Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 4(2): 176–192.
DOI:10.3934/math.2019.2.176
Received: 24 December 2018
Accepted: 11 February 2019
Published: 19 February 2019

Research article

Some results on deep holes of generalized projective Reed-Solomon codes

Xiaofan Xu[1,*] **and Yongchao Xu**[2]

[1] Department of Mathematics, Sichuan Tourism University, Chengdu 610100, P.R. China
[2] Mathematical College, Sichuan University, Chengdu 610064, P.R. China

* **Correspondence:** Email: xxf@sctu.edu.cn; Tel: +862884637124; Fax: +862884828201.

Abstract: Let $l \geq 1$ be an integer and $a_1, \ldots, a_l$ be arbitrarily given l distinct elements of the finite field $\mathbf{F}_q$ of q elements with the odd prime number p as its characteristic. Let $D = \mathbf{F}_q \backslash \{a_1, \ldots, a_l\}$ and k be an integer such that $2 \leq k \leq q - l - 1$. For any $f(x) \in \mathbf{F}_q[x]$, we let $f(D) = (f(y_1), \ldots, f(y_{q-l}))$ if $D = \{y_1, ..., y_{q-l}\}$ and $c_{k-1}(f(x))$ be the coefficient of x^{k-1} of $f(x)$. In this paper, by using Dür's theorem on the relation between the covering radius and minimum distance of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$, we show that if $u(x) \in \mathbf{F}_q[x]$ with $\deg u(x) = k$, then the received word $(u(D), c_{k-1}(u(x)))$ is a deep hole of $\mathrm{GPRS}_q(D, k)$ if and only if $\sum_{y \in I} y \neq 0$ for any subset $I \subseteq D$ with $\#(I) = k$. We show also that if j is an integer with $1 \leq j \leq l$ and $u_j(x) := \lambda_j(x - a_j)^{q-2} + \nu_j x^{k-1} + f^{(j)}_{\leq k-2}(x)$ with $\lambda_j \in \mathbf{F}^*_q$, $\nu_j \in \mathbf{F}_q$ and $f^{(j)}_{\leq k-2}(x) \in \mathbf{F}_q[x]$ being a polynomial of degree at most $k - 2$, then $(u_j(D), c_{k-1}(u_j(x)))$ is a deep hole of $\mathrm{GPRS}_q(D, k)$ if and only if $\binom{q-2}{k-1}(-a_j)^{q-1-k} \prod_{y \in I}(a_j - y) + e \neq 0$ for any subset $I \subseteq D$ with $\#(I) = k$, where e is the identity of $\mathbf{F}^*_q$. Furthermore, $(u(\mathbf{F}^*_q), c_{k-1}(u(x)))$ is not a deep hole of the primitive projective Reed-Solomon code $\mathrm{PPRS}_q(\mathbf{F}^*_q, k)$ if $\deg u(x) = k$, and $(u(\mathbf{F}^*_q), \delta)$ is a deep hole of $\mathrm{PPRS}_q(\mathbf{F}^*_q, k)$ if $u(x) = \lambda x^{q-2} + \delta x^{k-1} + f_{\leq k-2}(x)$ with $\lambda \in \mathbf{F}^*_q$ and $\delta \in \mathbf{F}_q$.

Keywords: generalized projective Reed-Solomon codes; MDS codes; deep holes; Lagrange interpolation polynomial
Mathematics Subject Classification: 11C20, 11T71, 94B35, 94B65

1. Introduction and the statements of the main results

Let $\mathbf{F}_q$ be the finite field of q elements with p as its characteristic. Let n and k be positive integers such that $k < n$. Let $D = \{x_1, \cdots, x_n\}$ be a subset of $\mathbf{F}_q$, which is called the *evaluation set*. The *generalized Reed-Solomon code* $\mathrm{GRS}_q(D, k)$ of length n and dimension k over $\mathbf{F}_q$ is defined by:

$$\mathrm{GRS}_q(D, k) := \{(f(x_1), \ldots, f(x_n)) \in \mathbf{F}^n_q \mid f(x) \in \mathbf{F}_q[x], \deg f(x) \leq k - 1\}.$$

Moreover, the *generalized projective Reed-Solomon code* $\mathrm{GPRS}_q(D,k)$ of length $n+1$ and dimension k over $\mathbf{F}_q$ is defined as follows:

$$\mathrm{GPRS}_q(D,k) := \{(f(x_1),\ldots,f(x_n),c_{k-1}(f(x))) \in \mathbf{F}_q^{n+1} \mid f(x)\in \mathbf{F}_q[x], \deg f(x) \le k-1\},$$

where $c_{k-1}(f(x))$ is the coefficient of x^{k-1} of $f(x)$. If $D = \mathbf{F}_q^*$, then it is called *primitive projective Reed-Solomon code*, namely,

$$\mathrm{PPRS}_q(\mathbf{F}_q^*,k) := \{(f(1),\ldots,f(\alpha^{q-2}),c_{k-1}(f(x))) \in \mathbf{F}_q^{q} \mid f(x)\in \mathbf{F}_q[x], \deg f(x) \le k-1\},$$

where α is a primitive element of $\mathbf{F}_q$. If $D = \mathbf{F}_q$, then it is called the *extended projective Reed Solomon code*. For $u = (u_1,\ldots,u_n) \in \mathbf{F}_q^n$, $v = (v_1,\ldots,v_n) \in \mathbf{F}_q^n$, the *Hamming distance* $d(u,v)$ is defined by

$$d(u,v) := \#\{1 \le i \le n \mid u_i \ne v_i, u_i \in \mathbf{F}_q, v_i \in \mathbf{F}_q\}.$$

For any $[n,k]_q$ linear code C, the *minimum distance* $d(C)$ is defined by

$$d(C) := \min\{d(x,y) \mid x\in C, y\in C, x\ne y\},$$

where $d(\cdot,\cdot)$ denotes the *Hamming distance* of two codewords. A linear $[n,k,d]$ code is called *maximum distance separable* (MDS) code if $d = n-k+1$. The *error distance* to code C of a received word $u \in \mathbf{F}_q^n$ is defined by

$$d(u,C) := \min_{v\in C}\{d(u,v)\}.$$

Clearly, $d(u,C) = 0$ if and only if $u \in C$. The maximum error distance

$$\rho(C) = \max\{d(u,C) \mid u \in \mathbf{F}_q^n\}$$

is called the *covering radius* of C.

The most important algorithmic problem in coding theory is the maximum likelihood decoding (MLD): Given a received word $u \in \mathbf{F}_q^n$, find a codeword $v \in C$ such that $d(u,v) = d(u,C)$, then we decode u to v [1]. Therefore, it is very crucial to decide $d(u,C)$ for the received word u. Guruswami and Sudan [2] provided a polynomial time list decoding algorithm for the decoding of u when $d(u,C) \le n-\sqrt{nk}$. When the error distance increases, Guruswami and Vardy [3] showed that maximum-likelihood decoding is NP-hard for the family of Reed-Solomon codes. We also notice that Dür [4] studied the Cauchy codes. In particular, Dür [4] got the relation between the covering radius and minimum distance of $\mathrm{GPRS}_q(D,k)$. When decoding the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D,k)$, for a received word $u = (u_1,\ldots,u_n,u_{n+1}) \in \mathbf{F}_q^{n+1}$, we define the *Lagrange interpolation polynomial* $u(x)$ of the first n components of u by

$$u(x) := \sum_{i=1}^{n} u_i \prod_{\substack{j=1\\ j\ne i}}^{n} \frac{x-x_j}{x_i-x_j} \in \mathbf{F}_q[x],$$

i.e., $u(x)$ is the unique polynomial of degree $\deg u(x) \le n-1$ such that $u(x_i) = u_i$ for $1 \le i \le n$. It is clear that $u \in \mathrm{GPRS}_q(D,k)$ if and only if $d(u,\mathrm{GPRS}_q(D,k)) = 0$ if and only if $\deg u(x) \le k-1$ and $c_{k-1}(u(x)) = u_{n+1}$. Equivalently, $u \notin \mathrm{GPRS}_q(D,k)$ if and only if $d(u,\mathrm{GPRS}_q(D,k)) \ge 1$ if and only if

$k \le \deg u(x) \le n-1$ or $c_{k-1}(u(x)) \ne u_{n+1}$. Evidently, we have the following simple bounds of $d(u, \mathrm{GRS}_q(D,k))$ which are due to Li and Wan.

