Solomon codes

ZHANG Jun, FU FangWei & LIAO QunYing

Abstract Deep holes play an important role in the decoding of generalized Reed-Solomon codes. Recently, Wu and Hong found a new class of deep holes for standard Reed-Solomon codes. In the present paper, we give a simple method to obtain a new class of deep holes for generalized Reed-Solomon codes. In particular, for standard Reed-Solomon codes, we got the new class of deep holes. Li and Wan studied deep holes of generalized Reed-Solomon codes $\text{GRS}_k(\mathbb{F}_q, D)$ and characterized deep holes defined by polynomials of degree $k+1$. They showed that this problem is reduced to be a subset sum problem in finite fields. Using the method of Li and Wan, we obtain some new deep holes for special Reed-Solomon codes over finite fields with even characteristic. Furthermore, we study deep holes of the extended Reed-Solomon code, i.e., $D = \mathbb{F}_q$ and characterize the deep holes defined by polynomials of degree $k+2$. And we show that polynomials of degree $k+2$ can not define deep holes.

Keywords coding theory, Reed-Solomon code, decoding, deep hole, multiplicative character, quadratic equation

MSC(2010) 94B35, 11C08

doi: 10.1360/012012-30