AIMS Mathematics

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

AIMS Mathematics, 4(5): 1336–1347.
DOI:10.3934/math.2019.5.1336
Received: 23 July 2019
Accepted: 26 August 2019
Published: 04 September 2019

Research article

Some results on ordinary words of standard Reed-Solomon codes

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

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

* **Correspondence:** Email: sfhong@scu.edu.cn; Tel: +862885412720; Fax: +862885471501.

Abstract: The Reed-Solomon codes are widely used to establish a reliable channel to transmit information in digital communication which has a strong error correction capability and a variety of efficient decoding algorithm. We usually use the maximum likelihood decoding algorithm (MLD) in the decoding process of Reed-Solomon codes. MLD algorithm lies in determining its error distance. Li, Wan, Hong and Wu et al obtained some results on the error distance. For the Reed-Solomon code $RS_q(\mathbb{F}_q^*, k)$, the received word $\mathbf{u}$ is called an ordinary word of $RS_q(\mathbb{F}_q^*, k)$ if the error distance $d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = n - \deg(u(x))$ with $u(x)$ being the Lagrange interpolation polynomial of $\mathbf{u}$. In this paper, we make use of the polynomial method and particularly, we use the König-Rados theorem on the number of nonzero solutions of polynomial equation over finite fields to show that if $q \geq 4, 2 \leq k \leq q-2$, then the received word $\mathbf{u} \in \mathbb{F}_q^{q-1}$ of degree $q-2$ is an ordinary word of $RS_q(\mathbb{F}_q^*, k)$ if and only if its Lagrange interpolation polynomial $u(x)$ is of the form

$$u(x) = \lambda \sum_{i=k}^{q-2} a^{q-2-i} x^i + f_{\leq k-1}(x)$$

with $a, \lambda \in \mathbb{F}_q^*$ and $f_{\leq k-1}(x) \in \mathbb{F}_q[x]$ being of degree at most $k-1$. This answers partially an open problem proposed by J.Y. Li and D.Q. Wan in [On the subset sum problem over finite fields, Finite Fields Appls. 14 (2008), 911-929].

Keywords: Reed-Solomon code; ordinary word; König-Rados theorem
Mathematics Subject Classification: 11C08, 94B35

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let $D = \{x_1, \cdots, x_n\}$ be a subset of $\mathbb{F}_q$, which is called the *evaluation set*. The *generalized Reed-Solomon code* $RS_q(D, k)$ of length n and dimension k over $\mathbb{F}_q$ is defined as follows:

$$RS_q(D,k) := \{(f(x_1),\cdots,f(x_n)) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \le k-1\}.$$

If $D = \mathbb{F}_q^*$, then it is called *standard Reed-Solomon code*, i.e.,

$$RS_q(\mathbb{F}_q^*,k) := \{(f(1),f(\alpha),\cdots,f(\alpha^{q-2})) \in \mathbb{F}_q^n \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \le k-1\}, \tag{1.1}$$

where α is a primitive element of $\mathbb{F}_q$. We refer the above definition as the polynomial code version of the standard Reed-Solomon code. If $D = \mathbb{F}_q$, then it is called the *extended Reed-Solomon code*. For any $[n,k]_q$ linear code C, the *minimum distance* $d(C)$ is defined by

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

where $d(\cdot,\cdot)$ denotes the *Hamming distance* of two words which is the number of different entries of them and $w(\cdot)$ denotes the *Hamming weight* of a word which is the number of its non-zero entries. Since the Reed-Solomon code is a linear code, we have

$$d(C) = \min_{0\neq\mathbf{x}\in C}\{d(\mathbf{x},0)\} = \min_{0\neq\mathbf{x}\in C}\{w(\mathbf{x})\}.$$

The *error distance* to code C of a received word $\mathbf{u} \in \mathbb{F}_q^n$ is defined by

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

Clearly, $d(\mathbf{u},C) = 0$ if and only if $\mathbf{u} \in C$. The most important algorithmic problem in coding theory is the maximum likelihood decoding (MLD): Given a received word $\mathbf{u} \in \mathbb{F}_q^n$, find a codeword $\mathbf{v} \in C$ such that $d(\mathbf{u},\mathbf{v}) = d(\mathbf{u},C)$, then we decode $\mathbf{u}$ to $\mathbf{v}$ [4]. Therefore, it is very crucial to decide $d(\mathbf{u},C)$ for the word $\mathbf{u}$. When decoding the generalized Reed-Solomon code $RS_q(D,k)$, for a received word $\mathbf{u} = (u_1,\cdots,u_n) \in \mathbb{F}_q^n$, we define the Lagrange interpolation polynomial $u(x)$ of $\mathbf{u}$ by

$$u(x) := \sum_{i=1}^{n} u_i \prod_{\substack{j=1\\ j\neq i}}^{n} \frac{x-x_j}{x_i-x_j} \in \mathbb{F}_q[x], \tag{1.2}$$

i.e., $u(x)$ is the unique polynomial of degree $\deg(u(x)) \le n-1$ such that $u(x_i) = u_i$ for $1 \le i \le n$. For $\mathbf{u} \in \mathbb{F}_q^n$, we define the degree of $u(x)$ to be the *degree* of $\mathbf{u}$, i.e., $\deg(\mathbf{u}) := \deg(u(x))$. It is clear that $\mathbf{u} \in RS_q(D,k)$ if and only if $d(\mathbf{u},RS_q(D,k)) = 0$ if and only if $\deg(\mathbf{u}) \le k-1$. Equivalently, $\mathbf{u} \notin RS_q(D,k)$ if and only if $d(\mathbf{u},RS_q(D,k)) \ge 1$ if and only if $k \le \deg(\mathbf{u}) \le n-1$. Evidently, we have the following simple bounds due to Li and Wan [3].

