Wuhan University
Journal of Natural Sciences

2023, Vol.28 No.1, 015-019

Article ID 1007-1202(2023)01-0015-05
DOI https://doi.org/10.1051/wujns/2023281015

On Deep Holes of Projective Reed-Solomon Codes over Finite Fields with Even Characteristic

XU Xiaofan
School of Big Data and Statistics, Sichuan Tourism University, Chengdu 610100, Sichuan, China

Abstract: Projective Reed-Solomon code is an important class of maximal distance separable codes in reliable communication and deep holes play important roles in its decoding. In this paper, we obtain two classes of deep holes of projective Reed-Solomon codes over finite fields with even characteristic. That is, let $\mathbb{F}_q$ be finite field with even characteristic, $k \in \{2, q-2\}$, and let $u(x)$ be the Lagrange interpolation polynomial of the first q components of the received vector $\boldsymbol{u} \in \mathbb{F}_q^{q+1}$. Suppose that the $(q+1)$-th component of $\boldsymbol{u}$ is 0, and $u(x)=\lambda x^k+f_{\leqslant k-2}(x), \lambda x^{q-2}+f_{\leqslant k-2}(x)$, where $\lambda \in \mathbb{F}_q^*$, and $f_{\leqslant k-2}(x)$ is a polynomial over $\mathbb{F}_q$ with degree no more than $k-2$. Then the received vector $\boldsymbol{u}$ is a deep hole of projective Reed-Solomon codes PRS($\mathbb{F}_q, k$). In fact, our result partially solved an open problem on deep holes of projective Reed-Solomon codes proposed by Wan in 2020.

Key words: finite field; even characteristic; projective Reed-Solomon code; deep hole
CLC number: O 236.2

0 Introduction

In 1960, Reed and Solomon[1] presented an important error correcting code, that is the so-called Reed-Solomon code. In 1987, Dur[2] defined a double extended Reed-Solomon code, which was later called projective Reed-Solomon code. He further studied the covering radius, decoding problem and the deep holes of projective Reed-Solomon codes in Refs.[3-5].

Now, we first recall the following definition of projective Reed-Solomon codes.

Definition 1[2] Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_q = \{\alpha_1, \cdots, \alpha_q = 0\}$. Then the projective Reed-Solomon codes of length $q+1$ with dimension k over $\mathbb{F}_q$ can defined as

$$\mathrm{PRS}(\mathbb{F}_q, k) := \{(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_q), c_{k-1}(f)) \in \mathbb{F}_q^{q+1} | f(x) \in \mathbb{F}_q[x], \deg f(x) \leqslant k-1\} \quad (1)$$

where $c_{k-1}(f)$ is the coefficient of x^{k-1} in $f(x)$.

Subsequently, we give the definition of deep holes of linear code C. To do this, for a received vector $\boldsymbol{u}$, we first define the error distance $d(\boldsymbol{u}, C)$ and the covering radius $\rho(C)$ of linear code C.

Definition 2[5] Let C be an $[n, k]$ linear code over $\mathbb{F}_q$. The error distance of a received vector $\boldsymbol{u} \in \mathbb{F}_q^n$ to code C is defined by

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

Received date: 2022-07-14
Foundation item: Supported by Foundation of Sichuan Tourism University (20SCTUTY01) and Initial Scientific Research Fund of Doctors in Sichuan Tourism University
Biography: XU Xiaofan, male, Ph. D., research direction: coding theory. E-mail: xxfsctu@163.com

where $d(\boldsymbol{u},\boldsymbol{v})$ is the Hamming distance of $\boldsymbol{u}$ and $\boldsymbol{v}$.

Clearly, $d(\boldsymbol{u},C)=0$ if and only if $\boldsymbol{u}\in C$.