Theorem 1.1. [5] *Let u be a received word such that $u \notin \mathrm{GRS}_q(D,k)$. Then*

$$n - \deg u(x) \le d(u, \mathrm{GRS}_q(D,k)) \le n-k = \rho(\mathrm{GRS}_q(D,k)).$$

Let $u \in \mathbf{F}_q^n$. If $d(u, \mathrm{GRS}_q(D,k)) = \rho(\mathrm{GRS}_q(D,k))$, then the received word u is called a *deep hole* of $\mathrm{GRS}_q(D,k)$. From Theorem 1.1, one can easily see that the received word u is a deep hole of $\mathrm{GRS}_q(D,k)$ if its Lagrange interpolation polynomial is of degree k. In 2012, Wu and Hong [6] found another class of deep holes for the standard Reed-Solomon code $\mathrm{GRS}_q(\mathbf{F}_q^*, k)$. In fact, if $q \ge 4$ and $2 \le k \le q-2$, then they showed that the received word u is a deep hole if its Lagrange interpolation polynomial is of the form $ax^{q-2} + f_{\le k-1}(x)$ with $a \in \mathbf{F}_q^*$ and $f_{\le k-1}(x) \in \mathbf{F}_q[x]$ is a polynomial of degree at most $k-1$. In [7], Hong and Wu proved that the received word u is a deep hole of the generalized Reed-Solomon code $\mathrm{GRS}_q(D,k)$ if its Lagrange interpolation polynomial is $\lambda(x-a_i)^{q-2} + f_{\le k-1}(x)$, where $\lambda \in \mathbf{F}_q^*, a_i \in \mathbf{F}_q \backslash D$ and $f_{\le k-1}(x) \in \mathbf{F}_q[x]$ being a polynomial of degree at most $k-1$. In [8], Zhuang, Lin and Lv investigated the deep hole trees of generalized Reed-Solomon codes.

In what follows, we let l be a positive integer and $a_1, \ldots, a_l$ be any fixed l distinct elements of $\mathbf{F}_q$. Let

$$D := \mathbf{F}_q \backslash \{a_1, \ldots, a_l\}.$$

We write

$$D := \{y_1, \ldots, y_{q-l}\},$$

and for any $f(x) \in \mathbf{F}_q[x]$, we define

$$f(D) := (f(y_1), \ldots, f(y_{q-l})),$$

and use $c_{k-1}(f(x))$ to denote the coefficient of x^{k-1} of $f(x)$. Then we can rewrite the generalized projective Reed-Solomon code $\mathrm{GPRS}(D,k)$ with evaluation set D as

$$\mathrm{GPRS}_q(D,k) := \{(f(D), c_{k-1}(f(x))) \in \mathbf{F}_q^{q-l+1} \mid f(x) \in \mathbf{F}_q[x], \deg f(x) \le k-1\}.$$

Let $u \notin \mathrm{GPRS}_q(D,k)$. If $d(u, \mathrm{GPRS}_q(D,k)) = \rho(\mathrm{GPRS}_q(D,k))$, then u is also called a *deep hole* of generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D,k)$. In 2016, Zhang and Wan [9] studied the deep holes of projective Reed-Solomon code $\mathrm{GPRS}(\mathbf{F}_q,k)$. In fact, under the assumption that the only deep holes of $\mathrm{GRS}_q(\mathbf{F}_q,k)$ are those received words whose Lagrange interpolation polynomials are of degree k, they proved the following results by solving a subset sum problem.

Theorem 1.2. [9] *Let q be an odd prime power. Assume that $3 \le k+1 \le p$ or $3 \le q-p+1 \le k+1 \le q-2$. Then the received word $(f(\mathbf{F}_q), c_{k-1}(f(x)))$ with $\deg f(x) = k$ is a deep hole of $\mathrm{GPRS}(\mathbf{F}_q,k)$.*

Theorem 1.3. [9] *Let $\deg f(x) \ge k+1$ and $s := \deg f(x) - k + 1$. If there are positive constants c_1 and c_2 such that $s < c_1\sqrt{q}, (\frac{s}{2}+2)\log_2(q) < k < c_2 q$, then $(f(\mathbf{F}_q), c_{k-1}(f(x)))$ is not a deep hole of*

$\mathrm{GPRS}(\mathbf{F}_q, k)$.

In this paper, our main goal is to investigate the deep holes of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$. Actually, we will present characterizations for the received words of degrees k and $q-2$ to be deep holes of generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$. The main results of this paper can be stated as follows.

Theorem 1.4. *Let q be a prime power and let k, l be positive integers such that $q \geq 5$ and $2 \leq k \leq \min(q-3, q-l-1)$. Let $u(x) \in \mathbf{F}_q[x]$ with $\deg u(x) = k$. Then the received word $(u(D), c_{k-1}(u(x)))$ is a deep hole of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$ if and only if $\sum\limits_{y\in I} y \neq 0$ for any subset $I \subseteq D$ with $\#(I) = k$.*

Theorem 1.5. *Let q be a prime power and let k, l be positive integers such that $q \geq 4$ and $2 \leq k \leq q-l-1$. Let j be an integer with $1 \leq j \leq l$ and let $u_j(x) := \lambda_j(x-a_j)^{q-2} + \nu_j x^{k-1} + f_{\leq k-2}^{(j)}(x)$ with $\lambda_j \in \mathbf{F}_q^*$, $\nu_j \in \mathbf{F}_q$ and $f_{\leq k-2}^{(j)}(x) \in \mathbf{F}_q[x]$ being a polynomial of degree at most $k-2$. Then the received word $(u_j(D), c_{k-1}(u_j(x)))$ is a deep hole of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$ if and only if $\binom{q-2}{k-1} a_j^{q-1-k} \prod\limits_{y\in I}(y-a_j) \neq -e$ for any subset $I \subseteq D$ with $\#(I) = k$, where e is the identity of the multiplicative group $\mathbf{F}_q^*$.*

From Theorems 1.4 and 1.5, we can deduce the following results on the deep holes of the primitive projective Reed-Solomon codes. Note that the proof of Corollary 1.6 relies also on a result about the zero subsets sum of the group $\mathbf{F}_q^*$ (see Lemma 2.8 below).