Theorem 1.1. [3] *Let* $\mathbf{u}$ *be a received word such that* $\mathbf{u} \notin RS_q(D,k)$*. Then*

$$n - \deg(\mathbf{u}) \le d(\mathbf{u},RS_q(D,k)) \le n-k.$$

Let $\mathbf{u} \in \mathbb{F}_q^n$. If $d(\mathbf{u},RS_q(D,k)) = n-k$, then the received word $\mathbf{u}$ is called a *deep hole* of $RS_q(D,k)$. In 2007, Cheng and Murray [1] conjectured that a word $\mathbf{u}$ is a deep hole of $RS_q(\mathbb{F}_q^*,k)$ if and only if

$u(x) = ax^k + f_{\leq k-1}(x)$, where $u(x)$ is the Lagrange interpolation polynomial of the received word $\mathbf{u}$ and $a \in \mathbb{F}_q^*$. In 2012, Wu and Hong [9] disproved this conjecture by presenting a new class of deep holes for standard Reed-Solomon codes $RS_q(\mathbb{F}_q^*, k)$. In fact, let $q \geq 4$ and $2 \leq k \leq q-2$. They showed that the received word $\mathbf{u}$ is a deep hole if its Lagrange interpolation polynomial equals $ax^{q-2} + f_{\leq k-1}(x)$. Later on, the main result of [9] is extended to the generalized Reed-Solomon code in [2]. Recently, some progress on deep holes of generalized projective Reed-Solomon codes are made in [10] and [11].

On the other hand, the received word $\mathbf{u}$ is called an *ordinary word* of $RS_q(D,k)$ if $d(\mathbf{u}, RS_q(D,k)) = n - \deg(u(x))$. If $\deg(\mathbf{u}) = k$, then the upper bound is equal to the lower bound which implies that $\mathbf{u}$ is a deep hole and also an ordinary word. This immediately gives $(q-1)q^k$ ordinary words. We call these *trivial ordinary words*. It is an interesting problem to determine all the ordinary words. In 2008, Li and Wan [3] proposed an open problem to determine all the ordinary words of the standard Reed-Solomon code. In [4], by using Weil's estimate on character sums, the following result is obtained.

Theorem 1.2. [4] *Let* $\mathbf{u} \in \mathbb{F}_q^q$ *be such that* $k+1 \leq \deg(\mathbf{u}) \leq q-1$. *Assume that* $q > \max((\deg(\mathbf{u}))^2, (\deg(\mathbf{u}) - k - 1)^{2+\epsilon})$ *and* $k > (\frac{4}{\epsilon} + 1)(\deg(\mathbf{u}) - k) + \frac{4}{\epsilon} + 2$ *for some constant* $\epsilon > 0$. *Then* $\mathbf{u}$ *is an ordinary word of extended Reed-Solomon code* $RS_q(\mathbb{F}_q, k)$.

Furthermore, using Weil's character sum estimate and Li-Wan sieve for distinct coordinates counting, Zhu and Wan [12] showed the following result.

Theorem 1.3. [12] *Let* $\mathbf{u} \in \mathbb{F}_q^q$ *be such that* $k+1 \leq \deg(\mathbf{u}) \leq q-1$. *If there are positive constants* c_1 *and* c_2 *such that* $\deg(\mathbf{u}) - k < c_1 q^{1/2}, (\deg(\mathbf{u}) - k + 1)\log_2 q < k < c_2 q$, *then* $\mathbf{u}$ *is an ordinary word of extended Reed-Solomon code* $RS_q(\mathbb{F}_q, k)$.

In [5], Li and Zhu proved the following result.

Theorem 1.4. [5] *Let* $3 \leq k+2 \leq q-1$, *and* $\mathbf{u} \in \mathbb{F}_q^q$ *be represented by polynomial* $u(x) = x^{k+2} - bx^{k+1} + cx^k + v(x)$ *with* $\deg v(x) \leq k-1$. *If* $k+2 = q-1$ *and* $b^2 = c$, *then* $\mathbf{u}$ *is an ordinary word of extended Reed-Solomon code* $RS_q(\mathbb{F}_q, k)$.

In this paper, we make use of a well-known result, i.e. the so-called König-Rados theorem, to find all the ordinary words of degree $q-2$ of standard Reed-Solomon code $RS_q(\mathbb{F}_q^*, k)$. The main result of this paper can be stated as follows.

Theorem 1.5. *Let* $q \geq 4, 2 \leq k \leq q-2$ *and* $\mathbf{u} \in \mathbb{F}_q^{q-1}$ *be a received word with* $u(x)$ *being its Lagrange interpolation polynomial and* $\deg u(x) = q-2$. *Then* $\mathbf{u}$ *is an ordinary word of* $RS_q(\mathbb{F}_q^*, k)$ *if and only if* $u(x)$ *is of the following form*

$$u(x) = \lambda \sum_{i=k}^{q-2} a^{q-2-i} x^i + f_{\leq k-1}(x)$$

with $a, \lambda \in \mathbb{F}_q^*$ *and* $f_{\leq k-1}(x) \in \mathbb{F}_q[x]$ *being of degree at most* $k-1$.

If one picks $k = q-2$, then the ordinary words given by Theorem 1.5 are just the trivial ones. From Theorem 1.5, the following interesting result follows immediately.

