确定广义 Reed-Solomon 码的深洞树及其应用

献给万哲先教授 90 华诞

庄金成, 林东岱*, 吕昌

中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093

E-mail: zhuangjincheng@iie.ac.cn, ddlin@iie.ac.cn, lvchang@iie.ac.cn

收稿日期: 2017-01-20; 接受日期: 2017-06-06; 网络出版日期: 2017-07-07; * 通信作者

国家自然科学基金 (批准号: 61379139, 61502481 和 61672019) 资助项目

摘要 深洞在广义 Reed-Solomon 码译码中有重要的作用. 本文研究广义 Reed-Solomon 码的深洞树及其应用. 首先, 基于 Newton 插值对广义 Reed-Solomon 码的期望深洞树给出了一个显式的刻画. 然后, 应用期望深洞树的结论给出一个限制和集的结果.

关键词 Reed-Solomon 码 深洞树 Newton 插值 限制和集

MSC (2010) 主题分类 94B35, 11C08

1 引言

1.1 基本概念和问题

本文研究广义 Reed-Solomon 码的深洞树及其应用. 首先回顾相关的一些基本概念. 给定一个编码 C . 两个码字之间的 Hamming 距离定义为这两个码字之间不同坐标的个数. 一个接收的向量 u 到给定编码的错误距离是这个向量到所有码字的距离的最大值. C 的最小距离是指任意两个不同的码字之间的距离的最小值, 记为 d_C . C 的覆盖半径是任意一个接收的向量到编码距离的最大值. 一个深洞是指一个错误距离达到覆盖半径的向量. 线性码 $[n, k]_q$ 是最大距离可分码, 如果它达到 Singleton 界, 即 $d = n - k + 1$. 一个线性码可以由生成矩阵给出, 我们用矩阵的行向量表示编码的基底向量.

Reed-Solomon 码是一类重要的线性码. 给定特征为 p 的有限域 $\mathbb{F}_q$, 令 $D = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_q$. 定义在 $\mathbb{F}_q$ 上的长度为 n 、维数为 k 的标准化的广义 Reed-Solomon 码 $RS_q(D, k)$ 为

$$RS_q(D, k) = \{(f(\alpha_1), \dots, f(\alpha_n)) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x], \deg(f) \leq k-1\}.$$

$RS_q(D, k)$ 的编码算法等价于一个线性映射

$$\begin{aligned} \varphi: \mathbb{F}_q^k &\rightarrow \mathbb{F}_q^n, \\ (a_1, \dots, a_k) &\mapsto (f(\alpha_1), \dots, f(\alpha_n)), \end{aligned}$$

英文引用格式: Zhuang J C, Lin D D, Lv C. Determining deep hole trees of generalized Reed-Solomon codes and an application (in Chinese). Sci Sin Math, 2017, 47: 1615–1620, doi: 10.1360/N012017-00014

这里 $f(x) = a_k x^{k-1} + a_{k-1} x^{k-2} + \cdots + a_1 \in \mathbb{F}_q[x]$.

译码问题的困难性不仅影响编码的使用效率, 而且是某些基于编码构造密码方案的基础 (如文献 [1]), 这种方案目前被认为是能够抵抗量子算法攻击 (如文献 [2]) 的候选方案之一. 设计 $\text{RS}_q(D, k)$ 的高效译码算法是一个重要的研究课题. 给定一个接收向量 $u \in \mathbb{F}_q^n$, 如果错误距离小于 $n - \sqrt{nk}$, Sudan [3] 及 Guruswami 和 Sudan [4] 给出的列表解码算法可以在多项式时间内译码. 但是, 对一般的情形, $\text{RS}_q(D, k)$ 的最大似然译码是一个 NP 困难问题 (参见文献 [5]).