Corollary 1.6. *Let q be an odd prime power such that $q \geq 5$ and $2 \leq k \leq q-3$. If $u(x) = \lambda x^k + \gamma x^{k-1} + f_{\leq k-2}(x)$ with $\lambda \in \mathbf{F}_q^*, \gamma \in \mathbf{F}_q$ and $f_{\leq k-2}(x) \in \mathbf{F}_q[x]$ being a polynomial of degree at most $k-2$, then the received word $(u(\mathbf{F}_q^*), \gamma)$ is not a deep hole of the primitive projective Reed-Solomon code $\mathrm{PPRS}_q(\mathbf{F}_q^*, k)$.*

Corollary 1.7. *Let $q \geq 4$ and $2 \leq k \leq q-2$. If $u(x) = \lambda x^{q-2} + \delta x^{k-1} + f_{\leq k-2}(x)$ with $\lambda \in \mathbf{F}_q^*, \delta \in \mathbf{F}_q$ and $f_{\leq k-2}(x) \in \mathbf{F}_q[x]$ being a polynomial of degree at most $k-2$, then the received word $(u(\mathbf{F}_q^*), \delta)$ is a deep hole of the primitive projective Reed-Solomon code $\mathrm{PPRS}_q(\mathbf{F}_q^*, k)$.*

Remark 1.8. Letting $\delta = 0$. Corollary 1.7 gives us the main result of [10].

In the proofs of Theorems 1.4 and 1.5, the basic tools are the MDS code and Vandemonde determinant. A key ingredient in these proofs is the so-called Dür's theorem on the relation between the covering radius and minimum distance of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$ (see Lemma 2.6 below). Another important ingredient is a new result on the zero-sum problem in the finite field that we will prove in the next section.

This paper is organized as follows. First of all, in Section 2, we recall and prove several preliminary lemmas that are needed in the proofs of Theorems 1.4 and 1.5. Consequently, in Section 3, we use the lemmas presented in Section 2 to give the proofs of Theorem 1.4 and Corollary 1.6. Finally, by using the results given in Section 2, we supply in Section 4 the proofs of Theorem 1.5 and Corollary 1.7.

2. Preliminary lemmas

In this section, our main goal is to prove several lemmas that are needed in the proof of Theorems 1.4 and 1.5. We begin with the following result on MDS codes.

Lemma 2.1. *Let C be a MDS code and $u_0 \in C$ be a given codeword. Then the received word u is a deep hole of C if and only if the received word $u + u_0$ is a deep hole of C.*

Proof. First of all, let u be a received word. Then by the definition of deep hole, one knows that u is a deep hole of C if and only if $d(u, C) = \rho(C)$ with $\rho(C)$ being the covering radius of C, if and only if

$$\min_{v\in C}\{d(u, v)\} = \rho(C). \tag{2.1}$$

Likewise, one has that the received word $u + u_0$ is a deep hole of C if and only if

$$\min_{v\in C}\{d(u + u_0, v)\} = \rho(C). \tag{2.2}$$

Since

$$\{d(u + u_0, v)|v \in C\} = \{d(u + u_0, v + u_0)|v \in C\},$$

it follows that

$$\min_{v\in C}\{d(u + u_0, v)\} = \min_{v\in C}\{d(u + u_0, v + u_0)\}. \tag{2.3}$$

But $d(u + u_0, v + u_0) = d(u, v)$ for any codeword u_0. Hence (2.3) tells us that

$$\min_{v\in C}\{d(u + u_0, v)\} = \min_{v\in C}\{d(u, v)\}. \tag{2.4}$$

Now from (2.1), (2.2) and (2.4), one can deduce that u is a deep hole of C if and only if $u + u_0$ is a deep hole of C as one desires. So Lemma 2.1 is proved. □

Remark 2.1. We should point out that if the word u_0 is not in C, then Lemma 2.1 is not true.

In what follows, we let

$$P_{k-1} := \{f(x) \mid f(x) \in \mathbf{F}_q[x], \deg f(x) \le k - 1\}.$$

We have the following result.

Lemma 2.2. *Let $\#(D) = q - l$ and let $u = (u_1, \cdots, u_{q-l}, u_{q-l+1}) \in \mathbf{F}_q^{q-l+1}$ and $v = (v_1, \cdots, v_{q-l}, v_{q-l+1}) \in \mathbf{F}_q^{q-l+1}$ be two received words with $u(x)$ and $v(x)$ being the Lagrange interpolation polynomial of the first $q - l$ components of u and v. If $u(x) = \lambda v(x) + f_{\le k-2}(x), u_{q-l+1} = \lambda v_{q-l+1}$, where $\lambda \in \mathbf{F}_q^*$ and $f_{\le k-2}(x) \in \mathbf{F}_q[x]$ is a polynomial of degree at most $k - 2$, then*

$$d(u, \mathrm{GPRS}_q(D, k)) = d(v, \mathrm{GPRS}_q(D, k)).$$

Further, u is a deep hole of $\mathrm{GPRS}_q(D,k)$ *if and only if v is a deep hole of* $\mathrm{GPRS}_q(D,k)$.

Proof. Since $u(x) = \lambda v(x) + f_{\le k-2}(x)$, we have $u(D) = \lambda v(D) + f_{\le k-2}(D)$. By the definition of Hamming distance, we know that for any code C over $\mathbf{F}_q$, if u and v are two codewords of C, then

$$d(u,v) = d(u+w, v+w) = d(\lambda u, \lambda v)$$

hold for any codeword w of C and any $\lambda \in \mathbf{F}_q^*$. Then from the definition of error distance and noticing that $u = (u(D), u_{q-l+1})$, we can deduce immediately that

$$\begin{aligned}
&d(u, \mathrm{GPRS}_q(D,k))\\
=&\min_{g\in P_{k-1}} d(u, (g(D), c_{k-1}(g(x))))\\
=&\min_{g\in P_{k-1}} d((u(D), u_{q-l+1}), (g(D), c_{k-1}(g(x))))\\
=&\min_{g\in P_{k-1}} d((\lambda v(D) + f_{\le k-2}(D), u_{q-l+1}), (g(D), c_{k-1}(g(x))))\\
=&\min_{g\in P_{k-1}} d((\lambda v(D) + f_{\le k-2}(D), \lambda v_{q-l+1}), (g(D), c_{k-1}(g(x))))\\
=&\min_{g\in P_{k-1}} d((\lambda v(D) + f_{\le k-2}(D), \lambda v_{q-l+1}), (g(D) + f_{\le k-2}(D), c_{k-1}(g(x))))\\
=&\min_{g\in P_{k-1}} d((\lambda v(D), \lambda v_{q-l+1}), (g(D), c_{k-1}(g(x))))\\
=&\min_{g\in P_{k-1}} d((\lambda v(D), \lambda v_{q-l+1}), (\lambda g(D), \lambda c_{k-1}(g(x))))(\text{since } \lambda \in \mathbf{F}_q^*)\\
=&\min_{g\in P_{k-1}} d((v(D), v_{q-l+1}), (g(D), c_{k-1}(g(x))))\\
=&d((v(D), v_{q-l+1}), \mathrm{GPRS}_q(D,k))\\
=&d(v, \mathrm{GPRS}_q(D,k))
\end{aligned}$$

as required. The proof of Lemma 2.2 is complete. □

For a linear $[n,k]$ code C with n and k being the length and dimension of C, respectively, we define the *generator matrix*, denoted by G, to be the $k \times n$ matrix of the form $G := (g_1, \dots, g_k)^T$, where $\{g_1, \dots, g_k\}$ is a basis of C as a vector space. Since $D = \{y_1, \dots, y_{q-l}\}$, the following $k \times (q-l+1)$ matrix

$$\begin{pmatrix} 1(D) & c_{k-1}(1) \\ x(D) & c_{k-1}(x) \\ \vdots & \vdots \\ x^{k-2}(D) & c_{k-1}(x^{k-2}) \\ x^{k-1}(D) & c_{k-1}(x^{k-1}) \end{pmatrix} = \begin{pmatrix} 1 & \dots & 1 & 0 \\ y_1 & \dots & y_{q-l} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ y_1^{k-2} & \dots & y_{q-l}^{k-2} & 0 \\ y_1^{k-1} & \dots & y_{q-l}^{k-1} & 1 \end{pmatrix} \tag{2.5}$$

forms a generator matrix of $\mathrm{GPRS}_q(D,k)$. For the purpose of this paper, we will choose the above matrix as the generator matrix of $\mathrm{GPRS}_q(D,k)$.