Proposition 1.6. *Let $q \geq 4, 2 \leq k \leq q-2$. Then the number of ordinary words of degree $q-2$ of the standard Reed-Solomon code $RS_q(\mathbb{F}_q^*, k)$ is equal to $(q-1)^2 q^k$.*

This paper is organized as follows. First, in Section 2, we show several preliminary lemmas that are needed in the proof of Theorem 1.5. Consequently, we show Theorem 1.5 in Section 3. Finally, we present two examples to illustrate the validity of our main result.

2. Auxiliary lemmas

In this section, our main goal is to prove several lemmas that are needed in the proof of Theorem 1.5. In what follows, we let

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

and

$$f(\mathbb{F}_q^*) := (f(1), f(\alpha), \cdots, f(\alpha^{q-2})),$$

where α is a primitive element of $\mathbb{F}_q$. We begin with the following lemma.

Lemma 2.1. *Let $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^{q-1}$ be two words. If $\mathbf{u} = \lambda\mathbf{v} + f_{\leq k-1}(\mathbb{F}_q^*)$, where $\lambda \in \mathbb{F}_q^*$ and $f_{\leq k-1}(x) \in \mathbb{F}_q[x]$ is a polynomial of degree at most $k-1$. Then each of the following is true:*

(i). *We have $d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = d(\mathbf{v}, RS_q(\mathbb{F}_q^*, k))$.*

(ii). *The word $\mathbf{u}$ is an ordinary word of $RS_q(\mathbb{F}_q^*, k)$ if and only if the word $\mathbf{v}$ is an ordinary word of $RS_q(\mathbb{F}_q^*, k)$.*

Proof. (i). Since $RS_q(\mathbb{F}_q^*, k)$ is a linear code, we obtain that

$$\begin{aligned}
d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) &= \min_{\mathbf{c}\in RS_q(\mathbb{F}_q^*,k)} \{d(\mathbf{u}, \mathbf{c})\} \\
&= \min_{\mathbf{c}\in RS_q(\mathbb{F}_q^*,k)} \{d(\lambda\mathbf{v} + f_{\leq k-1}(\mathbb{F}_q^*), \mathbf{c})\} \\
&= \min_{\mathbf{c}\in RS_q(\mathbb{F}_q^*,k)} \{d(\lambda\mathbf{v} + f_{\leq k-1}(\mathbb{F}_q^*), \mathbf{c} + f_{\leq k-1}(\mathbb{F}_q^*))\} \\
&= \min_{c(x)\in P_{k-1}} \#\{x \in \mathbb{F}_q^* | \lambda v(x) + f_{\leq k-1}(x) - c(x) - f_{\leq k-1}(x) \neq 0\} \\
&= \min_{c(x)\in P_{k-1}} \#\{x \in \mathbb{F}_q^* | \lambda v(x) - c(x) \neq 0\} \\
&= \min_{\mathbf{c}\in RS_q(\mathbb{F}_q^*,k)} \{d(\lambda\mathbf{v}, \mathbf{c})\} \\
&= \min_{\mathbf{c}\in RS_q(\mathbb{F}_q^*,k)} \{d(\lambda\mathbf{v}, \lambda\mathbf{c})\} (\text{since } \lambda \in \mathbb{F}_q^*) \\
&= \min_{c(x)\in P_{k-1}} \#\{x \in \mathbb{F}_q^* | \lambda v(x) - \lambda c(x) \neq 0\} \\
&= \min_{c(x)\in P_{k-1}} \#\{x \in \mathbb{F}_q^* | v(x) - c(x) \neq 0\} \\
&= \min_{\mathbf{c}\in RS_q(\mathbb{F}_q^*,k)} \{d(\mathbf{v}, \mathbf{c})\} \\
&= d(\mathbf{v}, RS_q(\mathbb{F}_q^*, k))
\end{aligned}$$

as desired.

(ii). Since $\mathbf{u} = \lambda\mathbf{v} + f_{\leq k-1}(\mathbb{F}_q^*)$, one has $\deg\mathbf{u} = \deg\mathbf{v}$. Hence $\mathbf{u}$ is an ordinary word of $RS_q(\mathbb{F}_q^*, k)$ if and only if

$$d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = q - 1 - \deg\mathbf{u},$$

if and only if

$$d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = q - 1 - \deg\mathbf{v}. \tag{2.1}$$

But part (i) tells us that $d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = d(\mathbf{v}, RS_q(\mathbb{F}_q^*, k))$. So (2.1) holds if and only if

$$d(\mathbf{v}, RS_q(\mathbb{F}_q^*, k)) = q - 1 - \deg\mathbf{v}. \tag{2.2}$$

So $\mathbf{u}$ is ordinary holds if and only if (2.2) is true. In other words, $\mathbf{u}$ is ordinary if and only if $\mathbf{v}$ is ordinary.

This completes the proof of Lemma 2.1. □

Consequently, we give another useful fact.