$\text{RS}_q(D, k)$ 的最小距离为 $n - k + 1$, 覆盖半径为 $n - k$. u 是一个深洞, 如果 $d(u, \text{RS}_q(D, k)) = n - k$. 下面的问题是, 如何确定 $\text{RS}_q(D, k)$ 的深洞. $\text{RS}_q(D, k)$ 的深洞问题不仅与译码算法有关, 而且与 MDS (maximal distance separable) 猜想有紧密的联系. 给定一个接收向量 $u = (u_1, u_2, \dots, u_n) \in \mathbb{F}_q^n$, 我们构造 Lagrange 插值多项式

$$u(x) = \sum_{i=1}^n u_i \prod_{\substack{j=1 \\ j \neq i}}^n \frac{x - \alpha_j}{\alpha_i - \alpha_j} \in \mathbb{F}_q[x],$$

称一个函数 $u(x)$ 生成一个向量 $u \in \mathbb{F}_q^n$, 如果 $u = (u(\alpha_1), u(\alpha_2), \dots, u(\alpha_n))$. 我们有如下结论:

- (1) 如果 $\deg(u) \leq k - 1$, 那么 $u \in \text{RS}_q(D, k)$, $d(u, \text{RS}_q(D, k)) = 0$;
- (2) 如果 $\deg(u) = k$, 那么文献 [6] 证明了 u 是一个深洞.

称函数 $f(x), g(x) \in \mathbb{F}_q[x]$ 在 $D \subset \mathbb{F}_q$ 上等价, 如果存在 $a \in \mathbb{F}_q^*$ 和次数小于 k 的函数 $h(x)$ 使得 $g(x)$ 和 $af(x) + h(x)$ 在 D 上取值相等.

1.2 相关工作和结果

文献 [7] 提出了如下关于 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞的猜想:

猜想 1.1 [7] 给定特征为 p 的有限域 $\mathbb{F}_q$. 如果 $p \neq 2$ 或者 $p = 2, k \neq q - 3$, 那么 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞 u 满足 $\deg(u) = k$, 其中 $2 \leq k \leq q - 2$.

文献 [8] 提出了如下的关于 $\text{RS}_q(\mathbb{F}_q^*, k)$ 的深洞的猜想:

猜想 1.2 [8] 给定特征为 p 的有限域 $\mathbb{F}_q$. 如果 $p \neq 2$ 或者 $p = 2, k \neq q - 3$, 那么 $\text{RS}_q(\mathbb{F}_q^*, k)$ 的深洞 u 满足下述条件之一:

- (1) $u(x)$ 等价于 x^k ;
- (2) $u(x)$ 等价于 x^{q-2} .

文献 [7] 应用有理点估计证明了一定条件下一些向量不是 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞. 文献 [9] 应用 Weil 指数和估计的结果证明了一定条件下一些向量不是 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞. 文献 [10] 进一步改进了上面的结果. 文献 [11] 应用代数几何的工具证明了一定条件下一些向量不是 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞. 文献 [12] 应用 Weil 指数和估计与关于不同坐标计数的筛法 [13] 证明了一定条件下一些向量不是 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞. 文献 [14] 得到了几类特殊参数下 $\text{RS}_q(\mathbb{F}_q, k)$ 的深洞的结果. 文献 [15] 考察了当收到的向量的次数为特定常数时的深洞问题. 文献 [16] 考察了当赋值集合为 Dickson 多项式像集的深洞问题. 文献 [17] 考察了射影 Reed-Solomon 码的深洞问题. 文献 [18] 通过深洞树研究了 $\text{RS}_q(D, k)$ 的深洞问题, 并且证明了一类参数下的所有深洞都是期望深洞. 文献 [19] 基于 Reed-Solomon 码的 MDS 扩展的结果改进了上面的结果.

给定集合 S , $n \wedge S$ 表示所有 S 中 n 个不同元素的和的集合. 限制和集的估计和利用深洞树确定深洞之间有密切的联系.

本文第 2 节首先给出期望深洞树的一个显式表达式, 所使用的工具为 Newton 插值. 第 3 节应用 $RS_q(D, k)$ 所有深洞均为期望深洞的条件给出一个限制和集的结果.

2 期望深洞树的显式构造

本节给出期望深洞树的一个显式刻画, 所使用的主要工具为 Newton 插值.