Lemma 2.3. [11] *Let C be an* $[n,k]$ *linear code and G be the generator matrix of C. Then C is a MDS code if and only if any k distinct columns of G are linear independent over finite field* $\mathbf{F}_q$.

Throughout this paper, for any nonempty set $\{\gamma_1, \ldots, \gamma_n\} \subset \mathbf{F}_q$, the *Vandermonde determinant*, denoted by $V(\gamma_1, \ldots, \gamma_n)$, is defined as follows:

$$V(\gamma_1, \ldots, \gamma_n) := \det \begin{pmatrix} 1 & \ldots & 1 \\ \gamma_1 & \ldots & \gamma_n \\ \vdots & \vdots & \vdots \\ \gamma_1^{n-1} & \ldots & \gamma_n^{n-1} \end{pmatrix}.$$

We have the following well-known result.

Lemma 2.4. [11] *One has*

$$V(\gamma_1, \ldots, \gamma_n) = \prod_{1 \le i < j \le n} (\gamma_j - \gamma_i).$$

In the following, we show that the generalized projective Reed-Solomon code is a MDS code.

Lemma 2.5. *Let $D \subset \mathbf{F}_q$. Then $\mathrm{GPRS}_q(D, k)$ is a $[q - l + 1, k]$ MDS code over finite field $\mathbf{F}_q$.*

Proof. Let G be the generator matrix of $\mathrm{GPRS}_q(D, k)$ given in (2.5). Write $G := (G_1, \ldots, G_{q-l+1})$. Let $i_1, \ldots, i_k$ be arbitrary k distinct integers such that $1 \le i_1 < \cdots < i_k \le q - l + 1$. We claim that $\det(G_{i_1}, \ldots, G_{i_k}) \neq 0$ which will be proved in what follows.

If $i_k \le q - l$, then it follows that

$$\det(G_{i_1}, \ldots, G_{i_k}) = V(y_{i_1}, \ldots, y_{i_k}) = \prod_{1 \le t < s \le k} (y_{i_s} - y_{i_t}) \neq 0.$$

The claim is true in this case.

If $i_k = q - l + 1$, then by expanding the determinant according to the last column, we arrive at

$$\det(G_{i_1}, \ldots, G_{i_k}) = V(y_{i_1}, \ldots, y_{i_{k-1}}) = \prod_{1 \le t < s \le k-1} (y_{i_s} - y_{i_t}) \neq 0.$$

The claim is proved in this case.

Now by the claim, we can derive that any k columns of the generator matrix G is linear independent. Then $\mathrm{GPRS}_q(D, k)$ is a MDS code by Lemma 2.3. This concludes the proof of Lemma 2.5. □

The following result about the relation between the covering radius and minimum distance of $\mathrm{GPRS}_q(D, k)$ will play a key role in this paper which is due to Dür [4].

Lemma 2.6. [4] *Let D be a proper subset of $\mathbf{F}_q$. Then*

$$\rho(\mathrm{GPRS}_q(D, k)) = d(\mathrm{GPRS}_q(D, k)) - 1.$$

Now we give a criterion to determine whether a received word is a deep hole of MDS code C.

Lemma 2.7. *Let G be a generator matrix of a MDS code $C = [n,k]$ over the finite field $\mathbf{F}_q$. If the covering radius $\rho(C) = n-k$, then a received word $u \in \mathbf{F}_q^n$ is a deep hole of C if and only if the $(k+1)\times n$ matrix $\begin{pmatrix} G \\ u \end{pmatrix}$ can be served as the generator matrix of another MDS code.*

Proof. We first show the sufficient part. Let C' be a $[n, k+1]$ MDS code with $\begin{pmatrix} G \\ u \end{pmatrix}$ as its generator matrix. Since $u \in C' \backslash C$, one can derived that

$$n-k = n-(k+1)+1 = d(C') \le d(u,C) \le \rho(C) = n-k.$$

It follows that

$$d(u,C) = \rho(C) = n-k.$$

Therefore u is a deep hole of C.

Now we turn to prove the necessity part. Assume that $\begin{pmatrix} G \\ u \end{pmatrix}$ cannot be served as a generator matrix of any MDS code. By lemma 2.3, we known that there exist $k+1$ distinct columns of

$$\begin{pmatrix} G \\ u \end{pmatrix} = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \vdots & \vdots \\ g_{k1} & \cdots & g_{kn} \\ u_1 & \ldots & u_n \end{pmatrix}_{(k+1)\times n}$$

are linear dependent over $\mathbf{F}_q$. Without loss of generality, we can suppose the first $k+1$ columns are linear dependent. Thus we have

$$\mathrm{rank}\begin{pmatrix} g_{11} & \cdots & g_{1,k+1} \\ \vdots & \vdots & \vdots \\ g_{k1} & \cdots & g_{k,k+1} \\ u_1 & \ldots & u_{k+1} \end{pmatrix}_{(k+1)\times(k+1)} \le k.$$

On the other hand, since G is a generator matrix of the $[n,k]$ MDS code C over the finite field $\mathbf{F}_q$, one can obtain that

$$\mathrm{rank}\begin{pmatrix} g_{11} & \cdots & g_{1k} \\ \vdots & \vdots & \vdots \\ g_{k1} & \cdots & g_{kk} \end{pmatrix}_{k\times k} = k.$$

Hence there exist k coefficients $a_1, \cdots, a_k \in \mathbf{F}_q$ that are not all zero such that $(u_1, \cdots, u_{k+1}) = \sum_{i=1}^{k} a_i(g_{i1}, \cdots, g_{i,k+1})$. Now let $v = \sum_{i=1}^{k} a_i(g_{i1}, \cdots, g_{in}) \in C$. One can immediately deduce that

$$d(u,C) = \min_{w\in C}\{d(u,w)\} \le d(u,v) \le n-(k+1) < n-k = \rho,$$

which is a contradiction with the hypothesis that u is a deep hole of C. So Lemma 2.7 is proved. □

In what follows, we show a result on the zero-sum problem in the finite field of odd characteristic.

Lemma 2.8. *Let $q = p^s$ with p being an odd prime number and k be an integer with $2 \le k \le q-3$. Then there exist a subset $I \subseteq \mathbf{F}_q^*$ with $\#(I) = k$ such that $\sum\limits_{z\in I} z = 0$.*

Proof. Since p is an odd prime number, it follows that for any $z \in \mathbf{F}_q^*$, one has $-z \in \mathbf{F}_q^*$ and $z \neq -z$ since $2z \neq 0$. But $|\mathbf{F}_q^* \setminus \{z, -z\}| = q - 3 \ge 2$ since $q \ge k + 3 \ge 5$. Now one can pick $z' \in \mathbf{F}_q^* \setminus \{z, -z\}$. Then $-z' \in \mathbf{F}_q^* \setminus \{z, -z, z'\}$ since $2z' \neq 0$. Continuing in this way, we finally arrive at

$$\mathbf{F}_q^* = \{z_1, -z_1, \cdots, z_{\frac{q-1}{2}}, -z_{\frac{q-1}{2}}\}. \tag{2.6}$$

We consider the following cases.