Lemma 2.2. *Let $\mathbf{u} \in \mathbb{F}_q^{q-1}$ be a received word and $u(x)$ be its Lagrange interpolation polynomial. Then one has*

$$d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = q - 1 - \max_{v(x)\in P_{k-1}} \#\{\beta \in \mathbb{F}_q^* | u(\beta) = v(\beta)\}.$$

Proof. By (1.1), we have

$$\begin{aligned} d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) &= \min_{\mathbf{v}\in RS_q(\mathbb{F}_q^*,k)} \{d(\mathbf{u}, \mathbf{v})\} \\ &= \min_{v(x)\in P_{k-1}} \#\{1 \leq i \leq q-1 | u(\alpha^{i-1}) \neq v(\alpha^{i-1})\} \\ &= q - 1 - \max_{v(x)\in P_{k-1}} \#\{1 \leq i \leq q-1 | u(\alpha^{i-1}) = v(\alpha^{i-1})\} \\ &= q - 1 - \max_{v(x)\in P_{k-1}} \#\{\beta \in \mathbb{F}_q^* | u(\beta) = v(\beta)\} \end{aligned}$$

as required.

The proof of Lemma 2.2 is complete. □

The following result gives a formula on the number of nonzero solutions of polynomial equation over finite fields and is due to König and Rados (see, for instance, [6–8]). It is a key and important ingredient in the proof of our main result.

Lemma 2.3. (König-Rados) ([6–8]) *Let $f(x) = a_0 + a_1x + \cdots + a_{q-2}x^{q-2} \in \mathbb{F}_q[x]$. Then the number of nonzero solution of equation $f(x) = 0$ in $\mathbb{F}_q$ is equal to $q - 1 - \mathrm{rank}(A)$, where A is the left $(q-1)\times(q-1)$ circulant matrix defined by*

$$A := \begin{pmatrix} a_0 & a_1 & \ldots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \ldots & a_{q-2} & a_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{q-2} & a_0 & \ldots & a_{q-4} & a_{q-3} \end{pmatrix}.$$

3. Proof of Theorem 1.5

In this section, we use the lemmas presented in the previous section to give the proof of Theorem 1.5.

Proof of Theorem 1.5. First of all, we show the sufficiency part. Let

$$u(x) = \lambda \sum_{i=k}^{q-2} a^{q-2-i} x^i + f_{\leq k-1}(x),$$

where a and $\lambda \in \mathbb{F}_q^*$, $f_{\leq k-1}(x) \in \mathbb{F}_q[x]$ is a polynomial of degree at most $k-1$. Define

$$u_k(x) := \sum_{i=k}^{q-2} a^{q-2-i} x^i. \tag{3.1}$$

Then $u(x) = \lambda u_k(x) + f_{\leq k-1}(x)$. Now we pick a primitive element α of $\mathbb{F}_q$ and let

$$\mathbf{u}_k := (u_k(1), u_k(\alpha), \cdots, u_k(\alpha^{q-2})).$$

By Lemma 2.1, one gets that

$$d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = d(\mathbf{u}_k, RS_q(\mathbb{F}_q^*, k)).$$

Therefore, in order to show that

$$\mathbf{u} := (u(1), u(\alpha), \cdots, u(\alpha^{q-2}))$$

is an ordinary word, it suffices to prove that $\mathbf{u}_k$ is an ordinary word. Equivalently, we need only to show that

$$d(\mathbf{u}_k, RS_q(\mathbb{F}_q^*, k)) = q - 1 - \deg u_k(x) = 1, \tag{3.2}$$

since $\deg u_k(x) = q-2$. This will be done in what follows.

By Lemma 2.2, we have

$$d(\mathbf{u}_k, RS_q(\mathbb{F}_q^*, k)) = q - 1 - \max_{v(x)\in P_{k-1}} \#\{\beta \in \mathbb{F}_q^* | u_k(\beta) = v(\beta)\}. \tag{3.3}$$

For any $v(x) \in P_{k-1}$, one has $\deg v(x) \leq k-1$. But $\deg u_k(x) = q-2 \geq k$. Hence

$$\deg(u_k(x) - v(x)) = \deg u_k(x).$$

It then follows that for any $v(x) \in P_{k-1}$, one has

$$\begin{aligned} &\#\{\gamma \in \mathbb{F}_q^* | u_k(\gamma) = v(\gamma)\} \\ =&\#\{\gamma \in \mathbb{F}_q^* | u_k(\gamma) - v(\gamma) = 0\} \\ \leq& \deg(u_k(x) - v(x)) \\ =& \deg u_k(x) = q-2. \end{aligned} \tag{3.4}$$

On the other hand, we take

$$v_0(x) := -\sum_{i=0}^{k-1} a^{q-2-i}x^i.$$

Then $v_0(x) \in P_{k-1}$. Furthermore, by (3.1) we have

$$\begin{aligned}
&\#\{\gamma \in \mathbb{F}_q^* | u_k(\gamma) - v_0(\gamma) = 0\} \\
=&\#\Big\{\gamma \in \mathbb{F}_q^* \Big| \sum_{i=k}^{q-2} a^{q-2-i}\gamma^i + \sum_{i=0}^{k-1} a^{q-2-i}\gamma^i = 0\Big\} \\
=&\#\Big\{\gamma \in \mathbb{F}_q^* \Big| \sum_{i=0}^{q-2} a^{q-2-i}\gamma^i = 0\Big\}.
\end{aligned} \tag{3.5}$$

Since

$$x^{q-1} - 1 = \prod_{i=1}^{q-1}(x - \alpha^i)$$

and $a \in \mathbb{F}_q^*$ implying that

$$x^{q-1} - 1 = (x - a)\sum_{i=0}^{q-2} a^{q-2-i}x^i,$$

it then follows that

$$\sum_{i=0}^{q-2} a^{q-2-i}x^i = \frac{\prod_{i=1}^{q-1}(x - \alpha^i)}{x - a}.$$