For a given projective Reed-Solomon code $\mathrm{PRS}(\mathbb{F}_q,k)$, we define the Lagrange interpolation polynomial $u(x)$ of the first q components of received vector $\boldsymbol{u}=(u_1,\cdots,u_q,u_{q+1})\in\mathbb{F}_q^{q+1}$ by

$$u(x):=\sum_{i=1}^{q}u_i\prod_{\substack{j=1\\ j\neq i}}^{q}\frac{x-\alpha_j}{\alpha_i-\alpha_j} \tag{2}$$

Obviously, one has $u(\alpha_i)=u_i$ for $1\leqslant i\leqslant q$ and further $d(\boldsymbol{u},\mathrm{PRS}(\mathbb{F}_q,k))=0$ if and only if $\deg u(x)\leqslant k-1, c_{k-1}(u(x))=u_{q+1}$.

Definition 3[5] Let C be an $[n,k]$ linear code over $\mathbb{F}_q$. Then

$$\rho(C):=\max\{d(\boldsymbol{u},C)|\boldsymbol{u}\in\mathbb{F}_q^n\}$$

is called as the covering radius of C.

In fact, there is a well known conjecture on the covering radius of projective Reed-Solomon codes.

Conjecture 1[6] Let k be an integer with $2\leqslant k\leqslant q-2$. Suppose $2|q, k\in\{2,q-2\}$, then

$$\rho(\mathrm{PRS}(\mathbb{F}_q,k))=q-k+1.$$

otherwise, $\rho(\mathrm{PRS}(\mathbb{F}_q,k))=q-k$.

Now we can propose the definition of deep holes of linear code as follows.

Definition 4 [7] Let C be a $[n,k]$ linear code over $\mathbb{F}_q$. If the received vector $\boldsymbol{u}$ such that $d(\boldsymbol{u},C)=\rho(C)$, then $\boldsymbol{u}$ is called a deep hole of C.

In 2016, Zhang *et al*[8] proved that $(u(\alpha_1),\cdots,u(\alpha_q),0)+\mathrm{PRS}(\mathbb{F}_q,k)$ is a deep hole of projective Reed-Solomon codes $\mathrm{PRS}(\mathbb{F}_q,k)$ by solving the subset problem over finite field $\mathbb{F}_q$, where $u(x)=ax^k+f_{\leqslant k-1}(x)$, $a\in\mathbb{F}_q^*$, and $f_{\leqslant k-1}(x)$ is a polynomial over $\mathbb{F}_q$ with degree no more than $k-1$. Then, in 2017, Kaipa[9] studied the deep holes of projective Reed-Solomon codes $\mathrm{PRS}(\mathbb{F}_q,q-2)$ over $\mathbb{F}_q$ with odd characteristic. In 2018, Xu *et al*[10] proved that $(u(\alpha_1),\cdots,u(\alpha_{q-1}),0)+\mathrm{PRS}(\mathbb{F}_q^*,k)$ is a deep hole of $\mathrm{PRS}(\mathbb{F}_q^*,k)$, where $u(x)=ax^{q-2}+f_{\leqslant k-2}(x)$ with $a\in\mathbb{F}_q^*$ and $f_{\leqslant k-2}(x)$ being a polynomial over $\mathbb{F}_q$ whose degree not exceed $k-2$. In 2020, Zhang *et al*[6] completely determined all the deep holes of projective Reed-Solomon codes $\mathrm{PRS}(\mathbb{F}_q,q-3)$ by using the polynomial theory over finite fields and applying the finite geometry method. Meanwhile, they raised the following open problem.

Problem 1[6] For a given projective Reed-Solomon code $\mathrm{PRS}(\mathbb{F}_q,k)$, how to determine all its deep holes?

More results on deep holes of Reed-Solomon codes, one can see Refs.[11-15].

The main purpose of this paper is to study problem 1 over finite fields with even characteristic. Now, we describe the main theorem of this paper as following.

Theorem 1 Let $\mathbb{F}_q$ be finite field with even characteristic, $k\in\{2,q-2\}$. Let $u(x)$ be the Lagrange interpolation polynomial of the first q components of the received vector $\boldsymbol{u}\in\mathbb{F}_q^{q+1}$. Suppose that the $(q+1)$-th component of $\boldsymbol{u}$ is 0, and

$$u(x)=\lambda x^k+f_{\leqslant k-2}(x)$$

or

$$u(x)=\lambda x^{q-2}+f_{\leqslant k-2}(x),$$

where $\lambda\in\mathbb{F}_q^*$, and $f_{\leqslant k-2}(x)$ is a polynomial over $\mathbb{F}_q$ with degree no more than $k-2$. Then the received vector $\boldsymbol{u}$ is a deep hole of $\mathrm{PRS}(\mathbb{F}_q,k)$.