Case 1. $2 \mid k$. In this case, we let $I = \{z_1, -z_1, \cdots, z_{\frac{k}{2}}, -z_{\frac{k}{2}}\}$. Then $I \subset \mathbf{F}_q^*$ and we have

$$\sum_{z\in I} z = \sum_{i=1}^{\frac{k}{2}} (z_i + (-z_i)) = 0$$

as desired. Lemma 2.8 holds if $2 \mid k$.

Case 2. $2 \nmid k$. Then $k \ge 3$ and so $q \ge 7$ since $2 \le k \le q - 3$. We claim that there are three distinct elements $z', z'', z''' \in \mathbf{F}_q^*$ such that $z' + z'' + z''' = 0$, which will be proved by dividing into the following three subcases.

Case 2.1. $p = 3$. We pick a $z' \in \mathbf{F}_q^*$. Then $3z' = 0$, $-z' \neq 0$ and $2z' \neq 0$. The latter implies that $z' \neq -z'$. Since $p = 3$ and $q \ge 7$, we deduce that $q \ge 3^2 = 9$. Thus $|\mathbf{F}_q^* \setminus \{z', -z'\}| = q - 3 \ge 6$. So we can choose a $z'' \in \mathbf{F}_q^* \setminus \{z', -z'\}$. But $2z'' \neq 0$. Hence $-z'' \in \mathbf{F}_q^* \setminus \{z', -z', z''\}$. It implies that $z' + z'' \neq 0$, namely, $z' + z'' \in \mathbf{F}_q^*$. Furthermore, we have that $z' + z''$ is not equal to anyone of the four elements $z', -z', z''$ and $-z''$. That is, $z'+z'' \in \mathbf{F}_q^* \setminus \{z', -z', z'', -z''\}$. Hence $-(z'+z'') \in \mathbf{F}_q^* \setminus \{z', -z', z'', -z'', z'+z''\}$. Therefore there are three distinct elements z', z'' and $-(z' + z'')$ in $\mathbf{F}_q^*$ such that their sum equals zero. The claim holds in this case.

Case 2.2. $p = 5$. Take a $z' \in \mathbf{F}_q^*$. Then $5z' = 0$ and none of $z', 2z', 3z'$ and $4z'$ equals zero. It follows that the four elements $z', -z', 2z', -2z'$ are pairwise distinct. Since $q \ge 7 > 5$, one must have $q \ge 5^2 = 25$. Thus $|\mathbf{F}_q^* \setminus \{z', -z', 2z', -2z'\}| = q - 5 \ge 20$. So we can choose $z'' \in \mathbf{F}_q^* \setminus \{z', -z', 2z', -2z'\}$. Then $-z'' \in \mathbf{F}_q^* \setminus \{z', -z', 2z', -2z'\}$ and $z'+z'' \neq 0$. The latter one tells us that $-(z'+z'') \in \mathbf{F}_q^*$. Obviously, $-z'' \neq z''$ since $2z'' \neq 0$. Hence $-z'' \in \mathbf{F}_q^* \setminus \{z', -z', 2z', -2z', z''\}$.

Furthermore, we can deduce that $z' + z''$ is not equal to any of $z', -z', 2z', -2z', z''$ and $-z''$. This infers that $-(z' + z'') \in \mathbf{F}_q^* \setminus \{z', -z', 2z', -2z', z'', -z'', z' + z''\}$ since $2(z' + z'') \neq 0$. Therefore we can find three distinct elements z', z'' and $-(z' + z'')$ in $\mathbf{F}_q^*$ such that their sum equals zero. The claim holds in this case. The claim is proved in this case.

Case 2.3. $p \ge 7$. Then $le \neq 0$ for any integer l with $1 \le l \le 6$, where e stands for the identity of the group $\mathbf{F}_q^*$. Since $e \neq 0, 4e \neq 0$ and $5e \neq 0$, we have $e \neq 2e, e \neq -3e$ and $2e \neq -3e$. So there are three different elements $e, 2e, -3e$ in $\mathbf{F}_q^*$ such that their sum is equal to zero as one desires. The claim is true in this case.

Now by the claim, we know that there are three integers i_1, i_2 and i_3 such that $1 \le i_1 < i_2 < i_3 \le \frac{q-1}{2}$ and $z_{i_1} + z_{i_2} + z_{i_3} = 0$.

If $q = 7$, then letting $I = \{z_{i_1}, z_{i_2}, z_{i_3}\}$ gives us the desired result.

If $q > 7$, then $\mathbf{F}_q^* \setminus \{\pm z_{i_1}, \pm z_{i_2}, \pm z_{i_3}\}$ is nonempty. By (2.6), we obtain that

$$\begin{aligned}&\mathbf{F}_q^* \setminus \{\pm z_{i_1}, \pm z_{i_2}, \pm z_{i_3}\}\\=&\{\pm z_1, ..., \pm z_{i_1-1}, \pm z_{i_1+1}, ..., \pm z_{i_2-1}, \pm z_{i_2+1}, ..., \pm z_{i_3-1}, \pm z_{i_3+1}, ..., \pm z_{\frac{q-1}{2}}\}.\end{aligned} \tag{2.7}$$

Since $2 \nmid k$, $k-3$ is even. Evidently, the sum of the first $k-3$ elements on the right hand side of (2.7) is equal to zero because $z_i + (-z_i) = 0$ for all integers $1 \le i \le \frac{q-1}{2}$. Then the first $k-3$ elements on the right hand side of (2.7) together with the three elements $z_{i_1}, z_{i_2}, z_{i_3}$ gives us the desired result. Thus Lemma 2.8 is true if $2 \nmid k$.

This completes the proof of Lemma 2.8. □

3. Proofs of Theorem 1.4 and Corollary 1.6

In this section, we use the lemmas presented in the previous to give the proofs of Theorem 1.4 and Corollary 1.6. At first, we show Theorem 1.4.

Proof of Theorem 1.4. Since $\deg u(x) = k$, one may let $u(x) = \lambda x^k + \nu x^{k-1} + f_{\le k-2}(x)$ with $\lambda \in \mathbf{F}_q^*, \nu \in \mathbf{F}_q$ and $f_{\le k-2}(x) \in \mathbf{F}_q[x]$ being a polynomial of degree at most $k-2$. Then $(u(D), c_{k-1}(u(x))) = (u(D), \nu)$. By Lemma 2.2, we have that $(u(D), \nu)$ is a deep hole of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$ if and only if $(\lambda^{-1}u(D), \lambda^{-1}\nu)$ is a deep hole of $\mathrm{GPRS}_q(D, k)$. But $\lambda^{-1}u(x) = w_k(x) + r_k(x)$, where $w_k(x) := x^k$ and

$$r_k(x) := \lambda^{-1}\nu x^{k-1} + \lambda^{-1} f_{\le k-2}(x).$$

Then one has

$$(\lambda^{-1}u(D), \lambda^{-1}\nu) = (w_k(D) + r_k(D), \lambda^{-1}\nu) = (w_k(D), 0) + (r_k(D), \lambda^{-1}\nu).$$

Since $\deg r_k(x) \le k-1$, by the definition of $\mathrm{GPRS}_q(D, k)$ we have $(r_k(D), \lambda^{-1}\nu) \in \mathrm{GPRS}_q(D, k)$. Then it follows from Lemma 2.1 that $(\lambda^{-1}u(D), \lambda^{-1}\nu)$ is a deep hole of $\mathrm{GPRS}_q(D, k)$ if and only if $(w_k(D), 0)$ is a deep hole of $\mathrm{GPRS}_q(D, k)$. Then we can deduce that $(u(D), c_{k-1}(u(x)))$ is a deep hole of $\mathrm{GPRS}_q(D, k)$ if and only if $(w_k(D), 0)$ is a deep hole of $\mathrm{GPRS}_q(D, k)$.