This infers that

$$\Big\{\gamma \in \mathbb{F}_q^* \Big| \sum_{i=0}^{q-2} a^{q-2-i}\gamma^i = 0\Big\} = \mathbb{F}_q^* \setminus \{a\},$$

from which one can derive that

$$\#\Big\{\gamma \in \mathbb{F}_q^* \Big| \sum_{i=0}^{q-2} a^{q-2-i}\gamma^i = 0\Big\} = q - 2. \tag{3.6}$$

So (3.4) together with (3.5) and (3.6) implies that

$$\max_{v(x)\in P_{k-1}} \#\Big\{\gamma \in \mathbb{F}_q^* \Big| u_k(\gamma) - v(\gamma) = 0\Big\} = q - 2. \tag{3.7}$$

Hence (3.2) follows immediately from (3.3) and (3.7). So $\mathbf{u}$ is an ordinary word of $RS_q(\mathbb{F}_q^*, k)$. This finishes the proof of the sufficiency part.

Now we turn our attention to the proof of the necessity part. Let $\mathbf{u}$ be an ordinary word of $RS_q(\mathbb{F}_q^*, k)$ and $\deg u(x) = q - 2$. Then by the definition of ordinary word, we have

$$d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = q - 1 - (q - 2) = 1.$$

Hence by Lemma 2.2, one has

$$\max_{v(x)\in P_{k-1}} \#\{x_i \in \mathbb{F}_q^* | u(x) - v(x) = 0\} = q - 1 - d(\mathbf{u}, RS_q(\mathbb{F}_q^*, k)) = q - 1 - 1 = q - 2.$$

Notice that for any $v(x) \in P_{k-1}$, one has

$$\#\{x_i \in \mathbb{F}_q^* | u(x) - v(x) = 0\} \le \deg(u(x) - v(x)) = q - 2.$$

So there is a polynomial $v_0(x) \in P_{k-1}$ such that

$$\#\{x \in \mathbb{F}_q^* | u(x) - v_0(x) = 0\} = q - 2.$$

Write

$$u(x) = \sum_{i=0}^{q-2} u_i x^i$$

and

$$v_0(x) = \sum_{i=0}^{k-1} v_i x^i.$$

Let $u_{q-2} = \lambda$. Since $\deg u(x) = q - 2$, one has $\lambda \in \mathbb{F}_q^*$. Then

$$\begin{aligned} u(x) - v_0(x) &= \sum_{i=0}^{q-2} u_i x^i - \sum_{i=0}^{k-1} v_i x^i \\ &= \sum_{i=k}^{q-2} u_i x^i + \sum_{i=0}^{k-1} (u_i - v_i) x^i \\ &= \lambda \Big(\sum_{i=k}^{q-2} \lambda^{-1} u_i x^i + \sum_{i=0}^{k-1} \lambda^{-1}(u_i - v_i) x^i \Big) \text{ (since } \lambda \in \mathbb{F}_q^*) \\ &:= \lambda \sum_{i=0}^{q-2} c_i x^i, \end{aligned}$$

with $c_i = \lambda^{-1} u_i$ for all integers i with $k \le i \le q-2$ and $c_i = \lambda^{-1}(u_i - v_i)$ for all integers i with $0 \le i \le k-1$. One then deduces that

$$\#\Big\{x \in \mathbb{F}_q^* \Big| \sum_{i=0}^{q-2} c_i x^i = 0\Big\} = q - 2. \tag{3.8}$$

On the other hand, Lemma 2.3 yields that

$$\#\Big\{x \in \mathbb{F}_q^* \Big| \sum_{i=0}^{q-2} c_i x^i = 0\Big\} = q - 1 - \mathrm{rank}(B), \tag{3.9}$$

where B is the left circulant matrix defined by

$$B := \begin{pmatrix} c_0 & c_1 & \dots & c_{q-3} & c_{q-2} \\ c_1 & c_2 & \dots & c_{q-2} & c_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{q-2} & c_0 & \dots & c_{q-4} & c_{q-3} \end{pmatrix}.$$

So from (3.8) and (3.9), we derive that rank$(B) = 1$. Since $c_{q-2} = \lambda^{-1}\lambda = 1$, one has

$$B = \begin{pmatrix} c_0 & c_1 & \dots & c_{q-3} & 1 \\ c_1 & c_2 & \dots & 1 & c_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & c_0 & \dots & c_{q-4} & c_{q-3} \end{pmatrix}.$$

Assume that $c_{q-3} = 0$. Then B holds a nonzero minor of order 2, and so one gets that rank$(B) \geq 2$, which is impossible. Hence we must have $c_{q-3} \neq 0$. In the following, we let $c_{q-3} = a$. Then $a \in \mathbb{F}_q^*$. For each integer i with $1 \leq i \leq q-1$, let $\mathbf{r}_i$ denote the i-th row of the matrix B. Then rank$(\mathbf{r}_i) = 1$ for each integer i with $1 \leq i \leq q-1$. Since rank(B)=1, there exists an element $a \in \mathbb{F}_q^*$ such that $\mathbf{r}_1 = a\mathbf{r}_2$. Then we deduce that $c_{q-2} = ac_0$ and $c_k = ac_{k+1}$ for $0 \leq k \leq q-3$. Since $c_{q-2} = 1$, one has $a = c_{q-3}, c_0 = a^{-1} = a^{q-2}$ and $c_k = a^{-1}c_{k-1}$ for $1 \leq k \leq q-2$. It then follows that $c_k = a^{q-2-k}$ for $0 \leq k \leq q-2$. This implies that

$$u(x) - v_0(x) = \lambda \sum_{i=0}^{q-2} a^{q-2-i} x^i.$$

Therefore

$$\begin{aligned} u(x) &= \lambda \sum_{i=k}^{q-2} a^{q-2-i} x^i + \lambda \sum_{i=0}^{k-1} a^{q-2-i} x^i + v_0(x) \\ &= \lambda \sum_{i=k}^{q-2} a^{q-2-i} x^i + f_{\leq k-1}(x), \end{aligned}$$

where

$$f_{\leq k-1}(x) := \lambda \sum_{i=0}^{k-1} a^{q-2-i} x^i + v_0(x) \in P_{k-1}.$$

So the necessity part is proved.