Actually, Theorem 1 partially solved Problem 1 raised by Ref.[6]. This paper is organized as follows. In Section 1, we supply some preliminary lemmas that are needed in the proof of Theorem 1. Then in Section 2, we present the proof of Theorem 1.

1 Preliminary Lemmas

In this section, we give some lemmas needed in the proof of Theorem 1. First, a formula of a special determinant over finite fields given as follows.

Lemma 1 Let $\{\beta_1,\cdots,\beta_n\}\subset\mathbb{F}_q^*$.Then

$$\det\begin{pmatrix}1&1&\cdots&1\\ \beta_1^2&\beta_2^2&\cdots&\beta_n^2\\ \vdots&\vdots&\vdots&\vdots\\ \beta_1^n&\beta_2^n&\cdots&\beta_n^n\end{pmatrix}=\left(\sum_{i=1}^{n}\beta_i^{-1}\right)\left(\prod_{i=1}^{n}\beta_i\right)\prod_{1\leqslant i<j\leqslant n}(\beta_j-\beta_i).$$

Proof Noticed that

$$\det\begin{pmatrix}1&1&\cdots&1&1\\ \beta_1&\beta_2&\cdots&\beta_n&x\\ \beta_1^2&\beta_2^2&\cdots&\beta_n^2&x^2\\ \vdots&\vdots&\vdots&\vdots&\vdots\\ \beta_1^n&\beta_2^n&\cdots&\beta_n^n&x^n\end{pmatrix}=\left(\prod_{i=1}^{n}(x-\beta_i)\right)\prod_{1\leqslant i<j\leqslant n}(\beta_j-\beta_i).$$

Then, one can immediately get Lemma 1 by comparing the coefficients of x on both sides of the above equality. This completes the proof of Lemma 1.

Next, we prove the following result on subset sum over finite fields with even characteristic.

Lemma 2 Let $\mathbb{F}_q$ be finite field with even characteristic. If $l\in\{1,2,q-3,q-2\}$, then the sum of any l different elements in $\mathbb{F}_q^*$ is nonzero.

Proof The Lemma 2 obviously holds when $l=1$. Put $\mathbb{F}_q^*=\{\gamma_1,\cdots,\gamma_{q-1}\}$. Now we give the proof for $l=2,q-3,q-2$, respectively.

Case 1. $l=2$. Without loss of generality, one can take two distinct elements of $\mathbb{F}_q^*$ as γ_1,γ_2. Since $\mathbb{F}_q$ is a finite filed with characteristic 2, hence one can get

$$\gamma_1+\gamma_2=\gamma_1-\gamma_2\neq 0.$$

Case 2. $l=q-3$. Without loss of generality, one can also choose $q-3$ distinct elements of $\mathbb{F}_q^*$ as $\gamma_1,\cdots,\gamma_{q-3}$. Notice that $\mathbb{F}_q$ is a finite filed with characteristic 2, therefore

$$\sum_{i=1}^{q-3}\gamma_i=\sum_{i=1}^{q-1}\gamma_i-\gamma_{q-2}-\gamma_{q-1}=\gamma_{q-2}-\gamma_{q-1},$$

and also $\gamma_{q-2}\neq\gamma_{q-1}$, thus $\sum_{i=1}^{q-3}\gamma_i\neq 0$.

Case 3. $l=q-2$. Without loss of generality, one can pick $q-2$ distinct elements $\gamma_1,\cdots,\gamma_{q-2}\in\mathbb{F}_q^*$. The character of $\mathbb{F}_q$ is 2 can tell us that

$$\sum_{i=1}^{q-2}\gamma_i=\sum_{i=1}^{q-1}\gamma_i-\gamma_{q-1}=\gamma_{q-1}\neq 0.$$

The proof of Lemma 2 is complete.

