On Determining Deep Holes of Generalized Reed-Solomon Codes

Jincheng Zhuang, Qi Cheng and Jiyou Li

***Abstract*—For a linear code, deep holes are defined to be vectors that are further away from codewords than all other vectors. The problem of deciding whether a received word is a deep hole for generalized Reed-Solomon codes is proved to be co-NP-complete by Guruswami and Vardy. For the extended Reed-Solomon codes $RS_q(\mathbb{F}_q, k)$, a conjecture was made to classify deep holes by Cheng and Murray. Since then efforts have been made to prove the conjecture, or its various forms. In this paper, we classify deep holes completely for generalized Reed-Solomon codes $RS_p(D, k)$, where p is a prime, $|D| > k \geqslant \frac{p-1}{2}$. Our techniques are built on the idea of deep hole trees, and several results concerning the Erdös-Heilbronn conjecture.**

***Index Terms*—Reed-Solomon codes, deep hole, Erdös-Heilbronn conjecture, MDS conjecture.**

I. Introduction

REED-SOLOMON codes are of special interest and importance both in theory and practice of error-correcting.

Definition 1: Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p. Let $D = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q$ be the evaluation set and $v_i \in \mathbb{F}_q^*, 1 \leqslant i \leqslant n$, be the column multipliers. The set of codewords of the generalized Reed-Solomon code $RS_q(D, k)$ of length n and dimension k over $\mathbb{F}_q$ is defined as

$$RS_q(D,k) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x], \deg(f) \leqslant k-1\}.$$

We will write generalized Reed-Solomon codes as GRS codes for short. If $D = \mathbb{F}_q^*$, it is called *primitive*. If $D = \mathbb{F}_q$, it is called *singly-extended*. A GRS code is called *normalized* if its column multipliers are all equal to 1. In this paper, we will work on normalized GRS codes without loss of generality.

The encoding algorithm of the GRS code can be described by the linear map $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$, in which a message $(a_1, \ldots, a_k)$ is mapped to a codeword $(f(\alpha_1), \ldots, f(\alpha_n))$, where $f(x) = a_k x^{k-1} + a_{k-1} x^{k-2} + \cdots + a_1 \in \mathbb{F}_q[x]$.

The research was partially supported by NSFC under Grant 61502481, Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06010701 for J. Zhuang, by China 973 Program under Grant 2013CB834201 and by US NSF under Grant CCF-1409294 for Q. Cheng, and by Ky and Yu-Fen Fan Fund Travel Grant from the AMS and by Shanghai NSF under Grant 13ZR1422500 for J. Li. The material in this paper was presented in part at the 24th International Symposium on Algorithms and Computation (ISAAC 2013).

J. Zhuang is with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: zhuangjincheng@iie.ac.cn).

Q. Cheng is with the School of Computer Science, University of Oklahoma, Norman, OK, 73019 USA (e-mail: qcheng@cs.ou.edu).

J. Li is with the Department of Mathematics, Shanghai Jiao Tong University, Shanghai, China (e-mail: lijiyou@sjtu.edu.cn).

The *Hamming distance* between two words (vectors) is the number of their distinct coordinates. The *error distance* of a received word $u \in \mathbb{F}_q^n$ to the code is defined as its minimum Hamming distance to codewords. The *minimum distance* of a code, which is denoted by d, is the smallest distance between any two distinct codewords of the code. The *covering radius* of a code is the maximum distance from any vector in $\mathbb{F}_q^n$ to the nearest codeword. A *deep hole* is a vector achieving the covering radius. A linear code $[n, k]_q$ is called *maximum distance separable* (in short, MDS) if it attains the *Singleton bound*, i.e., $d = n-k+1$. GRS code is a linear MDS code, and its minimum distance is known to be $n-k+1$ and the covering radius is $n-k$. Thus for the GRS code, u is a deep hole if $d(u, RS_q(D,k)) = n-k$. A linear code can be represented by a generator matrix. In this paper, we assume that the rows of a generator matrix form a basis for the code.

A. Related work

Efforts have been made to obtain an efficient decoding algorithm for GRS codes. Given a received word $u \in \mathbb{F}_q^n$, if the error distance is smaller than $n - \sqrt{nk}$, then the list decoding algorithm of Sudan [18] and Guruswami-Sudan [8] solves the decoding in polynomial time. However, in general, the maximum likelihood decoding of GRS codes is NP-hard [9].

We would like to determine all the deep holes of the code. To this end, given a received word $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$, we consider the following Lagrange interpolating polynomial

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

where $D = \{\alpha_1, \ldots, \alpha_n\}$ is the evaluation set. The Lagrange interpolating polynomial is the unique polynomial in $\mathbb{F}_q[x]$ of degree less than n that satisfies $u(\alpha_i) = u_i, 1 \leqslant i \leqslant n$. In this paper, we say that a function $u(x)$ *generates* a vector $u \in \mathbb{F}_q^n$ if $u = (u(\alpha_1), u(\alpha_2), \ldots, u(\alpha_n))$. We have the following conclusions:

1) If $\deg(u) \leqslant k-1$, then $u \in RS_q(D,k)$ by definition and $d(u, RS_q(D,k)) = 0$.
2) If $\deg(u) = k$, then it can be shown that u is a deep hole by the following proposition [10], i.e., $d(u, RS_q(D,k)) = n-k$.

Proposition 1: ([10]) For $k \leqslant \deg(u) \leqslant n-1$, we have the inequality

$$n - \deg(u) \leqslant d(u, RS_q(D,k)) \leqslant n-k.$$

When the degree of $u(x)$ becomes larger than k, the situation becomes complicated for GRS codes. However, in the case of singly-extended GRS codes, the situation seems to be much simpler. Cheng and Murray [5] conjectured in 2007 that the vectors generated by polynomials of degree k are the only possible deep holes.

Conjecture 1: ([5]) A word u is a deep hole of $RS_q(F_q, k)$ if and only if $\deg(u) = k$.

There is an analogous conjecture for deep holes of primitive Reed-Solomon codes by Wu and Hong [22].

Conjecture 2: ([22]) A word u is a deep hole of $RS_q(F_q^*, k)$ if and only if:

$$u(x) = ax^k + f_{\leqslant k-1}(x), a \neq 0;$$

or

$$u(x) = bx^{q-2} + f_{\leqslant k-1}(x), b \neq 0;$$

where $f_{\leqslant k-1}(x)$ denotes a polynomial with degree not larger than $k-1$.

Cheng and Murray [5] proved the following result by reducing the deep hole problem to the existence of rational points on a hypersurface over $\mathbb{F}_q$.