This concludes the proof of Theorem 1.5 □

4. Examples and final remarks

In this last section, we supply two examples to demonstrate the validity of Theorem 1.5.

Example 4.1. Let $q = 7, n = q-1 = 6, k = 3$. Putting $\alpha = 3$ gives us the standard Reed-Solomon code

$$RS_7(\mathbb{F}_7^*, 3) = \{(f(1), f(3), \cdots, f(3^5)) \in \mathbb{F}_7^6 \mid f(x) \in \mathbb{F}_7[x], \deg f(x) \leq 2\}.$$

Using the MATLAB 2011a programming, we search for the ordinary word and find out all the ordinary words of degree $q-2=5$ of standard Reed-Solomon code $RS_7(\mathbb{F}_7^*, 3)$ that are listed in Table 1. By (1.2), we can get the Lagrange interpolation polynomial $u(x)$ of the ordinary word u of degree 5 of $RS_7(\mathbb{F}_7^*, 3)$ listed also in Table 1. This coincides with Theorem 1.5.

Suppose that $\mathbf{u}$ is an ordinary word of degree 5 of $RS_7(\mathbb{F}_7^*, 3)$. Then

$$d(\mathbf{u}, RS_7(\mathbb{F}_7^*, 3)) = n - \deg u(x) = 6 - 5 = 1.$$

On the other hand, one has

$$d(\mathbf{u}, RS_7(\mathbb{F}_7^*, 3)) = \min_{\mathbf{v} \in RS_7(\mathbb{F}_7^*, 3)} \{d(\mathbf{u}, \mathbf{v})\}.$$

So it is sufficient to find a codeword v in $RS_7(\mathbb{F}_7^*, 3)$ such that $d(\mathbf{u}, \mathbf{v}) = 1$. For the received ordinary word $\mathbf{u} = \lambda(3, 1, 0, 6, 0, 4) + \mathbf{f}$ of degree 5, by (1.2) we compute and get that $u(x) = \lambda \sum_{i=3}^{5} x^i + f(x)$. Furthermore, one can search and find the word $\mathbf{v} = \lambda(4, 1, 0, 6, 0, 4) + \mathbf{f} \in RS_7(\mathbb{F}_7^*, 3)$ such that $d(\mathbf{u}, \mathbf{v}) = 1$. For the other ordinary words $\mathbf{u}$ of degree 5, one can also find the corresponding codewords $\mathbf{v}$ such that $d(\mathbf{u}, \mathbf{v}) = 1$. We can easily compute the Lagrange interpolation polynomial $v(x)$ of $\mathbf{v}$ also listed in Table 1.

Table 1. Ordinary words of degree 5 for $RS_7(\mathbb{F}_7^*, 3)$.
$\lambda \in \mathbb{F}_7^*$, $\mathbf{f} = l_2\mathbf{e}^2 + l_1\mathbf{e} + l_0$, $f(x) = l_2x^2 + l_1x + l_0$ with $\mathbf{e}^i = (1, 3^i, 2^i, 6^i, 4^i, 5^i)$ and l_0, l_1, l_2 running over $\mathbb{F}_7$, $d(u, v) = 1$

Ordinary word $\mathbf{u}$	LIP $u(x)$ of $\mathbf{u}$	Codeword $\mathbf{v}$	LIP $v(x)$ of $\mathbf{v}$
$\lambda(3, 1, 0, 6, 0, 4) + \mathbf{f}$	$\lambda(x^5 + x^4 + x^3) + f(x)$	$\lambda(4, 1, 0, 6, 0, 4) + \mathbf{f}$	$\lambda(6x^2 + 6x + 6) + f(x)$
$\lambda(0, 2, 5, 4, 0, 3) + \mathbf{f}$	$\lambda(x^5 + 2x^4 + 4x^3) + f(x)$	$\lambda(0, 2, 2, 4, 0, 3) + \mathbf{f}$	$\lambda(6x^2 + 5x + 3) + f(x)$
$\lambda(6, 1, 5, 0, 2, 0) + \mathbf{f}$	$\lambda(x^5 + 3x^4 + 2x^3) + f(x)$	$\lambda(6, 6, 5, 0, 2, 0) + \mathbf{f}$	$\lambda(x^2 + 3x + 2) + f(x)$
$\lambda(0, 5, 0, 1, 6, 2) + \mathbf{f}$	$\lambda(x^5 + 4x^4 + 2x^3) + f(x)$	$\lambda(0, 5, 0, 1, 1, 2) + \mathbf{f}$	$\lambda(6x^2 + 3x + 5) + f(x)$
$\lambda(3, 0, 4, 0, 5, 2) + \mathbf{f}$	$\lambda(x^5 + 5x^4 + 4x^3) + f(x)$	$\lambda(3, 0, 4, 0, 5, 5) + \mathbf{f}$	$\lambda(x^2 + 5x + 4) + f(x)$
$\lambda(1, 0, 3, 4, 6, 0) + \mathbf{f}$	$\lambda(x^5 + 6x^4 + x^3) + f(x)$	$\lambda(1, 0, 3, 3, 6, 0) + \mathbf{f}$	$\lambda(x^2 + 6x + 1) + f(x)$