In 1991, Dur[3] had given the following result on covering radius of projective Reed-Solomon codes over finite fields with even characteristic by using the finite geometry method.

Lemma 3[3] Let $2|q$, $k\in\{2,q-2\}$. Then

$$\rho(\mathrm{PRS}(\mathbb{F}_q,k))=q-k+1.$$

Finally, we recall a theorem on the received vector $\boldsymbol{u}$ is whether or not a deep hole of maximal distance separable code C.

Lemma 4[16] Let C be $[n,k]$ maximal distance separable code over finite field $\mathbb{F}_q$. If the covering radius $\rho(C)$ of code C is $n-k$, then the received vector $\boldsymbol{u}\in\mathbb{F}_q^n$ is a deep hole of C if and only if any $k+1$ columns of the $(k+1)\times n$ matrix $\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{u}\end{pmatrix}$ is linearly independent, where $\boldsymbol{G}$ is the generator matrix of code C.

2 Proof of Theorem 1

In this section, we use the lemmas presented in Section 1 to give the proof of Theorem 1.

Proof Let $\mathbb{F}_q=\{x_1,\cdots,x_q=0\}$. By (1) and (2), one can immediately get that

$$\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{u}\end{pmatrix}=\begin{pmatrix}1 & 1 & \cdots & 1 & 0\\ x_1 & x_2 & \cdots & x_q & 0\\ x_1^2 & x_2^2 & \cdots & x_q^2 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ x_1^{k-1} & x_2^{k-1} & \cdots & x_q^{k-1} & 1\\ u(x_1) & u(x_2) & \cdots & u(x_q) & 0\end{pmatrix}$$

$$:=(\bar{\boldsymbol{G}}_1,\bar{\boldsymbol{G}}_2,\cdots,\bar{\boldsymbol{G}}_{q+1}).$$

Assume that $\bar{\boldsymbol{G}}_{j_1},\bar{\boldsymbol{G}}_{j_2},\cdots,\bar{\boldsymbol{G}}_{j_{k+1}}$ are any $k+1$ columns of $\begin{pmatrix}\boldsymbol{G}\\ \boldsymbol{u}\end{pmatrix}$, where $j_1,j_2,\cdots,j_{k+1}$ are arbitrary $k+1$ integers with $1\leqslant j_1<j_2<\cdots<j_{k+1}\leqslant q+1$. To complete the proof of the Theorem, it suffices to show

$$\det(\bar{\boldsymbol{G}}_{j_1},\bar{\boldsymbol{G}}_{j_2},\cdots,\bar{\boldsymbol{G}}_{j_{k+1}})\neq 0 \tag{3}$$

To do so, we give the proof as the following eight cases.

Case 1. $u(x)=\lambda x^k+f_{\leqslant k-2}(x)$. The four cases are considered as follows.

Case 1-1. $j_{k+1}<q$. At this time, one has

$$\det(\bar{\boldsymbol{G}}_{j_1},\bar{\boldsymbol{G}}_{j_2},\cdots,\bar{\boldsymbol{G}}_{j_{k+1}})=\det\begin{pmatrix}1 & 1 & \cdots & 1\\ x_{j_1} & x_{j_2} & \cdots & x_{j_{k+1}}\\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_{k+1}}^2\\ \vdots & \vdots & \vdots & \vdots\\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_{k+1}}^{k-1}\\ u(x_{j_1}) & u(x_{j_2}) & \cdots & u(x_{j_{k+1}})\end{pmatrix}$$

$$=\lambda\prod_{1\leqslant s<t\leqslant k+1}(x_{j_t}-x_{j_s})\neq 0 \tag{4}$$

Case 1-2. $j_{k+1}=q$. By $x_q=0$, one can know that

$$\det(\bar{\boldsymbol{G}}_{j_1},\bar{\boldsymbol{G}}_{j_2},\cdots,\bar{\boldsymbol{G}}_{j_{k+1}})=\lambda\det\begin{pmatrix}1 & 1 & \cdots & 1 & 1\\ x_{j_1} & x_{j_2} & \cdots & x_{j_k} & 0\\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_k}^2 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_k}^{k-1} & 0\\ x_{j_1}^k & x_{j_2}^k & \cdots & x_{j_k}^k & 0\end{pmatrix}$$

$$=(-1)^{k+2}\lambda\left(\prod_{i=1}^{k}x_{j_i}\right)\prod_{1\leqslant s<t\leqslant k}(x_{j_t}-x_{j_s})\neq 0 \tag{5}$$