Theorem 1: ([5]) Let $u \in \mathbb{F}_q^q$ such that $1 \leqslant \Delta := \deg(u) - k \leqslant q-1-k$. If $q \geqslant \max(k^{7+\epsilon}, \Delta^{\frac{13}{3}+\epsilon})$ for some constant $\epsilon > 0$, then u is not a deep hole.

Following a similar approach of Cheng-Wan [6], Li and Wan [12] improved the above result with Weil's character sum estimate.

Theorem 2: ([12]) Let $u \in \mathbb{F}_q^q$ such that $1 \leqslant \Delta := \deg(u) - k \leqslant q-1-k$. If

$$q > \max((k+1)^2, \Delta^{2+\epsilon}), k > (\frac{2}{\epsilon}+1)\Delta + \frac{8}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then u is not a deep hole.

Then Liao [14] proved the following result:

Theorem 3: ([14]) Let $r \geqslant 1$ be an integer. For any received word $u \in \mathbb{F}_q^q, r \leqslant \Delta := \deg(u) - k \leqslant q-1-k$, if

$$q > \max(2\binom{k+r}{2} + \Delta, \Delta^{2+\epsilon}), k > (\frac{2}{\epsilon}+1)\Delta + \frac{2r+4}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then $d(u, RS_q(\mathbb{F}_q, k)) \leqslant q-k-r$, which implies that u is not a deep hole.

Cafure, Matera and Privitelli[4] proved the following result with tools from algebraic geometry:

Theorem 4: ([4]) Let $u \in \mathbb{F}_q^q$ such that $1 \leqslant \Delta := \deg(u) - k \leqslant q-1-k$. If

$$q > \max((k+1)^2, 14\Delta^{2+\epsilon}), k > (\frac{2}{\epsilon}+1)\Delta,$$

for some constant $\epsilon > 0$, then u is not a deep hole.

Using Weil's character sum estimate and Li-Wan's new sieve [11] for distinct coordinates counting, Zhu and Wan [24] showed the following result:

Theorem 5: ([24]) Let $r \geqslant 1$ be an integer. For any received word $u \in \mathbb{F}_q^q, r \leqslant \Delta := \deg(u) - k \leqslant q-1-k$, there are positive constants c_1 and c_2 such that if

$$d < c_1 q^{1/2}, (\frac{\Delta + r}{2} + 1)\log_2(q) < k < c_2 q,$$

then $d(u, RS_q(\mathbb{F}_q, k)) \leqslant q-k-r$, which implies that u is not a deep hole.

Recently, Wan and Keti [20] obtained some new results about deep holes of Reed-Solomon codes based on Dickson polynomials. Li and Zhu [13] found some new families of deep holes by reducing the task to solving certain systems of equations over finite fields.

The deep hole problem for Reed-Solomon codes is also closely related to the famous MDS conjecture in coding theory. On one hand, GRS codes are MDS codes. On the other hand, it is known that all long enough MDS codes are essentially GRS codes. Following the notation of [15], let $N_{\min}(k, q)$ be the minimal integer, if any, such that every $[n, k]$ MDS code over $\mathbb{F}_q$ with $n > N_{\min}(k, q)$ is GRS and be $q+2$ if no such integer exists. For the case of $k = 3$, Segre [16] obtained the following result:

Theorem 6: ([16]) If q is odd, every $[n, 3]$ MDS code over $\mathbb{F}_q$ with $q - \frac{\sqrt{q}-7}{4} < n \leqslant q+1$ is GRS.

When $q = p$ is a prime, Voloch [19] obtained the following result:

Theorem 7: ([19]) If p is an odd prime number, every $[n, 3]$ MDS code over $\mathbb{F}_p$ with $p - \frac{p}{45} + 2 < n \leqslant p+1$ is GRS.

Further, there is a relation for $N_{\min}(k+1, q)$ and $N_{\min}(k, q)$ [15] as follows:

Lemma 1: ([15]) For $3 \leqslant k \leqslant q-2$, we have

$$N_{\min}(k+1, q) \leqslant N_{\min}(k, q) + 1.$$

Ball [2] showed the following result:

Theorem 8: [2] Let S be a set of vectors of the vector space $\mathbb{F}_q^k$, with the property that every subset of S of size k is a basis. If $|S| = q+1$ and $k \leqslant p$ or $3 \leqslant q-p+1 \leqslant k \leqslant q-2$, where p is the characteristic of $\mathbb{F}_q$, then S is equivalent to the following set:

$$\{(1, \alpha, \alpha^2, \ldots, \alpha^{k-1}) \mid \alpha \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\}.$$

B. Our result

In this paper, we classify the deep holes in many cases. Firstly, we show:

Theorem 9: Let $p > 2$ be a prime number, $k \geqslant \frac{p-1}{2}, D = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ with $k < n \leqslant p$. The only deep holes of $RS_p(D, k)$ are generated by functions which are equivalent to the following:

$$f(x) = x^k, \quad f_\delta(x) = \frac{1}{x - \delta},$$

where $\delta \in \mathbb{F}_p \setminus D$. Here two functions $f(x)$ and $g(x)$ are equivalent if and only if there exists $a \in \mathbb{F}_p^*$ and $h(x)$ with degree less than k such that

$$g(x) = af(x) + h(x).$$

Our techniques are built on the idea of deep hole trees, and several results concerning the Erdös-Heilbronn conjecture. We also show the following theorem based on some results of finite geometry.

Theorem 10: Given a finite filed $\mathbb{F}_q$ with characteristic $p > 2$, we have

1) If $k+1 \leqslant p$ or $3 \leqslant q-p+1 \leqslant k+1 \leqslant q-2$, then Conjecture 1 is true.
2) If $3 \leqslant k < \dfrac{\sqrt{q}+1}{4}$, then Conjecture 2 is true.
3) If $3 \leqslant k < \dfrac{p}{45}$, and $q=p$ is prime, then Conjecture 2 is true.

This paper is organized as follows: Section II presents some preliminaries; Section III describes the idea of the deep hole tree; Section IV demonstrates the proof of Theorem 9; Section V gives the proof of Theorem 10.

II. Preliminaries

A. A criterion for deep holes of RS codes

By definition, deep holes of a code are words that has a maximum distance to the code. In the case of RS codes, there is another way to characterize the deep hole as follows. The following is well known:

Proposition 2: Let $\mathbb{F}_q$ be a finite field with characteristic p. Suppose G is a generator matrix for a RS code $C=[n,k]_q$ with covering radius $\rho = n-k$, then $u \in \mathbb{F}_q^n$ is a deep hole of C if and only if

$$G' = \left[\frac{G}{u}\right]$$

generates an MDS code.