Example 4.2. Let $q = 11, n = q - 1 = 10, k = 5$. Putting $\alpha = 2$ gives us the standard Reed-Solomon code

$$RS_{11}(\mathbb{F}_{11}^*, 5) = \{(f(1), f(2), \cdots, f(2^9)) \in \mathbb{F}_{11}^{10} \mid f(x) \in \mathbb{F}_{11}[x], \deg f(x) \le 5\}.$$

Using the MATLAB 2011a programming, we search for the ordinary word and find out all the ordinary words of degree $q-2 = 9$ of standard Reed-Solomon code $RS_{11}(\mathbb{F}_{11}^*, 5)$ that are listed in Table 2. By (1.2), one can easily calculate the Lagrange interpolation polynomial $u(x)$ of the ordinary word $\mathbf{u}$ of degree 9 of $RS_{11}(\mathbb{F}_{11}^*, 5)$ listed also in Table 2. This coincides with Theorem 1.5.

Suppose that $\mathbf{u}$ is an ordinary word of degree 9 of $RS_{11}(\mathbb{F}_{11}^*, 5)$. Then

$$d(\mathbf{u}, RS_{11}(\mathbb{F}_{11}^*, 5)) = n - \deg u(x) = 10 - 9 = 1.$$

On the other hand, one has

$$d(\mathbf{u}, RS_{11}\mathbb{F}_{11}^*, 5)) = \min_{\mathbf{v} \in RS_{11}(\mathbb{F}_{11}^*, 5)} \{d(\mathbf{u}, \mathbf{v})\}.$$

So it is sufficient to find a codeword $\mathbf{v}$ in $RS_{11}(\mathbb{F}_{11}^*, 5)$ such that $d(\mathbf{u}, \mathbf{v}) = 1$. For the received ordinary word $\mathbf{u} = \lambda(5, 2, 0, 5, 0, 10, 0, 4, 0, 7) + \mathbf{f}$ of degree 9, by (1.2) we compute and get that $u(x) = \lambda \sum_{i=5}^{9} x^i + f(x)$. Furthermore, one can search and find the codeword $\mathbf{v} = \lambda(6, 2, 0, 5, 0, 10, 0, 4, 0, 7) + \mathbf{f} \in RS_{11}(\mathbb{F}_{11}^*, 5)$ such that $d(\mathbf{u}, \mathbf{v}) = 1$. For the other ordinary words u of degree 9, one can also find the corresponding codewords v such that $d(\mathbf{u}, \mathbf{v}) = 1$. It is easy to compute the Lagrange interpolation polynomial $v(x)$ of $\mathbf{v}$ that is listed in Table 2.

Table 2. Ordinary words of degree 9 for $RS_{11}(\mathbb{F}_{11}^*, 5)$.
$\lambda \in \mathbb{F}_{11}^*$, $\mathbf{f} = l_4\mathbf{e}^4 + l_3\mathbf{e}^3 + l_2\mathbf{e}^2 + l_1\mathbf{e} + l_0$, $f(x) = l_4x^4 + l_3x^3 + l_2x^2 + l_1x + l_0$ with $\mathbf{e}^i = (1, 2^i, 4^i, 8^i, 5^i, 10^i, 9^i, 7^i, 3^i, 6^i)$ and l_0, l_1, l_2, l_3, l_4 running over $\mathbb{F}_{11}$, $d(\mathbf{u}, \mathbf{v}) = 1$