Case 1-3. $j_k\leqslant q-1, j_{k+1}=q+1$. One can deduce that

$$\det(\bar{\boldsymbol{G}}_{j_1},\bar{\boldsymbol{G}}_{j_2},\cdots,\bar{\boldsymbol{G}}_{j_{k+1}})=\lambda\det\begin{pmatrix}1 & 1 & \cdots & 1 & 0\\ x_{j_1} & x_{j_2} & \cdots & x_{j_k} & 0\\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_k}^2 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_k}^{k-1} & 1\\ x_{j_1}^k & x_{j_2}^k & \cdots & x_{j_k}^k & 0\end{pmatrix}$$

$$=(-1)^{2k+1}\lambda\left(\sum_{i=1}^{k}x_{j_i}\right)\prod_{1\leqslant s<t\leqslant k}(x_{j_t}-x_{j_s}).$$

And also $2|q, k\in\{2,q-2\}$, it follows from Lemma 2 that $\sum_{i=1}^{k}x_{j_i}\neq 0$. Then one can derive that

$$\det(\bar{\boldsymbol{G}}_{j_1},\bar{\boldsymbol{G}}_{j_2},\cdots,\bar{\boldsymbol{G}}_{j_{k+1}})\neq 0 \tag{6}$$

Case 1-4. $j_k=q, j_{k+1}=q+1$. By $x_q=0$, one can derive that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}})$$

$$= \lambda \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 0 \\ x_{j_1} & x_{j_2} & \cdots & x_{j_{k-1}} & 0 & 0 \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_{k-1}}^2 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_{k-1}}^{k-1} & 0 & 1 \\ x_{j_1}^k & x_{j_2}^k & \cdots & x_{j_{k-1}}^k & 0 & 0 \end{pmatrix}$$

$$= (-1)^{3k+2} \lambda \left(\sum_{i=1}^{k-1} x_{j_i} \right) \left(\prod_{i=1}^{k-1} x_{j_i} \right) \prod_{1 \leqslant s < t \leqslant k-1} (x_{j_t} - x_{j_s}).$$

Notice that $k-1=1, q-3$, by Lemma 2, one can get $\sum_{i=1}^{k-1} x_{j_i} \neq 0$. It follows that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) \neq 0 \tag{7}$$

Case 2. $v(x) = \lambda x^{q-2} + f_{\leqslant k-2}(x)$. One only need to deal with the four cases as follows.

Case 2-1. $j_{k+1} < q$. Notice that for any integer i with $1 \leqslant i \leqslant k+1$, one has $x_{j_i}^{q-2} = x_{j_i}^{-1}$. It then follows that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) = \lambda \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_{j_1} & x_{j_2} & \cdots & x_{j_{k+1}} \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_{k+1}}^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_{k+1}}^{k-1} \\ x_{j_1}^{-1} & x_{j_2}^{-1} & \cdots & x_{j_{k+1}}^{-1} \end{pmatrix}$$

$$= (-1)^k \lambda \left(\prod_{i=1}^{k+1} x_{j_i}^{-1} \right) \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_{j_1} & x_{j_2} & \cdots & x_{j_{k+1}} \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_{k+1}}^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^k & x_{j_2}^k & \cdots & x_{j_{k+1}}^k \end{pmatrix}$$

$$= (-1)^k \lambda \left(\prod_{i=1}^{k+1} x_{j_i}^{-1} \right) \prod_{1 \leqslant s < t \leqslant k+1} (x_{j_t} - x_{j_s}) \neq 0 \tag{8}$$

Case 2-2. $j_{k+1} = q$. Since $x_{j_i}^{q-2} = x_{j_i}^{-1} (1 \leqslant i \leqslant k)$ and $x_q = 0$, so