We provide a proof for the sake of completeness.

Proof: $\Rightarrow$ Suppose u is a deep hole of $C=[n,k]_q$, we need to show that G' is a generator matrix for another MDS code. Equivalently, we need to show that any $k+1$ columns of G' are linearly independent.

Assume there exist $k+1$ columns of G' which are linearly dependent. Without loss of generality, we assume that the first $k+1$ columns of G' are linear dependent. Consider the submatrix consisting of the intersection of the first $k+1$ rows and the first $k+1$ columns of G'. Hence there exist $a_1,\ldots,a_k \in \mathbb{F}_q$, not all zero, such that

$$(u_1,\ldots,u_{k+1}) = a_1 r_{1,k+1} + \cdots + a_k r_{k,k+1},$$

where $r_{i,k+1}$ is the vector consisting of the first $k+1$ elements of the i-th row of G for $1 \leqslant i \leqslant k$. Let $v = a_1 r_1 + \cdots + a_k r_k \in C$, where r_i is the i-th row of G for $1 \leqslant i \leqslant k$. We have

$$d(u,v) \leqslant n-(k+1) < \rho,$$

which is a contradiction with the assumption that u is a deep hole of C.

$\Leftarrow$ Now suppose G' is a generator matrix for an MDS code, i.e., any $k+1$ columns of G' are linearly independent. We need to show that $d(u,C)=n-k$.

Assume that $d(u,C) < n-k$. Equivalently, there exist $a_1,\ldots,a_k \in \mathbb{F}_q$ such that u and $v=a_1r_1+\cdots+a_kr_k$ have more than k common coordinates, where r_i is the i-th row of G for $1 \leqslant i \leqslant k$. Without loss of generality, we assume that the first $k+1$ coordinates of u and v are the same. Consider the submatrix consisting of the first $k+1$ columns. Since the rank of the matrix is less than $k+1$, thus the first $k+1$ columns of G' are linearly dependent, which contradicts the assumption. ∎

Lemma 2: Let $D_1 \subset D_2 \subset \mathbb{F}_q$. If f generates a deep hole for $RS_q(D_2,k)$, then it also generates a deep hole for $RS_q(D_1,k)$.

Proof: Without loss of generality, we assume that $D_1 = \{\alpha_1,\ldots,\alpha_{d_1}\} \subset D_2 = \{\alpha_1,\ldots,\alpha_{d_1},\ldots,\alpha_{d_2}\}$, where $d_1 \leqslant d_2$. Consider the matrix

$$G' = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{d_2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{d_2}^{k-1} \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_{d_2}) \end{bmatrix}.$$

Since f generates a deep hole for $RS_q(D_2,k)$, we conclude that any $k+1$ columns of G' are linearly dependent by Proposition 2. This implies that any $k+1$ columns from the first d_1 columns of G' are linearly dependent, which is equivalent to that f generates a deep hole for $RS_q(D_1,k)$ by Proposition 2 again. ∎

B. Some additive combinatorics results

In this section, we introduce some additive combinatorics results that we will use later. The first theorem is about the estimation of the size of restricted sum sets, which was first proved by Dias da Silva and Hamidoune [17]. Then Alon, Nathanson and Ruzsa [1] gave a simple proof using the polynomial method.

Theorem 11: ([17], [1]) Let $\mathbb{F}$ be a field with characteristic p and n be a positive integer. Then for any finite subset $S \subset \mathbb{F}$ we have

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

where $n^{\wedge}S$ denotes the set of all sums of n distinct elements of S.

Brakemeier [3], Gallardo, Grekos and Pihko [7] established the following theorem:

Theorem 12: ([3], [7]) Let n be a positive integer and $S \subset \mathbb{Z}/n\mathbb{Z}$. If $|S| > \frac{n}{2}+1$, then

$$2^{\wedge}S = \mathbb{Z}/n\mathbb{Z},$$

where $2^{\wedge}S$ denotes the set of all sums of 2 distinct elements of S.

Hence we have the following corollary:

Corollary 1: Let $\mathbb{F}_p$ be a prime finite field, $S \subset \mathbb{F}_p^*$. If $|S| > \frac{p+1}{2}$, then each element of $\mathbb{F}_p^*$ is the product of two distinct elements of S.

Proof: Let g be a generator of $\mathbb{F}_p^*$. Let

$$S' = \{e | g^e \in S\} \subset \mathbb{Z}/(p-1)\mathbb{Z}.$$

For any given element $\alpha = g^a \in \mathbb{F}_p^*$, we need to show that there exist two distinct elements $b \neq c$ such that

$$g^a = g^b g^c,$$

where $b,c \in S'$. This is equivalent to

$$a = b + c,$$

which follows from Theorem 12. ∎

III. Construction of the deep hole tree

Let $\mathbb{F}_q = \{\alpha_1, \alpha_2, \cdots, \alpha_q = 0\}$. The polynomials in $\mathbb{F}_q[x]$ of degree less than q form a $\mathbb{F}_q$-linear space, with a basis

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

Given a polynomial $f(x) \in \mathbb{F}_q[x]$ with degree $q-1$ we have

$$f(x) = l(x) + c_1 \prod_{i=1}^{k}(x-\alpha_i) + \cdots + c_{q-k}\prod_{i=1}^{q-1}(x-\alpha_i),$$

where $l(x)$ is of degree less than k. We want to determine when $f(x)$ generates a deep hole. By Proposition 2, $f(x)$ generates a deep hole of $RS_q(\mathbb{F}_q, k)$ if and only if

$$G' = \left[\frac{G}{u}\right]$$

generates an MDS code, where G is the generator matrix of $RS_q(\mathbb{F}_q, k)$, and $u = (f(\alpha_1), \ldots, f(\alpha_q))$.

From Lemma 2, we conclude that a function that generates a deep hole for $RS_q(D_2, k)$, also generates a deep hole for $RS_q(D_1, k)$ if $D_1 \subset D_2$. Instead of considering the deep holes for $RS_q(\mathbb{F}_q, k)$ at the first step, we consider a smaller evaluation set at the beginning and make it increase gradually. To be more precise, we first determine c_1 over $D_1 = \{\alpha_1, \ldots, \alpha_{k+1}\}$, then we determine c_2 over $D_2 = \{\alpha_1, \ldots, \alpha_{k+2}\}$ based on the knowledge of c_1, so on and so forth. We present the result as a tree, which we will call a *deep hole tree*.