2.1 期望深洞树的概念

文献 [18] 定义了 $RS_q(D, k)$ 的深洞树, 包括期望深洞树和完全深洞树, 为此考虑 $\mathbb{F}_q$ 上次数不超过 q 的多项式构成的线性空间, 并且采用了一组混合的基底

$$\left\{ 1, x, \dots, x^{k-1}, \prod_{i=1}^k (x - \alpha_i), \dots, \prod_{i=1}^{q-1} (x - \alpha_i) \right\}.$$

考虑 $D = \{\alpha_1, \dots, \alpha_{k+l}\}$, $1 \leq l \leq q - k - 1$, $D = \mathbb{F}_q \setminus \{\alpha_{k+l+1}, \dots, \alpha_q = 0\}$, 可以证明函数 $f = x^k$, $f_{\alpha_{k+l+i}}(x) = \frac{1}{x - \alpha_{k+l+i}}$ ($1 \leq i \leq q - k - l$) 及其等价函数产生 $RS_q(D, k)$ 的深洞 (参见文献 [6, 8, 14, 18]), 称这些深洞为期望深洞. 进一步给定 $\mathbb{F}_q$ 和 k , 定义期望深洞树如下:

- (1) 根节点为 $c_1 = 1$.
- (2) 期望深洞树共有 $q - k - 1$ 个分支, 分支的深度从 2 到 $q - k$ 不等. 我们记深度 l 的分支为 b_l .
 - (i) 如果 $l = q - k$, 那么 $b_{q-k} = (1, 0, \dots, 0)$;
 - (ii) 如果 $2 \leq l \leq q - k - 1$, 那么 $b_l = (c_{l,1}, \dots, c_{l,l})$, 这里 $f = \frac{1}{x - \alpha_{k+l+1}}$ 在 $D = \{\alpha_1, \dots, \alpha_{k+l}\}$ 等价于

$$c_{l,1} \prod_{i=1}^k (x - \alpha_i) + \dots + c_{l,l} \prod_{i=1}^{k+l-1} (x - \alpha_i).$$

例 2.1 考虑 $p = 11$, $k = 6$. 赋值集合元素排序为 $\alpha_i = i$, $1 \leq i \leq 11$. 对应的期望深洞树见图 1. 在每一层对应的是赋值集合和深洞多项式的系数. 例如, 考虑第二层对应的赋值集合为 $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$, 取 $c_1 = 1$, $c_2 = 4$, 那么对应的多项式 $f = \prod_{i=1}^6 (x - i) + 4 \prod_{i=1}^7 (x - i)$ 生成 $RS_{11}(D, 6)$ 的一个期望深洞.

图 1 $p = 11$, $k = 6$ 对应的期望深洞树

2.2 期望深洞树的显示表达式

文献 [18] 只是指出了期望深洞树的存在性, 下面我们应用 Newton 插值公式给出这类深洞的生成多项式的一个显式表达.

定理 2.2 给定 $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_k, \dots, \alpha_q = 0\}$ 和 k . 期望深洞树共有 $q - k - 1$ 个分支, 每个分支的长度属于 $[2, q - k]$. 节点表达式如下:

(1) $f = x^k$ 在期望深洞树中对应的分支长度为 $q - k$, 对应节点为 $(1, 0, \dots, 0)$;

(2) $f_{\alpha_{k+l+1}}(x) = \frac{1}{x - \alpha_{k+l+1}}$ 在期望深洞树中对应的分支长度为 l , 对应节点为 $(c_{l,1} = 1, c_{l,2}, \dots, c_{l,l})$, 这里

$$c_{l,i} = \frac{\sum_{j=1}^{k+i} \frac{f_{\alpha_{k+l+1}}(\alpha_j)}{\prod_{m=1, m \neq j}^{k+i} (\alpha_m - \alpha_j)}}{\sum_{j=1}^{k+1} \frac{f_{\alpha_{k+l+1}}(\alpha_j)}{\prod_{m=1, m \neq j}^{k+1} (\alpha_m - \alpha_j)}}.$$

证明 应用 Newton 插值, 深洞树中只需要次数大于等于 k 的基底项对应的系数. 假设 $f = x^k$ 在基底 $\{1, x - \alpha_1, \dots, \prod_{j=1}^k (x - \alpha_j), \dots, \prod_{j=1}^{q-1} (x - \alpha_j)\}$ 对应的系数为 $(e_0, e_1, \dots, e_k, 0, \dots, 0)$, 深洞树分支对应 $(e_k, 0, \dots, 0)$, 因为 $e_k \neq 0$, 所以标准化得到 $(1, 0, \dots, 0)$.