Ordinary word $\mathbf{u}$	LIP $u(x)$ of $\mathbf{u}$	Codeword $\mathbf{v}$	LIP $v(x)$ of $\mathbf{v}$
$\lambda(5, 2, 0, 5, 0, 10, 0, 4, 0, 7) + \mathbf{f}$	$\lambda(x^9 + x^8 + x^7 + 10x^6 + x^5) + f(x)$	$\lambda(6, 2, 0, 5, 0, 10, 0, 4, 0, 7) + \mathbf{f}$	$\lambda(10x^4 + 10x^3 + 10x^2 + 10x + 10) + f(x)$
$\lambda(9, 8, 1, 0, 8, 0, 5, 0, 2, 0) + \mathbf{f}$	$\lambda(x^9 + 2x^8 + 4x^7 + 8x^6 + 5x^5) + f(x)$	$\lambda(9, 3, 1, 0, 8, 0, 5, 0, 2, 0) + \mathbf{f}$	$\lambda(x^4 + 2x^3 + 4x^2 + 8x + 5) + f(x)$
$\lambda(0, 9, 0, 7, 0, 5, 0, 6, 9, 8) + \mathbf{f}$	$\lambda(x^9 + 3x^8 + 9x^7 + 5x^6 + 4x^5) + f(x)$	$\lambda(0, 9, 0, 7, 0, 5, 0, 6, 2, 8) + \mathbf{f}$	$\lambda(10x^4 + 8x^3 + 2x^2 + 6x + 7) + f(x)$
$\lambda(0, 10, 4, 6, 0, 4, 0, 8, 0, 1) + \mathbf{f}$	$\lambda(x^9 + 4x^8 + 5x^7 + 9x^6 + 3x^5) + f(x)$	$\lambda(0, 10, 7, 6, 0, 4, 0, 8, 0, 1) + \mathbf{f}$	$\lambda(10x^4 + 7x^3 + 6x^2 + 2x + 8) + f(x)$
$\lambda(0, 3, 0, 8, 1, 7, 0, 1, 0, 2) + \mathbf{f}$	$\lambda(x^9 + 5x^8 + 3x^7 + 4x^6 + 9x^5) + f(x)$	$\lambda(0, 3, 0, 8, 10, 7, 0, 1, 0, 2) + \mathbf{f}$	$\lambda(10x^4 + 6x^3 + 8x^2 + 7x + 2) + f(x)$
$\lambda(4, 0, 10, 0, 9, 0, 8, 0, 3, 10) + \mathbf{f}$	$\lambda(x^9 + 6x^8 + 3x^7 + 7x^6 + 9x^5) + f(x)$	$\lambda(4, 0, 10, 0, 9, 0, 8, 0, 3, 1) + \mathbf{f}$	$\lambda(x^4 + 6x^3 + 3x^2 + 7x + 9) + f(x)$
$\lambda(7, 0, 3, 0, 10, 0, 1, 7, 5, 0) + \mathbf{f}$	$\lambda(x^9 + 7x^8 + 5x^7 + 2x^6 + 3x^5) + f(x)$	$\lambda(7, 0, 3, 0, 10, 0, 1, 4, 5, 0) + \mathbf{f}$	$\lambda(x^4 + 7x^3 + 5x^2 + 2x + 3) + f(x)$
$\lambda(6, 0, 5, 2, 3, 0, 2, 0, 4, 0) + \mathbf{f}$	$\lambda(x^9 + 8x^8 + 9x^7 + 6x^6 + 4x^5) + f(x)$	$\lambda(6, 0, 5, 9, 3, 0, 2, 0, 4, 0) + \mathbf{f}$	$\lambda(x^4 + 8x^3 + 9x^2 + 6x + 4) + f(x)$
$\lambda(0, 6, 0, 9, 0, 2, 3, 10, 0, 3) + \mathbf{f}$	$\lambda(x^9 + 9x^8 + 4x^7 + 3x^6 + 5x^5) + f(x)$	$\lambda(0, 6, 0, 9, 0, 2, 8, 10, 0, 3) + \mathbf{f}$	$\lambda(10x^4 + 2x^3 + 7x^2 + 8x + 6) + f(x)$
$\lambda(1, 0, 7, 0, 4, 6, 9, 0, 6, 0) + \mathbf{f}$	$\lambda(x^9 + 10x^8 + x^7 + 10x^6 + x^5) + f(x)$	$\lambda(1, 0, 7, 0, 4, 5, 9, 0, 6, 0) + \mathbf{f}$	$\lambda(x^4 + 10x^3 + x^2 + 10x + 1) + f(x)$

Remark 4.3. In this paper, we determine all the ordinary words of maximal degree $q-2$ of the standard Reed-Solomon code $RS_q(\mathbb{F}_q^*, k)$. In the close future, we will explore the ordinary words of degree no more than $q - 3$ of the standard Reed-Solomon code $RS_q(\mathbb{F}_q^*, k)$.

Acknowledgments

The authors would like to thank the anonymous referees for their careful readings of the manuscript and helpful comments and suggestions that improved the presentation of the paper. 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 Tourism University under Grant # 19SCTUZZ01.

Conflict of interest

We declare that we have no conflict of interest.

References

1. Q. Cheng and E. Murray, *On deciding deep holes of Reed-Solomon codes*. In: J.Y. Cai, S.B. Cooper, H. Zhu(eds) Theory and Applications of Models of Computation. TAMC 2007, Lecture Notes in Computer Science, vol. **4484**, Springer, Berlin, Heidelberg.
2. S. F. Hong and R. J. Wu, *On deep holes of generalized Reed-Solomon codes*, AIMS Math., **1** (2016), 96–101.

3. J. Y. Li and D. Q. Wan, *On the subset sum problem over finite fields*, Finite Fields Th. App., **14** (2008), 911–929.

4. Y. J. Li and D. Q. Wan, *On error distance of Reed-Solomon codes*, Sci. China Math., **51** (2008), 1982–1988.

5. Y. J. Li and G. Z. Zhu, *On the error distance of extended Reed-Solomon codes*, Adv. Math. Commun., **10** (2016), 413–427.

6. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, 2 Eds., Cambridge: Cambridge University Press, 1997.

7. G. Rados, *Zur Theorie der Congruenzen höheren Grades*, J. reine angew. Math., **99** (1886), 258–260.

8. G. Raussnitz, *Zur Theorie de Conguenzen höheren Grades*, Math. Naturw. Ber. Ungarn., **1** (1882/83), 266–278.

9. R. J. Wu and S. F. Hong, *On deep holes of standard Reed-Solomon codes*, Sci. China Math., **55** (2012), 2447–2455.

10. X. F. Xu, S. F. Hong and Y. C. Xu, *On deep holes of primitive projective Reed-Solomon codes*, SCIENTIA SINICA Math., **48** (2018), 1087–1094.

11. X. F. Xu and Y. C. Xu, *Some results on deep holes of generalized projective Reed-Solomon codes*, AIMS Math., **4** (2019), 176–192.

12. G. Z. Zhu and D. Q. Wan. *Computing error distance of Reed-Solomon codes*. In: TAMC 2012 Proceedings of the 9th Annual international conference on Theory and Applications of Models of Computation, (2012), 214–224.

AIMS Press