Remark 1: Wu and Hong [21] showed that if $D = \mathbb{F}_q \setminus \{\beta_1, \ldots, \beta_s\}$ then $f_{\beta_i}(x) = \frac{1}{x-\beta_i}$ generates a deep hole for $RS_q(D, k)$, where $1 \leqslant i \leqslant s$. Zhang, Fu, and Liao [23] got the same result using a different method. We can also deduce this from Proposition 2. We will call these deep holes, together with deep holes generated by functions of degree k, *expected deep holes*.

Motivated by Remark 1, we first construct the *expected deep hole tree* for $RS_p(D, k)$ as follows:

- The root node is 1 without loss of generality, i.e., $c_1 = 1$.
- There are $p-k-1$ branches of the tree, each with distinct length in $[2, p-k]$. And we designate the sequence of nodes in a branch with length l as b_l.
  - If $l = p-k$, then $b_{p-k} = \{1, 0, \ldots, 0\}$.
  - If $2 \leqslant l \leqslant p-k-1$, then $b_l = (c_1, \ldots, c_l)$, where $f = \frac{1}{x-\alpha_{k+l+1}}$ is equivalent to $c_1\prod_{i=1}^{k}(x-\alpha_i) + \cdots + c_l\prod_{i=1}^{k+l-1}(x-\alpha_i)$.

Proposition 3: The expected deep hole tree is a part of the full deep hole tree.

Proof: This follows from Remark 1. ∎

Now we can construct the full deep hole tree based on the expected deep hole tree.

- The root node is 1 without loss of generality, i.e., $c_1 = 1$.
- The children $\{c_{i+1}\}$ of a node $c_i, 1 \leqslant i \leqslant p-k-1$ are defined as follows: given the ancestors $(c_1, \ldots, c_i)$, for $\gamma \in \mathbb{F}_p$, if γ is the child of c_i in the expected deep hole tree, then keep it; otherwise, if

$$c_1\prod_{i=1}^{k}(x-\alpha_i) + \cdots + c_i\prod_{i=1}^{k+i-1}(x-\alpha_i) + \gamma\prod_{i=1}^{k+i}(x-\alpha_i)$$

satisfies the property of the function which generates a deep hole as in Proposition 2, then γ is a child of c_i.

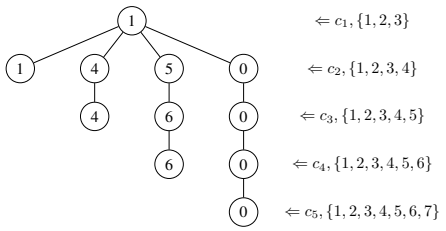

Fig. 1: Expected deep hole tree for $p = 7, k = 2$

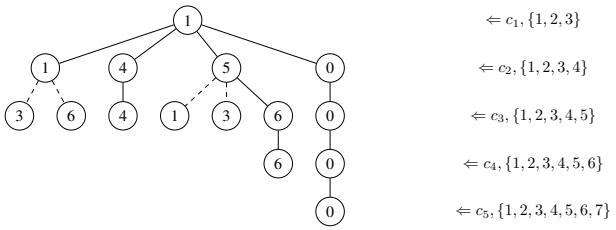

Fig. 2: Full deep hole tree for $p = 7, k = 2$

That is, we keep the nodes of the expected deep hole tree and add additional ones if necessary. Now we illustrate the procedure to construct the deep hole tree by some examples.

Example 1: Let $p = 7, k = 2$. The evaluation set is ordered such that $\alpha_i = i, 1 \leqslant i \leqslant 7$. The expected deep hole tree is shown in Figure 1.

Remark 2: We notice the following in Figure 1:

1) The root corresponds to the evaluation set $D_1 = \{1, 2, 3\}$. The expected deep holes are generated by functions equivalent to $\prod_{i=1}^{2}(x-i)$.
2) In depth 2, the evaluation set is $D_2 = \{1, 2, 3, 4\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x-i) + \prod_{i=1}^{3}(x-i)$, which is equivalent to $f_5 = \frac{1}{x-5}$.
3) In depth 3, the evaluation set is $D_3 = \{1, 2, 3, 4, 5\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x-i) + 4\prod_{i=1}^{3}(x-i) + 4\prod_{i=1}^{4}(x-i)$, which is equivalent to $f_6 = \frac{1}{x-6}$.
4) In depth 4, the evaluation set is $D_4 = \{1, 2, 3, 4, 5, 6\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x-i) + 5\prod_{i=1}^{3}(x-i) + 6\prod_{i=1}^{4}(x-i) + 6\prod_{i=1}^{5}(x-i)$, which is equivalent to $f_0 = \frac{1}{x}$.
5) In depth 5, the evaluation set is $D_5 = \{1, 2, 3, 4, 5, 6, 7\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x-i)$.

Example 2: Let $p = 7, k = 2$. The evaluation set is ordered such that $\alpha_i = i, 1 \leqslant i \leqslant 7$. The full deep hole tree is shown in Figure 2.

Remark 3: There are four more nodes here than the expected deep hole tree. They are all in depth three.

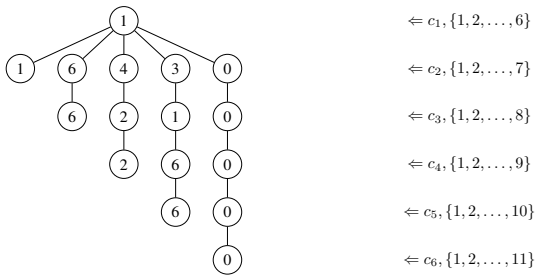

Fig. 3: Expected and full deep hole tree for $p = 11, k = 5$

1) The first additional deep hole is generated by the function $\prod_{i=1}^{2}(x-i) + \prod_{i=1}^{3}(x-i) + 3\prod_{i=1}^{4}(x-i)$.
2) The second additional deep hole is generated by the function $\prod_{i=1}^{2}(x-i) + \prod_{i=1}^{3}(x-i) + 6\prod_{i=1}^{4}(x-i)$.
3) The third additional deep hole is generated by the function $\prod_{i=1}^{2}(x-i) + 5\prod_{i=1}^{3}(x-i) + \prod_{i=1}^{4}(x-i)$.
4) The fourth additional deep hole is generated by the function $\prod_{i=1}^{2}(x-i) + 5\prod_{i=1}^{3}(x-i) + 3\prod_{i=1}^{4}(x-i)$.