We denote $\bar{w}_k := (w_k(D), 0)$. Let G be the generator matrix of $\mathrm{GPRS}_q(D, k)$ as given in (2.5). Then we have

$$\begin{aligned}\begin{pmatrix} G \\ \bar{w}_k \end{pmatrix} =& \begin{pmatrix} 1 & \dots & 1 & 0 \\ y_1 & \dots & y_{q-l} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ y_1^{k-2} & \dots & y_{q-l}^{k-2} & 0 \\ y_1^{k-1} & \dots & y_{q-l}^{k-1} & 1 \\ y_1^k & \dots & y_{q-l}^k & 0 \end{pmatrix}\\ :=&(\bar{G}_1, \dots, \bar{G}_{q-l}, \bar{G}_{q-l+1}).\end{aligned}$$

Now we pick $k+1$ distinct integers with $1 \le j_1 < \cdots < j_{k+1} \le q-l+1$.

Case 1. $j_{k+1} \le q - l$. Then one has

$$\det(\bar{G}_{j_1}, \ldots, \bar{G}_{j_{k+1}}) = \det\begin{pmatrix} 1 & \ldots & 1 \\ y_{j_1} & \ldots & y_{j_{k+1}} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-1} & \ldots & y_{j_{k+1}}^{k-1} \\ y_{j_1}^{k} & \ldots & y_{j_{k+1}}^{k} \end{pmatrix}$$
$$= V(y_{j_1}, \ldots, y_{j_{k+1}})$$
$$= \prod_{1\le t<s\le k+1} (y_{j_s} - y_{j_t}) \neq 0.$$

Case 2. $j_{k+1} = q - l + 1$. We can compute and get that

$$\det(\bar{G}_{j_1}, \ldots, \bar{G}_{j_k}, \bar{G}_{j_{q-l+1}}) = \det\begin{pmatrix} 1 & \ldots & 1 & 0 \\ y_{j_1} & \cdots & y_{j_k} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ y_{j_1}^{k-2} & \ldots & y_{j_k}^{k-2} & 0 \\ y_{j_1}^{k-1} & \ldots & y_{j_k}^{k-1} & 1 \\ y_1^{k} & \ldots & y_{j_k}^{k} & 0 \end{pmatrix}$$
$$= -\det\begin{pmatrix} 1 & \ldots & 1 \\ y_{j_1} & \cdots & y_{j_k} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-2} & \ldots & y_{j_k}^{k-2} \\ y_{j_1}^{k} & \ldots & y_{j_k}^{k} \end{pmatrix}. \tag{3.1}$$

Now we introduce an auxiliary polynomial $g(y)$ as follows:

$$g(y) = \det\begin{pmatrix} 1 & \ldots & 1 & 1 \\ y_{j_1} & \cdots & y_{j_k} & y \\ \vdots & \vdots & \vdots & \vdots \\ y_{j_1}^{k-1} & \ldots & y_{j_k}^{k-1} & y^{k-1} \\ y_{j_1}^{k} & \ldots & y_{j_k}^{k} & y^{k} \end{pmatrix}.$$

Then Lemma 2.4 tells us that

$$g(y) = \Big(\prod_{1\le s<t\le k} (y_{j_t} - y_{j_s})\Big) \prod_{i=1}^{k} (y - y_{j_i}) := \sum_{i=0}^{k} a_i y^i.$$

This infers that

$$a_{k-1} = -\Big(\sum_{i=1}^{k} y_{j_i}\Big) \prod_{1\le s<t\le k} (y_{j_t} - y_{j_s}). \tag{3.2}$$

But

$$a_{k-1} = -\det\begin{pmatrix} 1 & \dots & 1 \\ y_{j_1} & \cdots & y_{j_k} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-2} & \dots & y_{j_k}^{k-2} \\ y_{j_1}^{k} & \dots & y_{j_k}^{k} \end{pmatrix}. \tag{3.3}$$

Finally, (3.1) together with (3.2) and (3.3) gives us that

$$\det(\bar{G}_{j_1}, \dots, \bar{G}_{j_k}, \bar{G}_{j_{q-l+1}}) = -\Big(\sum_{i=1}^{k} y_{j_i}\Big) \prod_{1\le s<t\le k} (y_{j_t} - y_{j_s}). \tag{3.4}$$

By Lemma 2.5, we know that $\text{GPRS}_q(D, k)$ is a $[q - l + 1, k]$ MDS code which implies that

$$d(\text{GPRS}_q(D, k)) = q - l + 1 - k + 1 = q - l - k + 2.$$

Then by Lemma 2.6, one can deduce that

$$\begin{aligned} \rho(\text{GPRS}_q(D, k)) =& d(\text{GPRS}_q(D, k)) - 1 \\ =& q - l - k + 2 - 1 \\ =& q - l + 1 - k. \end{aligned} \tag{3.5}$$

It then follows immediately from Lemma 2.7 that $\bar{w}_k = (w_k(D), 0)$ is a deep hole of the generalized projective Reed-Solomon code $\text{GPRS}_q(D, k)$ if and only if the $(k + 1) \times (q - l + 1)$ matrix $\begin{pmatrix} G \\ \bar{w}_k \end{pmatrix}$ can be served as the generator matrix of a MDS code, if and only if any $k + 1$ columns of $\begin{pmatrix} G \\ \bar{w}_k \end{pmatrix}$ are linear independent, if and only if for any $1 \le j_1 < \dots < j_{k+1} \le q - l + 1$, one has

$$\det(\bar{G}_{j_1}, \dots, \bar{G}_{j_{k+1}}) \neq 0. \tag{3.6}$$

By the discussion in Cases 1 and 2, (3.4) tells us that (3.6) holds if and only if for any $1 \le j_1 < \dots < j_k \le q - l$, one has $\sum\limits_{i=1}^{k} y_{j_i} \neq 0$. Hence we can derive that $(w_k(D), 0)$ is a deep hole of the generalized projective Reed-Solomon code $\text{GPRS}_q(D, k)$ if and only if the sum $\sum\limits_{y\in I} y$ is nonzero for any subset $I \subseteq D$ with $\#(I) = k$ as desired.

Finally, we can conclude that $(u(D), c_{k-1}(u(x)))$ is a deep hole of the generalized projective Reed-Solomon code $\text{GPRS}_q(D, k)$ if and only if the sum $\sum\limits_{y\in I} y$ is nonzero for any subset $I \subseteq D$ with $\#(I) = k$.

This finishes the proof of Theorem 1.4. □

We can now use Theorem 1.4 to show Corollary 1.6.