下面考虑 $f_{\alpha_{k+l+1}} = \frac{1}{x - \alpha_{k+l+1}}$ 在基底 $\{1, x - \alpha_1, \dots, \prod_{j=1}^k (x - \alpha_j), \dots, \prod_{j=1}^{k+l-1} (x - \alpha_i)\}$ 上对应的系数 $(e_0, e_1, \dots, e_k, \dots, e_{k+l-1})$. 由 Newton 插值公式得

$$e_s = \sum_{j=1}^{s+1} \frac{f_{\alpha_{k+l+1}}(\alpha_j)}{\prod_{m=1, m \neq j}^{s+1} (\alpha_j - \alpha_m)}.$$

深洞树分支对应 $(e_k, \dots, e_{k+l-1})$, 这里 $e_k \neq 0$, 否则限制到 $D = \{\alpha_1, \dots, \alpha_{k+1}\}$ 上不能产生深洞. 将 e_k 标准化为 1, 得到对应的分支 $(1, c_{l,2}, \dots, c_{l,l})$, 其中

$$c_{l,i} = \frac{\sum_{j=1}^{k+i} \frac{f_{\alpha_{k+l+1}}(\alpha_j)}{\prod_{m=1, m \neq j}^{k+i} (\alpha_m - \alpha_j)}}{\sum_{j=1}^{k+1} \frac{f_{\alpha_{k+l+1}}(\alpha_j)}{\prod_{m=1, m \neq j}^{k+1} (\alpha_m - \alpha_j)}}.$$

证毕. □

特别地, 对有限素域的情形, 我们有如下的进一步的结果:

定理 2.3 给定素数 p 和整数 k . $\mathbb{F}_p = \{1, 2, \dots, p\}$, 也就是要求赋值集合按自然顺序排列. 期望深洞树共有 $p - k - 1$ 个分支, 分支的深度从 2 到 $p - k$. 那么期望深洞树表示如下:

(1) $f = x^k$ 在期望深洞树中对应的分支长度为 $p - k$, 对应节点为 $(1, 0, \dots, 0)$;

(2) $f_{k+l+1}(x) = \frac{1}{x - (k+l+1)}$ 在期望深洞树中对应的分支长度为 l , 对应节点为 $(c_{l,1} = 1, c_{l,2}, \dots, c_{l,l})$, 其中 $c_{l,j}^{-1} = A_{l-1}^{j-1} = (l-1) \cdots (l-j+1)$, $2 \leq j \leq l$.

证明 因为 $f = x^k$ 的表达式是显然的, 下面只需要考虑 $f_{k+l+1}(x) = \frac{1}{x - (k+l+1)}$ ($2 \leq l \leq p - k - 1$) 的情形, 此时分支深度为 l . 为此只需要证明对于给定的 $1 \leq m \leq l - 1$, 有

$$c_{l,m} \equiv (l - m)c_{l,m+1} \pmod{p}. \quad (2.1)$$

同余式 (2.1) 等价于

$$\sum_{j=1}^{k+m} \frac{f_{k+l+1}(j)}{\prod_{i=1, i \neq j}^{k+m} (j - i)} \equiv (l - m) \sum_{j=1}^{k+m+1} \frac{f_{k+l+1}(j)}{\prod_{i=1, i \neq j}^{k+m+1} (j - i)} \pmod{p},$$

即

$$\sum_{j=1}^{k+m+1} \frac{1}{\prod_{i=1, i \neq j}^{k+m+1} (j-i)} \equiv 0 \pmod{p}. \quad (2.2)$$