Example 3: Let $p = 11, k = 5$. The evaluation set is ordered such that $\alpha_i = i, 1 \leqslant i \leqslant 11$. The expected deep hole tree and full deep hole tree are shown in Figure 3, which are the same.

IV. Proof of Theorem 9

We first present several lemmas.

Lemma 3: In depth $d = 2$, the nodes are the same in both the expected deep hole tree and the full deep hole tree.

Proof: In depth $d = 2$, the evaluation set is $D = \{\alpha_1, \alpha_2, \ldots, \alpha_{k+2}\}$. Designate the set of nodes in depth 2 of the expected deep hole tree as S. Firstly, we show that $|S| = p-(k+1)$. This follows from the fact that the equivalent functions of the form

$$f(x) = \prod_{i=1}^{k}(x-\alpha_i) + c_2\prod_{i=1}^{k+1}(x-\alpha_i), \quad c_2 \in \mathbb{F}_p,$$

for $f = x^k$ and $f_\delta(x) = \frac{1}{x-\delta}$ take the same value at $\beta \in D \setminus \{\alpha_{k+2}\}$ but pairwise different values at α_{k+2}, where $\delta \in \mathbb{F}_p \setminus D$.

Next, we show that if $c_2 \notin S$ then $f(x) = \prod_{i=1}^{k}(x-\alpha_i) + c_2\prod_{i=1}^{k+1}(x-\alpha_i)$ does not generate a deep hole. Consider the following matrix

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{k+2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{k+2}^{k-1} \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_{k+2}) \end{bmatrix},$$

where $f(\alpha_i) = 0, 1 \leqslant i \leqslant k, f(\alpha_{k+1}) = \prod_{i=1}^{k}(\alpha_{k+1} - \alpha_i), f(\alpha_{k+2}) = \prod_{i=1}^{k}(\alpha_{k+2} - \alpha_i) + c_2\prod_{i=1}^{k+1}(\alpha_{k+2} - \alpha_i)$.

If $f(\alpha_{k+2}) = 0$, i.e., $c_2 = \frac{1}{\alpha_{k+1}-\alpha_{k+2}}$, then there are $k+1$ columns of G, namely, the first k columns and the last column, which are linearly dependent. Thus $f(x)$ does not generate a deep hole in this case. In the following, we assume $f(\alpha_{k+2}) \neq 0$. For any $k-1$ elements $\{\beta_1, \ldots, \beta_{k-1}\} \subset \{\alpha_1, \ldots, \alpha_k\}$, consider the submatrix

$$G' = \begin{bmatrix} 1 & \cdots & 1 & 1 & 1 \\ \beta_1 & \cdots & \beta_{k-1} & \alpha_{k+1} & \alpha_{k+2} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_{k-1}^{k-1} & \alpha_{k+1}^{k-1} & \alpha_{k+2}^{k-1} \\ 0 & \cdots & 0 & f(\alpha_{k+1}) & f(\alpha_{k+2}) \end{bmatrix}.$$

Thus $\det(G') = 0$ is equivalent to

$$f(\alpha_{k+1})\prod_{i=1}^{k-1}(\alpha_{k+2} - \beta_i) = f(\alpha_{k+2})\prod_{i=1}^{k-1}(\alpha_{k+1} - \beta_i),$$

that is,

$$\begin{aligned}\frac{f(\alpha_{k+2})}{f(\alpha_{k+1})} &= \prod_{i=1}^{k-1}\frac{\alpha_{k+2}-\beta_i}{\alpha_{k+1}-\beta_i} \\ &= \prod_{i=1}^{k-1}(1 + \frac{\alpha_{k+2}-\alpha_{k+1}}{\alpha_{k+1}-\beta_i}).\end{aligned}$$

Hence for each subset of $\{\beta_1, \ldots, \beta_{k-1}\} \subset \{\alpha_1, \ldots, \alpha_k\}$, there is a unique c_2 such that $\det(G') = 0$.

In total, there are $k+1$ elements of candidate c_2 such that the corresponding $f(x)$ does not generate a deep hole. This implies that if $c_2 \notin S$ then $f(x)$ does not generate a deep hole.

In conclusion, in depth $d = 2$, the nodes in the full deep hole tree are exactly those in the expected deep hole tree. ■

Lemma 4: Let p be an odd prime, $k \geqslant \frac{p-1}{2}, d \geqslant 2$ be a positive integer and $D_d = \{\alpha_1, \ldots, \alpha_{k+d}\} \subset \mathbb{F}_p, \delta \in \mathbb{F}_p \setminus D_d$. For any $\gamma \in \mathbb{F}_p$, there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_d$ such that the matrix

$$A = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & \gamma \end{bmatrix},$$

is singular.

Proof: Note that $\det(A) = \det(A') + \det(A'')$, where

$$A' = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & 0 \end{bmatrix}, A'' = \begin{bmatrix} 1 & \cdots & 1 & 0 \\ \beta_1 & \cdots & \beta_k & 0 \\ \vdots & \ddots & \vdots & 0 \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & 0 \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & \gamma \end{bmatrix}.$$

Since

$$\begin{aligned}
&\prod_{i=1}^{k}(\beta_i-\delta)\det(A')\\
=&\begin{vmatrix}\beta_1 & \cdots & \beta_k & 1\\ \beta_1^2 & \cdots & \beta_k^2 & 2\delta\\ \vdots & \ddots & \vdots & \vdots\\ \beta_1^k & \cdots & \beta_k^k & k\delta^{k-1}\\ 1 & \cdots & 1 & 0\end{vmatrix}\\
=&(-1)^k\frac{d}{dx}\begin{vmatrix}1 & \cdots & 1 & 1\\ \beta_1 & \cdots & \beta_k & x\\ \beta_1^2 & \cdots & \beta_k^2 & x^2\\ \vdots & \ddots & \vdots & \vdots\\ \beta_1^k & \cdots & \beta_k^k & x^k\end{vmatrix}\Bigg|_{x=\delta}\\
=&(-1)^k\frac{d}{dx}\left[\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\prod_{i=1}^{k}(x-\beta_i)\right]\Bigg|_{x=\delta},
\end{aligned}$$

thus

$$\begin{aligned}
\det(A')&=\frac{(-1)^k}{\prod_{i=1}^{k}(\beta_i-\delta)}\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\frac{d}{dx}\left[\prod_{i=1}^{k}(x-\beta_i)\right]\Bigg|_{x=\delta}\\
&=\frac{(-1)^k}{\prod_{i=1}^{k}(\beta_i-\delta)}\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\prod_{i=1}^{k}(\delta-\beta_i)\sum_{i=1}^{k}\frac{1}{\delta-\beta_i}\\
&=\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\sum_{i=1}^{k}\frac{1}{\delta-\beta_i}.
\end{aligned}$$