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) = \lambda \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_{j_1} & x_{j_2} & \cdots & x_{j_k} & 0 \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_k}^2 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_k}^{k-1} & 0 \\ x_{j_1}^{-1} & x_{j_2}^{-1} & \cdots & x_{j_k}^{-1} & 0 \end{pmatrix}$$

$$= (-1)^{k+2} \lambda \left(\prod_{i=1}^{k} x_{j_i}^{-1} \right) \det \begin{pmatrix} x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_k}^2 \\ x_{j_1}^3 & x_{j_2}^3 & \cdots & x_{j_k}^3 \\ \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^k & x_{j_2}^k & \cdots & x_{j_k}^k \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

Then by Lemma 1, one can derive that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) = (-1)^{2k+1} \lambda \left(\sum_{i=1}^{k} x_{j_i}^{-1} \right) \prod_{1 \leqslant s < t \leqslant k} (x_{j_t} - x_{j_s}).$$

Now note that $k \in \{2, q-2\}$ and $x_{j_i}^{-1} \in \mathbb{F}_q^*$. Then Lemma 2 can tell us that $\sum_{i=1}^{k} x_{j_i}^{-1} \neq 0$. This implies

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) \neq 0 \tag{9}$$

Case 2-3. $j_k \leqslant q-1, j_{k+1} = q+1$. Since $x_{j_i}^{q-2} = x_{j_i}^{-1} (1 \leqslant i \leqslant k)$, one then can deduce that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) = \lambda \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 \\ x_{j_1} & x_{j_2} & \cdots & x_{j_k} & 0 \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_k}^2 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_k}^{k-1} & 1 \\ x_{j_1}^{-1} & x_{j_2}^{-1} & \cdots & x_{j_k}^{-1} & 0 \end{pmatrix}$$

$$= (-1)^{2k+1} \lambda \left(\prod_{i=1}^{k} x_{j_i}^{-1} \right) \det \begin{pmatrix} x_{j_1} & x_{j_2} & \cdots & x_{j_k} \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_k}^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_k}^{k-1} \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$= (-1)^{3k} \lambda \left(\prod_{i=1}^{k} x_{j_i}^{-1} \right) \prod_{1 \leqslant s < t \leqslant k} (x_{j_t} - x_{j_s}) \neq 0 \tag{10}$$

Case 2-4. $j_k = q, j_{k+1} = q+1$. Owing to $x_{j_i}^{q-2} = x_{j_i}^{-1} (1 \leqslant i \leqslant k-1)$ and $x_q = 0$, one then can get

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}})$$

$$= \lambda \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 0 \\ x_{j_1} & x_{j_2} & \cdots & x_{j_{k-1}} & 0 & 0 \\ x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_{k-1}}^2 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_{k-1}}^{k-1} & 0 & 1 \\ x_{j_1}^{-1} & x_{j_2}^{-1} & \cdots & x_{j_{k-1}}^{-1} & 0 & 0 \end{pmatrix}$$

$$= (-1)^{3k+2} \lambda \left(\prod_{i=1}^{k-1} x_{j_i}^{-1} \right) \det \begin{pmatrix} x_{j_1}^2 & x_{j_2}^2 & \cdots & x_{j_{k-1}}^2 \\ x_{j_1}^3 & x_{j_2}^3 & \cdots & x_{j_{k-1}}^3 \\ \vdots & \vdots & \vdots & \vdots \\ x_{j_1}^{k-1} & x_{j_2}^{k-1} & \cdots & x_{j_{k-1}}^{k-1} \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

By Lemma 1, one can deduce that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}})$$

$$= (-1)^{4k} \lambda \left(\prod_{i=1}^{k-1} x_{j_i}^{-1} \right) \left(\sum_{i=1}^{k-1} x_{j_i}^{-1} \right) \left(\prod_{i=1}^{k-1} x_{j_i}^{-1} \right) \prod_{1 \leqslant s < t \leqslant k-1} (x_{j_t} - x_{j_s})$$

$$= \lambda \left(\sum_{i=1}^{k-1} x_{j_i}^{-1} \right) \prod_{1 \leqslant s < t \leqslant k-1} (x_{j_t} - x_{j_s}).$$