令 $f = 1$ 为常值函数, 则同余式 (2.2) 左边为 f 在 Newton 基底下对应 $\prod_{i=1}^{k+m}(x-i)$ 的系数, 从而为零. 从而同余式 (2.1) 成立, 得证. $\square$

例 2.4 考虑与例 2.1 中相同的参数, 在图 1 中 $f_{11} = \frac{1}{x}$ 对应的分支为 $(c_{4,1}, c_{4,2}, c_{4,3}, c_{4,4}) = (1, 4, 2, 2)$, 则有 $c_{4,1} \equiv (4-1)c_{4,2} \pmod{11}$, $c_{4,2} \equiv (4-2)c_{4,3} \pmod{11}$, $c_{4,3} \equiv (4-3)c_{4,4} \pmod{11}$.

3 期望深洞结论的一个应用

一般情形下, $\text{RS}_q(D, k)$ 除了期望深洞外还有其他的一些深洞. Zhuang 等^[18] 证明了一定条件下 $\text{RS}_p(D, k)$ 的所有深洞为期望深洞, 证明用到了关于限制和集的估计. 基于一般有限域的 $\text{RS}_q(D, k)$ 的深洞全部为期望深洞的结果, 我们给出一个限制集合求和的结论.

3.1 $\text{RS}_{p(D,k)}$ 深洞全为期望深洞的条件

Zhuang 等^[18] 证明了在特定参数 p 和 k 下所有的深洞都是期望深洞.

定理 3.1^[18] 假设 $p > 2$ 是一个素数, $k \geq \frac{p-1}{2}$, $D = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 并且 $k < n \leq p$, 那么 $\text{RS}_q(D, k)$ 仅有期望深洞.

文献 [19] 基于 Reed-Solomon 码的 MDS 扩展推广了上述结论.

定理 3.2^[19] 给定 $\mathbb{F}_q$, $k \geq \frac{q-1}{2}$, 这里 $\mathbb{F}_q$ 是一个特征为 p 的有限域.

(1) 若 $p \neq 2$ 或者 $p = 2$, $|D| \neq k + 3$, 则 $\text{RS}_q(D, k)$ 的所有深洞为期望深洞;

(2) 若 $p = 2$, $|D| = k + 3$, 则 $\text{RS}_q(D, k)$ 除了期望深洞还有 $f = x^{k+1} + (\sum_{\alpha \in D} \alpha)x^k$ 生成的深洞.

3.2 利用深洞结果给出限制和集的一个结论

在定理 3.1 的证明中用到了下面的关于限制和集的结论.

引理 3.3^[20, 21] 令 $\mathbb{F}$ 为一个特征为 p 的有限域, n 为一个正整数. 对于子集合 $S \subset \mathbb{F}$, 有

$$|n \wedge S| \geq \min\{p, n|S| - n^2 + 1\}.$$

反过来, 我们可以由定理 3.2 给出一个关于限制和集的结论.

定理 3.4 给定 $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$, $k \geq \frac{q-1}{2}$, 这里 $\mathbb{F}_q$ 是一个特征为 p 的有限域. 令

$$D_d = \{\alpha_1, \dots, \alpha_{k+d}\} \subset \mathbb{F}_q,$$

固定元素 $\delta \in \mathbb{F}_q \setminus D_d$, 定义集合 $S = \{\frac{1}{\delta - \beta_i} \mid \beta_i \in D_d\}$. 如果 $p \neq 2$ 或者 $p = 2$, $|D| \neq k + 3$, 那么 $k \wedge S = \mathbb{F}_q$.

证明 定理 3.1 证明过程说明, 如果 $D_{d+1} = \{\alpha_1, \dots, \alpha_{k+d}, \delta\}$, 那么 $f = \frac{1}{x-\delta}$ 不产生 $\text{RS}_q(D_{d+1}, k)$ 的充要条件是, $\forall \gamma \in \mathbb{F}_q$, $\exists \{\beta_1, \dots, \beta_k\} \subset D_d$, 使得 $\sum_{i=1}^k \frac{1}{\delta - \beta_i} = \gamma$. 因为定理 3.2 成立, 故定理得证. $\square$

注 3.5 能否采用类似定理 3.1 的方法, 结合深洞树与限制和集的结论证明定理 3.2 仍然是一个公开问题.