It follows that

$$\begin{aligned}
\det(A)&=\det(A')+\det(A'')\\
&=\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\sum_{i=1}^{k}\frac{1}{\delta-\beta_i}+\gamma\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)
\end{aligned}$$

Hence $\det(A)=0$ is equivalent to

$$\sum_{i=1}^{k}\frac{1}{\delta-\beta_i}+\gamma=0.$$

Designate the set $\{\frac{1}{\delta-\beta_i}|\beta_i\in D_d\}$ as S_1 with cardinality $k+d$. Since $\frac{p-1}{2}\leqslant k, 2\leqslant d$, from Theorem 11, we conclude that

$$\begin{aligned}
|k^{\wedge}S_1|&\geqslant\min\{p,k|S_1|-k^2+1\}\\
&=p,
\end{aligned}$$

which implies that for each $\gamma\in\mathbb{F}_p$, there exists a subset $\{\beta_1,\ldots,\beta_k\}\subset D_d$ such that $\sum_{i=1}^{k}\frac{1}{\delta-\beta_i}+\gamma=0$. ■

Lemma 5: Let p be an odd prime, $k\geqslant\frac{p-1}{2}, d\geqslant 2$ be a positive integer and $D_{d+1}=\{\alpha_1,\ldots,\alpha_{k+d+1}=\delta\}\subset\mathbb{F}_p$. For any $\delta'\in\mathbb{F}_p,\delta'\notin D_{d+1},\gamma\in\mathbb{F}_p,\gamma\neq\frac{1}{\delta-\delta'}$, there exists a subset $\{\beta_1,\ldots,\beta_k\}\subset D_{d+1}\setminus\{\delta\}$ such that the matrix

$$B=\begin{bmatrix}1 & \cdots & 1 & 1\\ \beta_1 & \cdots & \beta_k & \delta\\ \vdots & \ddots & \vdots & \vdots\\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1}\\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \gamma\end{bmatrix}$$

is singular.

Proof: Note that $\det(B)=\det(B')+\det(B'')$, where

$$B'=\begin{bmatrix}1 & \cdots & 1 & 1\\ \beta_1 & \cdots & \beta_k & \delta\\ \vdots & \ddots & \vdots & \vdots\\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1}\\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \frac{1}{\delta-\delta'}\end{bmatrix},$$

$$B''=\begin{bmatrix}1 & \cdots & 1 & 0\\ \beta_1 & \cdots & \beta_k & 0\\ \vdots & \ddots & \vdots & 0\\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & 0\\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \gamma-\frac{1}{\delta-\delta'}\end{bmatrix}.$$

Since

$$\begin{aligned}
&(\delta-\delta')\prod_{i=1}^{k}(\beta_i-\delta')\det(B')\\
=&\begin{vmatrix}\beta_1 & \cdots & \beta_k & \delta\\ \beta_1^2 & \cdots & \beta_k^2 & \delta^2\\ \vdots & \ddots & \vdots & \vdots\\ \beta_1^k & \cdots & \beta_k^k & \delta^k\\ 1 & \cdots & 1 & 1\end{vmatrix}\\
=&(-1)^k\begin{vmatrix}1 & \cdots & 1 & 1\\ \beta_1 & \cdots & \beta_k & \delta\\ \beta_1^2 & \cdots & \beta_k^2 & \delta^2\\ \vdots & \ddots & \vdots & \vdots\\ \beta_1^k & \cdots & \beta_k^k & \delta^k\end{vmatrix}\\
=&(-1)^k\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\prod_{i=1}^{k}(\delta-\beta_i),
\end{aligned}$$

we have

$$\begin{aligned}
&\det(B')\\
=&\frac{(-1)^k}{(\delta-\delta')\prod_{i=1}^{k}(\beta_i-\delta')}\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\prod_{i=1}^{k}(\delta-\beta_i)\\
=&\frac{1}{\delta-\delta'}\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\prod_{i=1}^{k}\frac{\beta_i-\delta}{\beta_i-\delta'},
\end{aligned}$$

and

$$\det(B'')=(\gamma-\frac{1}{\delta-\delta'})\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i).$$

Hence

$$\begin{aligned}
&\det(B)\\
=&\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\left[\frac{1}{\delta-\delta'}\prod_{i=1}^{k}\frac{\beta_i-\delta}{\beta_i-\delta'}+\frac{\gamma(\delta-\delta')-1}{\delta-\delta'}\right]\\
=&\frac{\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)}{\delta-\delta'}\left[\prod_{i=1}^{k}\frac{\beta_i-\delta}{\beta_i-\delta'}+\gamma(\delta-\delta')-1\right].
\end{aligned}$$

It follows that $\det(B)=0$ is equivalent to

$$\prod_{i=1}^{k}(1+\frac{\delta'-\delta}{\beta_i-\delta'})=1-\gamma(\delta-\delta').$$

If $|D_d| = k+2$, let $P = \prod_{i=1}^{k+2}(1+\frac{\delta'-\delta}{\alpha_i-\delta'})$. From Corollary 1, there exist two distinct elements $x, y \in D_d$ such that $(1+\frac{\delta'-\delta}{x-\delta'})(1+\frac{\delta'-\delta}{y-\delta'}) = \frac{P}{1-\gamma(\delta-\delta')}$, hence

$$\begin{aligned}&\prod_{\beta_i\in D_d\setminus\{x,y\}}(1+\frac{\delta'-\delta}{\beta_i-\delta'})\\ =&P/[(1+\frac{\delta'-\delta}{x-\delta'})(1+\frac{\delta'-\delta}{y-\delta'})]\\ =&1-\gamma(\delta-\delta'),\end{aligned}$$

for any $\gamma \neq \frac{1}{\delta-\delta'}$.

If $|D_d| > k+2$, we select a subset $D' \subset D_d$ such that $|D'| = k+2$, then apply the same argument as above. ∎

Lemma 6: Let p be an odd prime, $k \geqslant \frac{p-1}{2}, d \geqslant 2$ be a positive integer and $D_{d+1} = \{\alpha_1, \ldots, \alpha_{k+d+1} = \delta\} \subset \mathbb{F}_p$. For any $\gamma \in \mathbb{F}_p, \gamma \neq \delta^k$, there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_{d+1} \setminus \{\delta\}$ such that the matrix

$$C = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \beta_1^k & \cdots & \beta_k^k & \gamma \end{bmatrix}$$

is singular.