Notice that $k-1=1, q-3$ and $x_{j_i}^{-1} \in \mathbb{F}_q^*$. Applying

Lemma 2, one can obtain $\sum_{i=1}^{k-1} x_{j_i}^{-1} \neq 0$. It yields that

$$\det(\bar{\boldsymbol{G}}_{j_1}, \bar{\boldsymbol{G}}_{j_2}, \cdots, \bar{\boldsymbol{G}}_{j_{k+1}}) \neq 0 \tag{11}$$

Thus, (3) can be immediately obtained from (4) - (11), that is, any $k+1$columns of $\begin{pmatrix} \boldsymbol{G} \\ \boldsymbol{u} \end{pmatrix}$ are linearly independent. On the other hand, PRS($\mathbb{F}_q, k$) is a maximal distance separable code and Lemma 3 also tell us that the covering radius of PRS($\mathbb{F}_q, k$) is

$$\rho(\mathrm{PRS}(\mathbb{F}_q, k)) = q - k + 1 = n - k.$$

Therefore, by Lemma 4, one can know that $\boldsymbol{u}$ is a deep hole of projective Reed-Solomon codes PRS($\mathbb{F}_q, k$). This finish the proof of Theorem 1.

References

[1] Reed S, Solomon G. Polynomial codes over certain finite fields[J]. *Journal of the Society for Industrial and Applied Mathematics*, 1960, **8**(2): 300-304.

[2] Dur A. The automorphism groups of Reed-Solomon codes [J]. *J Combin Theory*, *Ser A*, 1987, **44**(1): 69-82.

[3] Dur A. The decoding of extended Reed-Solomon codes[J]. *Discrete Math*, 1991, **90**(1): 21-40.

[4] Dur A. Complete decoding of doubly-extended Reed-Solomon codes of minimum distance 5 and 6[J]. *Discrete Appl Math*, 1991, **33**(1/2/3): 95-107.

[5] Dur A. On the covering radius of Reed-Solomon codes[J]. *Discrete Math*, 1994, **126**(1/2/3): 99-105.

[6] Zhang J, Wan D Q, Kaipa K. Deep holes of projective Reed-Solomon codes[J]. *IEEE Trans Inform Theory*, 2020, **66**(4): 2392-2401.

[7] Cheng Q, Murray E. On deciding deep holes of Reed-Solomon codes[J]. *Lecture Notes in Comput Sci*, 2007, **4484**: 296-305.

[8] Zhang J, Wan D Q. On deep holes of projective Reed-Solomon codes[C]//2016 *IEEE International Symposium Information Theory.* Washington D C: IEEE, 2016: 925-929.

[9] Kaipa K. Deep holes and MDS extensions of Reed-Solomon codes[J]. *IEEE Trans Inform Theory*, 2017, **63**(8): 4940-4948.

[10] Xu X F, Hong S F, Xu Y C. On deep holes of primitive projective Reed-Solomon codes[J]. *Sci Sin Math*, 2018, **48**(8): 1087-1094.

[11] Hong S F, Wu R J. On deep holes of generalized Reed-Solomon codes[J]. *AIMS Math*, 2016, **1**(2): 96-101.

[12] Keti M, Wan D. Deep holes in Reed-Solomon codes based on Dickson polynomials[J]. *Finite Fields Appl*, 2016, **40**: 110-125.

[13] Li Y J, Wan D Q. On error distance of Reed-Solomon codes [J]. *Sci China Ser A*, 2008, **51**(11): 1982-1988.

[14] Li Y J, Zhu G Z. On the error distance of extended Reed-Solomon codes[J]. *Adv Math Commun*, 2016, **10**(2): 413-427.

[15] Wu R J, Hong S F. On deep holes of standard Reed-Solomon codes[J]. *Science China Math*, 2012, **55**(12): 2447-2455.

[16] Zhuang J C, Cheng Q, Li J Y. On determing deep holes of generalized Reed-Solomon codes[J]. *IEEE Trans Inform Theory*, 2016, **62**(1): 199-207.

□