参考文献

- 1 McEliece R J. A Public-key Cryptosystem Based on Algebraic Coding Theory. The Deep Space Network Progress Report 42-44. 1978, 44: 114-116
- 2 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of Foundations of Computer Science. Santa Fe: IEEE, 1994, 124-134
- 3 Sudan M. Decoding of Reed-Solomon codes beyond the error-correction bound. J Complexity, 1997, 13: 180-193
- 4 Guruswami V, Sudan M. Improved decoding of Reed-Solomon and algebraic-geometry codes. IEEE Trans Inform Theory, 1999, 45: 1757-1767
- 5 Guruswami V, Vardy A. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. IEEE Trans Inform Theory, 2005, 51: 2249-2256
- 6 Li J Y, Wan D Q. On the subset sum problem over finite fields. Finite Fields Appl, 2008, 14: 911-929
- 7 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
- 8 Wu R J, Hong S F. On deep holes of standard Reed-Solomon codes. Sci China Math, 2012, 55: 2447-2455
- 9 Li J Y, Wan D Q. On error distance of Reed-Solomon codes. Sci China Ser A, 2008, 51: 1982-1988
- 10 Liao Q Y. On Reed-Solomon codes. Chin Ann Math Ser B, 2011, 32: 89-98
- 11 Cafure A, Matera G, Privitelli M. Singularities of symmetric hypersurfaces and an application to reed-solomon codes. Adv Math Commun, 2012, 6: 69-94
- 12 Zhu G Z, Wan D Q. Computing error distance of Reed-Solomon codes. In: Lecture Notes in Computer Science, vol. 7287. Berlin: Springer, 2012, 214-224
- 13 Li J Y, Wan D Q. A new sieve for distinct coordinate counting. Sci China Math, 2010, 53: 2351-2362
- 14 张俊, 符方伟, 廖群英. 广义 Reed-Solomon 码的深洞. 中国科学: 数学, 2013, 43: 727-740
- 15 Li Y J, Zhu G Z. On error distance of received words with fixed degrees to Reed-Solomon code. ArXiv:1508.02804, 2015
- 16 Ketı M, Wan D Q. Deep holes in Reed-Solomon codes based on Dickson polynomials. Finite Fields Appl, 2016, 40: 110-125
- 17 Zhang J, Wan D Q. On deep holes of projective Reed-Solomon code. ArXiv:1605.02423, 2016
- 18 Zhuang J C, Cheng Q, Li J Y. On determining deep holes of generalized reed-solomon codes. IEEE Trans Inform Theory, 2016, 62: 199-207
- 19 Kaipa K. Deep holes and MDS extensions of Reed-Solomon code. IEEE Trans Inform Theory, 2017, in press
- 20 Da Silva J A, Hamidoune Y O. Cyclic spaces for grassmann derivatives and additive theory. Bull Lond Math Soc, 1994, 26: 140-146
- 21 Alon N, Nathanson M B, Ruzsa I Z. The polynomial method and restricted sums of congruence classes. J Number Theory, 1996, 56: 404-417

Determining deep hole trees of generalized Reed-Solomon codes and an application

ZHUANG JinCheng, LIN DongDai & LV Chang

Abstract Deep holes play an important role in decoding generalized Reed-Solomon codes. In this paper, we consider determining deep hole trees of generalized Reed-Solomon codes and its applications. Firstly, we describe expected deep holes of generalized Reed-Solomon codes in an explicit way based on Newton interpolation. Then, we apply conclusions about expected deep holes to give a result on restricted sumset.

Keywords Reed-Solomon codes, expected deep hole tree, Newton interpolation, restricted sumset

MSC(2010) 94B35, 11C08

doi: 10.1360/N012017-00014