Proof: Note that $\det(C) = \det(C') + \det(C'')$, where

$$C' = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \beta_1^k & \cdots & \beta_k^k & \delta^k \end{bmatrix},$$

$$C'' = \begin{bmatrix} 1 & \cdots & 1 & 0 \\ \beta_1 & \cdots & \beta_k & 0 \\ \vdots & \ddots & \vdots & 0 \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & 0 \\ \beta_1^k & \cdots & \beta_k^k & \gamma-\delta^k \end{bmatrix}.$$

Since

$$\det(C') = \prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)\prod_{i=1}^{k}(\delta-\beta_i),$$

$$\det(C'') = \prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)(\gamma-\delta^k),$$

we have

$$\frac{1}{\prod_{1\leqslant i<j\leqslant k}(\beta_j-\beta_i)}\det(C) = \prod_{i=1}^{k}(\delta-\beta_i)+\gamma-\delta^k.$$

Thus $\det(C) = 0$ is equivalent to

$$\prod_{i=1}^{k}(\delta-\beta_i) = \delta^k-\gamma.$$

If $|D_d| = k+2$, let $P = \prod_{i=1}^{k+2}(\delta-\alpha_i)$. From Corollary 1, there exist two distinct elements $x, y \in D_d$ such that $(\delta-x)(\delta-y) = \frac{P}{\delta^k-\gamma}$. Hence,

$$\prod_{\beta_i\in D_d\setminus\{x,y\}}(\delta-\beta_i) = \delta^k-\gamma,$$

for any $\gamma \neq \delta^k$.

If $|D_d| > k+2$, we select a subset $D' \subset D_d$ such that $|D'| = k+2$, then apply the same argument as above. ∎

Now we prove Theorem 9.

Proof: (of Theorem 9) Proceed by induction on the depth of the full deep hole tree.

Basis case. This follows from Lemma 3.

Inductive step. We need to show that if the set of nodes of the full deep hole tree coincide with the nodes of the expected deep hole tree in the same depth $d \geqslant 2$, then there are no additional nodes in depth $d+1$ except the expected ones. Denote the corresponding evaluation set by $D_d = \{\alpha_1, \ldots, \alpha_{k+d}\}$ in depth d and $D_{d+1} = \{\alpha_1, \ldots, \alpha_{k+d}, \alpha_{k+d+1} = \delta\}$ in depth $d+1$. In order to show there are no new nodes in depth $d+1$, There are three cases to consider.

Case 1: We need to show the branch, which is corresponding to the function $f = \frac{1}{x-\delta}$, will not continue in the depth $d+1$. It suffices to show that there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset \{\alpha_1, \ldots, \alpha_{k+d}\}$ such that for any $\gamma \in \mathbb{F}_p$ and matrix

$$A = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & \gamma \end{bmatrix},$$

we have $\det(A) = 0$. This follows from Lemma 4.

Case 2: We need to show that the branch, which is corresponding to the function $f = \frac{1}{x-\delta'}$, where $\delta' \notin D_{d+1}$, has only one child in depth $d+1$. It suffices to show that there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_d$ such that for any $\delta' \notin D_{d+1}, \gamma \in \mathbb{F}_p, \gamma \neq \frac{1}{\delta-\delta'}$ and matrix

$$B = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \gamma \end{bmatrix},$$

we have $\det(B) = 0$. This follows from Lemma 5.

Case 3: We need to show that the branch, which is corresponding to the function $f = x^k$ has only one child in each depth. It suffices to show that there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_d$ such that for any $\gamma \neq \delta^k$ and matrix

$$C = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \beta_1^k & \cdots & \beta_k^k & \gamma \end{bmatrix},$$

we have $\det(C) = 0$. This follows from Lemma 6.

From the principle of induction, the theorem is proved. ∎

V. Proof of Theorem 10

Proof: There are 3 cases to prove.

Case 1. Let $RS_q(F_q, k)$ be an extended GRS code over the finite field $\mathbb{F}_q$ whose characteristic p is odd. Let one of its generator matrix be

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_q \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_q^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_q^{k-1} \end{bmatrix},$$

where $\alpha_1, \ldots, \alpha_q$ are distinct element of $\mathbb{F}_q$.

Suppose that a word $u \in \mathbb{F}_q^q$ is a deep hole of $RS_q(F_q, k)$. From proposition 2, this is equivalent to the fact that

$$G' = \begin{bmatrix} G \\ \hline u \end{bmatrix}$$

generates another linear MDS code, where

$$u = (u_1, u_2, \ldots, u_q).$$

Thus the set

$$S = \{c_1, \ldots, c_q\} \cup \{(0, \ldots, 0, 1)\},$$

where c_i is the i-th column of G' for $1 \leqslant i \leqslant q$, has size $q+1$ and has the property that every subset of S of size $k+1$ is a basis.

Since $k+1 \leqslant p$ or $3 \leqslant q-p+1 \leqslant k+1 \leqslant q-2$, by Theorem 8, we deduce that S is equivalent to the set

$$\{(1, \alpha, \alpha^2, \ldots, \alpha^k) \mid \alpha \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\}.$$

Thus we conclude that

$$u(x) = ax^k + f_{\leqslant k-1}(x), a \neq 0;$$

where $f_{\leqslant k-1}(x)$ denotes a polynomial with degree not larger than $k-1$.

Case 2. Firstly, we get an estimation of $N_{\min}(k, q)$. Combining Theorem 6 and Lemma 1, we conclude that

$$\begin{aligned} N_{\min}(k, q) &\leqslant N_{\min}(3, q) + k - 3 \\ &\leqslant \lceil q - \frac{\sqrt{q} - 7}{4} \rceil + k - 3 \\ &\leqslant q - 1. \end{aligned}$$

Now let G be a generator matrix of $RS_q(F_q^*, k)$ of the following form

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q-1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{q-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{q-1}^{k-1} \end{bmatrix},$$

where $\alpha_1, \ldots, \alpha_{q-1}$ are distinct elements of $\mathbb{F}_q^*$. From proposition 2, a word $u \in \mathbb{F}_q^{q-1}$ is a deep hole of $RS_q(F_q^*, k)$ if and only if

$$G' = \begin{bmatrix} G \\ \hline u \end{bmatrix}$$

generates another linear MDS code $\mathcal{C}_2$, where

$$u = (u_1, u_2, \ldots, u_{q-1}).$$

Since $\mathcal{C}_2$ is of length $q-1$, thus the matrix G' is equivalent to a Vandermonde matrix of rank $k+1$. Notice that G is the given Vandermonde matrix of rank k. Thus there are two possibilities of u, i.e., its Lagrange interpolation polynomial satisfies the following conditions:

$$u_1(x) = ax^k + f_{\leqslant k-1}(x), a \neq 0;$$

or

$$u_2(x) = bx^{q-2} + f_{\leqslant k-1}(x), b \neq 0;$$

where $f_{\leqslant k-1}(x)$ denotes a polynomial with degree not larger than $k-1$.