Proof of Corollary 1.6. Let $l = 1$ and $a_1 = 0$. Then $D = \mathbf{F}_q^*$. By Lemma 2.8, there exist a subset $I \subseteq \mathbf{F}_q^*$ with $\#(I) = k$ such that $\sum\limits_{y\in I} y = 0$. It then follows from Theorem 1.4 that the received word $(u(\mathbf{F}_q^*), c_{k-1}(u(x)))=(u(\mathbf{F}_q^*), \gamma)$ is not a deep hole of the primitive projective Reed-Solomon code $\text{PPRS}_q(\mathbf{F}_q^*, k)$. Therefore Corollary 1.6 is proved. □

4. Proofs of Theorem 1.5 and Corollary 1.7

In this section, we give the proofs of Theorem 1.5 and Corollary 1.7. We begin with the proof of Theorem 1.5.

Proof of Theorem 1.5. First of all, we note that j is an integer with $1 \le j \le l$. We introduce a polynomial $f_j(x)$ as follows:

$$f_j(x) = (x - a_j)^{q-2},$$

and define a word $\bar{f}_j$ associated to $f_j(x)$ by

$$\bar{f}_j := (f_j(D), c_{k-1}(f_j(x))).$$

Then $u_j(x) = \lambda_j f_j(x) + \nu_j x^{k-1} + f^{(j)}_{\le k-2}(x)$ which implies that

$$c_{k-1}(u_j(x)) = \lambda_j c_{k-1}(f_j(x)) + \nu_j. \tag{4.1}$$

It follows from (4.1) that

$$\begin{aligned}
&(u_j(D), c_{k-1}(u_j(x)))\\
=&(\lambda_j f_j(D) + \nu_j x^{k-1}(D) + f^{(j)}_{\le k-2}(D), \lambda_j c_{k-1}(f_j(x)) + \nu_j)\\
=&(\lambda_j f_j(D), \lambda_j c_{k-1}(f_j(x))) + (\nu_j x^{k-1}(D) + f^{(j)}_{\le k-2}(D), \nu_j)\\
=&\lambda_j \bar{f}_j + (\nu_j x^{k-1}(D) + f^{(j)}_{\le k-2}(D), \nu_j).
\end{aligned}$$

But

$$\deg(\nu_j x^{k-1}(x) + f^{(j)}_{\le k-2}(x)) \le k - 1$$

and

$$c_{k-1}(\nu_j x^{k-1}(x) + f^{(j)}_{\le k-2}(x)) = \nu_j.$$

Hence

$$(\nu_j x^{k-1}(D) + f^{(j)}_{\le k-2}(D), \nu_j) \in \mathrm{GPRS}_q(D, k).$$

It follows from Lemmas 2.1 and 2.2 that the received word $(u_j(D), c_{k-1}(u_j(x)))$ is a deep hole of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$ if and only if $\bar{f}_j$ is a deep hole of $\mathrm{GPRS}_q(D, k)$.

Let G be the generator matrix of $\mathrm{GPRS}_q(D, k)$ as given in (2.5). Since $y_i \ne a_j$ for all integers i with $1 \le i \le q - l$, we have $(y_i - a_j)^{q-2} = (y_i - a_j)^{-1}$. It then follows that

$$\begin{aligned}
\begin{pmatrix} G \\ \bar{f}_j \end{pmatrix} =& \begin{pmatrix}
1 & \dots & 1 & 0\\
y_1 & \dots & y_{q-l} & 0\\
\vdots & \vdots & \vdots & \vdots\\
y_1^{k-2} & \dots & y_{q-l}^{k-2} & 0\\
y_1^{k-1} & \dots & y_{q-l}^{k-1} & 1\\
(y_1 - a_j)^{-1} & \dots & (y_{q-l} - a_j)^{-1} & c_{k-1}(f_j(x))
\end{pmatrix}\\
:=&(\hat{G}_1, \dots, \hat{G}_{q-l+1}).
\end{aligned} \tag{4.2}$$

On the other hand, from Lemma 2.7 we can deduce that $\bar{f}_j = (f_j(D), c_{k-1}(f_j(x)))$ is a deep hole of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D,k)$, if and only if $\begin{pmatrix} G \\ \bar{f}_j \end{pmatrix}$ generates a MDS code, by Lemma 2.3, if and only if any $k+1$ columns of $\begin{pmatrix} G \\ \bar{f}_j \end{pmatrix}$ are linear independent, if and only if for all $k+1$ integers $j_1, \ldots, j_{k+1}$ with $1 \le j_1 < \cdots < j_{k+1} \le q-l+1$, one has

$$\det(\hat{G}_{j_1}, \ldots, \hat{G}_{j_{k+1}}) \neq 0. \tag{4.3}$$

In what follows, we choose arbitrarily $k+1$ integers $j_1, \ldots, j_{k+1}$ such that $1 \le j_1 < \cdots < j_{k+1} \le q-l+1$. Consider the following two cases.

Case 1. $j_{k+1} \neq q-l+1$. Then $k+1 \le j_{k+1} \le q-l$ and by (4.2), one has

$$(\hat{G}_{j_1}, \ldots, \hat{G}_{j_{k+1}}) = \begin{pmatrix} 1 & \ldots & 1 \\ y_{j_1} & \ldots & y_{j_{k+1}} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-1} & \ldots & y_{j_{k+1}}^{k-1} \\ (y_{j_1}-a_j)^{-1} & \ldots & (y_{j_{k+1}}-a_j)^{-1} \end{pmatrix}.$$

Thus one can deduce that

$$\begin{aligned}
&\det(\hat{G}_{j_1}, \ldots, \hat{G}_{j_{k+1}}) \\
=&\left(\prod_{i=1}^{k+1}(y_{j_i}-a_j)^{-1}\right)\det\begin{pmatrix} y_{j_1}-a_j & \ldots & y_{j_{k+1}}-a_j \\ y_{j_1}(y_{j_1}-a_j) & \ldots & y_{j_{k+1}}(y_{j_{k+1}}-a_j) \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-1}(y_{j_1}-a_j) & \ldots & y_{j_{k+1}}^{k-1}(y_{j_{k+1}}-a_j) \\ 1 & \ldots & 1 \end{pmatrix} \\
=&\left(\prod_{i=1}^{k+1}(y_{j_i}-a_j)^{-1}\right)\det\begin{pmatrix} y_{j_1} & \ldots & y_{j_{k+1}} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k} & \ldots & y_{j_{k+1}}^{k} \\ 1 & \ldots & 1 \end{pmatrix} \\
=&(-1)^k\left(\prod_{i=1}^{k+1}(y_{j_i}-a_j)^{-1}\right)V(y_{j_1}, \ldots, y_{j_{k+1}}) \\
=&(-1)^k\left(\prod_{i=1}^{k+1}(y_{j_i}-a_j)^{-1}\right)\prod_{1\le s<t\le k+1}(y_{j_t}-y_{j_s}) \neq 0
\end{aligned}$$

since $y_{j_1}, \ldots, y_{j_{k+1}}$ are pairwise distinct.