To show that $u_2(x)$ satisfies the condition, we prove that the submatrix U consisted of the first $k+1$ columns of G' is non-singular without loss of generality. Since the vector generated by $f_{\leqslant k-1}(x)$ is a linear combination of the k row vectors of G, thus

$$b \det(U) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{k+1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{k+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{k+1}^{k-1} \\ \alpha_1^{q-2} & \alpha_2^{q-2} & \cdots & \alpha_{k+1}^{q-2} \end{vmatrix}.$$

Since $\alpha_i^{q-1} = 1$ for $1 \leqslant i \leqslant k+1$, we have

$$b \prod_{i=1}^{k+1} \alpha_i \det(U) = \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{k+1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{k+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^k & \alpha_2^k & \cdots & \alpha_{k+1}^k \\ 1 & 1 & \cdots & 1 \end{vmatrix}.$$

Hence

$$b \prod_{i=1}^{k+1} \alpha_i \det(U) = (-1)^k \prod_{1 \leq i < j \leq k+1} (\alpha_j - \alpha_i).$$

Thus $\det(U) \neq 0$, which implies U is non-singular.

Case 3. This is similar with the proof of case 2 and we will make use of Theorem 7. ∎

VI. Concluding Remarks

In this paper, we classify deep holes completely of the generalized Reed-Solomon codes $RS_p(D, k)$ for the case that p is a prime and $k \geqslant \frac{p-1}{2}$. If p is a prime and $k < \frac{p-1}{2}$, then the problem of classifying deep holes is still kept open. On the other hand, we suspect that a similar result holds over finite fields of composite order, and leave it as another open problem.

Acknowledgement

The authors would like to thank the reviewers and the editor for their much appreciated comments and suggestions.

REFERENCES

[1] N. Alon, M.B. Nathanson, and I.Z. Ruzsa. The polynomial method and restricted sums of congruence classes. *Journal of Number Theory*, 56(2):404–417, 1996.

[2] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society*, 14(3):733–748, 2012.

[3] W. Brakemeier. Eine anzahlformel von zahlen modulo n. *Monatshefte für Mathematik*, 85:277–282, 1978.

[4] A. Cafure, G. Matera, and M. Privitelli. Singularities of symmetric hypersurfaces and an application to reed-solomon codes. *Advances in Mathematics of Communications*, 6(1):69–94, 2012.

[5] Q. Cheng and E. Murray. On deciding deep holes of Reed-Solomon codes. In *TAMC*, pages 296–305, 2007.

[6] Q. Cheng and D. Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM Journal on Computing*, 37(1):195–209.

[7] L. Gallardo, G. Grekos, and J. Pihko. On a variant of the Erdös-Ginzburg-Ziv theorem. *Acta Arithmetica*, 89:331–336, 1999.

[8] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transaction on Information Theory*, 45(6):1757–1767, 1999.

[9] V. Guruswami and A. Vardy. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. In *Proceeding of SODA*, 2005.

[10] J. Li and D. Wan. On the subset sum problem over finite fields. *Finite Fields and Their Applications*, 14:911–929, 2008.

[11] J. Li and D. Wan. A new sieve for distinct coordinate counting. *Science China Mathematics*, 53(9):2351–2362, 2010.

[12] Y. Li and D. Wan. On error distance of Reed-Solomon codes. *Science in China Series A: Mathematics*, 51:1982–1988, 2008.

[13] Y. Li and G. Zhu. On error distance of received words with fixed degrees to Reed-Solomon code. 2015. arXiv:1508.02804.

[14] Q. Liao. On Reed-Solomon codes. *Chinese Annals of Mathematics, Series B*, 32B:89–98, 2011.

[15] R. M. Roth and A. Lempel. On MDS codes via cauchy matrices. *IEEE Transactions on Information Theory*, 35:1314–1319, 1989.

[16] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Annali di Matematica Pura ed Applicata*, 39(1):357–379, 1955.

[17] J. A. Dias Da Silva and Y. O. Hamidoune. Cyclic spaces for grassmann derivatives and additive theory. *Bulletin of the London Mathematical Society*, 26:140–146, 1994.

[18] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13:180–193, 1997.

[19] J. F. Voloch. Arcs in projective plans over prime fields. *Journal of Geometry*, 38:198–200, 1990.

[20] D. Wan and M. Keti. Deep holes in Reed-Solomon codes based on Dickson polynomials. 2015. arXiv:1507.01653.

[21] R. Wu and S. Hong. On deep holes of generalized Reed-Solomon codes. 2012. arXiv:1205.7016.

[22] R. Wu and S. Hong. On deep holes of standard Reed-Solomon codes. *Science China Mathematics*, 55(12):2447–2455, 2012.

[23] J. Zhang, F. Fu, and Q. Liao. New deep holes of generalized Reed-Solomon codes. *Scientia Sinica Mathematica*, 43(7):727–740, 2013.

[24] G. Zhu and D. Wan. Computing error distance of Reed-Solomon codes. In *TAMC2012*, LNCS 7287, pages 214–224.

Jincheng Zhuang received the B.S. degree and M.S. degree in Department of Mathematics in Shandong University in 2008 and 2011 respectively, and Ph.D. degree in computer science from University of Oklahoma in 2014.

He is now an assistant research fellow of State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His research interests include coding theory, cryptography and theoretical computer science.

Qi Cheng received the B.S. degree from Nankai University in 1992, the M.S. degree from Fudan University in 1995, and Ph.D. degree in computer science from University of Southern California in 2001.

He joined the University of Oklahoma in Norman, OK in 2001, where he is now the Williams Company Foundation Presidential Professor of Computer Science. His research interests include coding theory, cryptography and theoretical computer science.

Jiyou Li received the B.S. degree in Mathematics from Yunnan University in 2001, the M.S. degree in Mathematics from Beijing Normal University in 2004 and the Ph.D. degree in Mthematics from Peking University in 2008.

He is now an Associate Professor of Mathematics at Shanghai Jiao Tong University. His research interests include number theory, coding theory and combinatorics.