Case 2. $j_{k+1} = q-l+1$. Then $1 \le j_1 < \cdots < j_k \le q-l$. From (4.2) and Lemma 2.4, we can deduce that

$$\det(\hat{G}_{j_1}, \ldots, \hat{G}_{j_k}, \hat{G}_{j_{q-l+1}})$$

$$
\begin{aligned}
&= \det \begin{pmatrix} 1 & \dots & 1 & 0 \\ y_{j_1} & \cdots & y_{j_k} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ y_{j_1}^{k-2} & \dots & y_{j_k}^{k-2} & 0 \\ y_{j_1}^{k-1} & \dots & y_{j_k}^{k-1} & 1 \\ (y_{j_1}-a_j)^{-1} & \dots & (y_{j_k}-a_j)^{-1} & c_{k-1}(f_j(x)) \end{pmatrix} \\
&= c_{k-1}(f_j(x)) \det \begin{pmatrix} 1 & \dots & 1 \\ y_{j_1} & \cdots & y_{j_k} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-1} & \dots & y_{j_k}^{k-1} \end{pmatrix} - \det \begin{pmatrix} 1 & \dots & 1 \\ y_{j_1} & \cdots & y_{j_k} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-2} & \dots & y_{j_k}^{k-2} \\ (y_{j_1}-a_j)^{-1} & \dots & (y_{j_k}-a_j)^{-1} \end{pmatrix} \\
&= c_{k-1}(f_j(x)) V(y_{j_1},\dots,y_{j_k}) - \det \begin{pmatrix} 1 & \dots & 1 \\ y_{j_1} & \cdots & y_{j_k} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-2} & \dots & y_{j_k}^{k-2} \\ (y_{j_1}-a_j)^{-1} & \dots & (y_{j_k}-a_j)^{-1} \end{pmatrix} \\
&= c_{k-1}(f_j(x)) V(y_{j_1},\dots,y_{j_k}) - \Big(\prod_{i=1}^{k}(y_{j_i}-a_j)^{-1}\Big) \det \begin{pmatrix} y_{j_1} & \dots & y_{j_k} \\ \vdots & \vdots & \vdots \\ y_{j_1}^{k-1} & \dots & y_{j_k}^{k-1} \\ 1 & \dots & 1 \end{pmatrix} \\
&= c_{k-1}(f_j(x)) V(y_{j_1},\dots,y_{j_k}) + (-1)^k \Big(\prod_{i=1}^{k}(y_{j_i}-a_j)^{-1}\Big) V(y_{j_1},\dots,y_{j_k}) \\
&= \Big(c_{k-1}(f_j(x)) + (-1)^k \prod_{i=1}^{k}(y_{j_i}-a_j)^{-1}\Big) \prod_{1\le s<t\le k}(y_{j_t}-y_{j_s}) \\
&= \Big(c_{k-1}(f_j(x)) + \prod_{i=1}^{k}(a_j-y_{j_i})^{-1}\Big) \prod_{1\le s<t\le k}(y_{j_t}-y_{j_s}). \qquad (4.4)
\end{aligned}
$$

Now from Cases 1 and 2, we can deduce by (4.4) that (4.3) holds for all $k+1$ integers $j_1,\dots,j_{k+1}$ with $1 \le j_1 < \cdots < j_{k+1} \le q-l+1$ if and only if for all integers $j_1,\dots,j_k$ with $1 \le j_1 < \cdots < j_k \le q-l$, one has

$$c_{k-1}(f_j(x)) + \prod_{i=1}^{k}(a_j-y_{j_i})^{-1} \neq 0,$$

which is equivalent to

$$c_{k-1}(f_j(x)) \prod_{i=1}^{k}(a_j-y_{j_i}) + e \neq 0. \qquad (4.5)$$

Since $f_j(x) = (x-a_j)^{q-2}$, the binomial theorem gives us that

$$c_{k-1}(f_j(x)) = \binom{q-2}{k-1}(-a_j)^{q-k-1}.$$

Then one derives that (4.5) holds for all integers $j_1, \ldots, j_k$ with $1 \le j_1 < \cdots < j_k \le q - l$ if and only if the following is true:

$$\binom{q-2}{k-1}(-a_j)^{q-k-1}\prod_{i=1}^{k}(a_j - y_{j_i}) + e \neq 0, \tag{4.6}$$

or equivalently,

$$\binom{q-2}{k-1}a_j^{q-k-1}\prod_{i=1}^{k}(y_{j_i} - a_j) + e \neq 0 \tag{4.7}$$

since q is odd. In other words, $\bar{f}_j = (f_j(D), c_{k-1}(f_j(x)))$ is a deep hole of the generalized projective Reed-Solomon code $\mathrm{GPRS}_q(D, k)$ if and only if the sum

$$\binom{q-2}{k-1}a_j^{q-1-k}\prod_{y\in I}(y - a_j) + e$$

is nonzero for any subset $I \subseteq D$ with $\#(I) = k$. Hence the desired result follows immediately. The proof of Theorem 1.5 is complete. □

We can now present the proof of Corollary 1.7 as the conclusion of this paper.

Proof of Corollary 1.7. Letting $l = 1$ and $a_1 = 0$ gives us that $D = \mathbf{F}_q^*$. Then it follows from $a_1 = 0$ that

$$\binom{q-2}{k-1}a_j^{q-1-k}\prod_{y\in I}(y - a_j) + e = 0 \cdot \binom{q-2}{k-1}\prod_{y\in I}(y - a_j) + e = e \neq 0$$

for any subset $I \subseteq D$ with $\#(I) = k$. Hence by Theorem 1.5, one can deduce that $(u_j(D), c_{k-1}(u_j(x))) = (u(\mathbf{F}_q^*), \delta)$ is a deep hole of $\mathrm{PPRS}_q(\mathbf{F}_q^*, k)$. This ends the proof of Corollary 1.7. □

Acknowledgments

The authors would like to thank the anonymous referees for their very careful reading of the manuscript and helpful comments. This work was supported partially by National Science Foundation of China Grant #11771304, by the Fundamental Research Funds for the Central Universities and by Foundation of Sichuan Provincial Department of Education under Grant # 2016ZB0342.

Conflict of interest

We declare that we have no conflict of interest.

References

1. Y. Li, D. Wan, *On error distance of Reed-Solomon codes*, Sci. China, Ser. A: Math., **51** (2008), 1982–1988.

2. V. Guruswami, M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometry codes*, IEEE Trans. Inform. Theory, **45** (1999), 1757–1767.
3. V. Guruswami, A. Vardy, *Maximum-likelihood decoding of Reed-Solomon codes is NP-hard*, IEEE Trans. Inform. Theory, **51** (2005), 2249–2256.
4. A. Dür, *The decoding of extended Reed-Solomon codes*, Discrete Math., **90** (1991), 21–40.
5. J. Li, D. Wan, *On the subset sum problem over finite fields*, Finite Fields Th. App., **14** (2008), 911–929.
6. R. Wu, S. Hong, *On deep holes of standard Reed-Solomon codes*, Sci. China Math., **55** (2012), 2447–2455.
7. S. Hong, R. Wu, *On deep holes of generalized Reed-Solomon codes,* AIMS Math., **1** (2016), 96–101.
8. J. Zhuang, D. Lin, C. Lv, *Determining deep hole trees of generalized Reed-Solomon codes and an application (in Chinese)*, Sci. Sin. Math., **47** (2017), 1615–1620.
9. J. Zhang, D. Wan, *On deep holes of projective Reed-Solomon codes*, 2016 IEEE Internal Symposium on Information Theory, (2016), 925–929.
10. X. Xu, S. Hong, Y. Xu, *On deep holes of primitive projective Reed-Solomon codes (in Chinese)*, Sci. Sin. Math., **48** (2018), 1087–1094.
11. J. Van lint, *Introduction to coding theory*, 3 Eds., Heidelberg: Springer-Verlag Berlin, 1998.

AIMS Press