Journal of ALGEBRAIC STRUCTURES and THEIR APPLICATIONS

Journal of Algebraic Structures and Their Applications

ISSN: 2382-9761

www.as.yazd.ac.ir

Algebraic Structures and Their Applications Vol. 6 No. 1 (2019) pp 35-45.

A GENERAL CONSTRUCTION OF REED-SOLOMON CODES BASED ON GENERALIZED DISCRETE FOURIER TRANSFORM

NAJME SAHAMI AND MAJID MAZROOEI

Abstract. In this paper, we employ the concept of the Generalized Discrete Fourier Transform, which in turn relies on the Hasse derivative of polynomials, to give a general construction of Reed-Solomon codes over Galois fields of characteristic not necessarily co-prime with the length of the code. The constructed linear codes enjoy nice algebraic properties just as the classic one.

1. Introduction

In 1960, I.S. Reed and G. Solomon introduced a family of error-correcting cyclic codes that are doubly blessed [8]. In the decades since their discovery, Reed-Solomon codes (RS codes, for short) have enjoyed countless applications, from data retrieval of bar codes and QR codes in our daily lives to sending data to and from spacecrafts launched in deep-space missions. RS codes can be arranged in the class of Maximum Distance Separable (MDS) codes [1], thus reaching the Singleton bound. Their main advantage lies in two facts: high capability of correcting both random and burst errors; and existence of efficient decoding algorithms for

MSC(2010): Primary:65T50, 94B05.

Keywords: Generalized Discrete Fourier Transform, Hasse Derivatives, Linear Codes, Reed-Solomon Codes.

Received: 23 April 2018, Accepted: 06 March 2019.

∗Corresponding author

them [2,4]. A breakthrough has been made by M. Sudan in 1997 about the list decoding of RS codes [10] and further improved by V. Guruswami and M. Sudan [3,10].

Beside trying to find new decoding algorithms for RS codes, there are growing appeals for generalizing the algebraic construction of RS codes. In [7], Quintin, Barbier and Chabot introduce a generalization of RS codes over (not necessarily commutative) rings with unity. They showed that the main results about RS codes (over finite fields) still hold in this more general situation. Another generalization of RS codes is given by Shokrollahi [9]. Instead of looking at consecutive powers for constructing an RS code, the author constructs p codes of length n/p in a similar manner as an RS code, and then apply a Fourier transform of length p componentwise on the vectors of these constituent codes. As a result, Shokrollahi showed that if the initial constituent codes are chosen appropriately, then the resulting code is MDS; in fact, it is a generalized RS code equivalent to a code obtained by evaluating polynomials of degree less than k on the desired set of roots.

A common feature in almost all generalized Reed-Solomon codes is that the length of the generalized code is coprime to the characteristic of the base field. This means that, for a base field of order $q = p^a$, p a prime number and $a \geq 1$ an integer, the constructed code has length $q - 1$. This problem motivated us to give a more general description of Reed-Solomon codes in which more lengths can be included. For our work, the main tool is the *generalized discrete Fourier transform*, which in turn relies on the *Hasse derivative* of polynomials. Our method leads to construct a family of linear cyclic codes of length $n = p^a m$, where p is the characteristic of the finite field F_q and $(m, p) = 1$ (thus the blocklength of the code is not neccessarily coprime to p), including RS codes as a special case.

2. **Preliminaries**

A linear $[n, k]$-code C, $n \geq k \geq 1$, over the Galois field F_q, q a prime power, is a k-dimensional vector subspace of F_q^n. An element of C is called a codeword of C. The (Hamming) weight of a vector $\mathbf{c} \in F_q^n$ is the number of its nonzero coordinates which is denoted by $w(\mathbf{c})$. For a linear code C, the distance $d := d(C)$ is defined as the minimum weight of all nonzero codewords. The distance of a code C is important to determine the error correction capability of C (that is, the number of errors can be coorected) and the error detection capability (that is, the number of errors can be detected). For an $[n, k, d]$-linear code C, it is well-known that $d \leq n - k + 1$. A linear code achieving this bound is called maximum distance separable (MDS). These codes have been under study extensively due to their error correcting ability. The dual code of a linear code C, denoted by $C^{\perp}$, is defined as

$$C^{\perp} = \{\mathbf{v} \in F_q^n \mid \langle \mathbf{v}, \mathbf{u} \rangle = 0, \ \forall \ \mathbf{u} \in C\},$$

where $\langle \mathbf{x}, \mathbf{y} \rangle$ denotes the inner product of the vectors $\mathbf{x}$ and $\mathbf{y}$ which is defined as $\sum_{i=0}^{n-1} x_i y_i \pmod{q}$. The dual code $C^{\perp}$ has dimension $n-k$ if the code C has dimension k. A linear code C is called cyclic if the cyclic shift of every codeword is also a codeword, i.e.,

$$(c_0, ..., c_{n-1}) \in C \to (c_{n-1}, c_0, ..., c_{n-2}) \in C.$$

To describe the algebraic properties of a cyclic codes, a ring theoretic structure of cyclic codes is introduced. Consider the univariate polynomial ring $F_q[x]$ and the ideal $I = \langle x^n - 1 \rangle$. If we denote the ring $F_q[x]/I$ by R, then there exists a bijective correspondence between the vectors of F_q^n and the residue classes of polynomials in R:

$$\mathbf{v} = (v_0, ..., v_{n-1}) \longleftrightarrow v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}.$$

We can view linear codes as subsets of the ring R, thanks to the correspondence above. A linear $[n, k, d]$-code C is cyclic if and only if C is an ideal of R. Since R is a principal ideal ring, if C is not trivial, then there exists a unique monic polynomial g that generates C. The polynomial g is called the generator polynomial of C. Note that g divides $x^n - 1$ in $F_q[x]$. If the dimension of the code C is k then the generator polynomial has degree $n-k$. Linear codes are widely studied because of their algebraic structure, which makes them easier to describe than non-linear codes.

One of the most important families of cyclic MDS codes is Reed-Solomon (RS, for short). An RS code of length n and dimension k over the Galois field F_q is defined as the vector space of polynomials f such that $f(\beta) = 0$ for all β in the set $Z = \{\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+n-k-1}\}$. Here α can be any element in F_q of multiplicative order at least n where n is a divisor of $q-1$.

Another interesting method for constructing Reed-Solomon codes is the discrete Fourier transform (DFT, for short) approach [1, Section 6]. Let ω be an n-th root of unity in (a sufficiently large) extension of the Galois field F_q, where q is a prime power p^a and n is coprime with p. The discrete Fourier transform of an n-bit vector $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ is defined as follows:

$$\mathcal{F}\{(v_0, v_1, \ldots, v_{n-1})\} = (V_0, V_1, \ldots, V_{n-1}),$$

where $V_j = \sum_{i=0}^{n-1} v_i \omega^{ij}$, $j = 0, \ldots, n-1$. The vector $\mathbf{V} = \mathcal{F}\{v\}$ is called *the frequency-domain function* or the *spectrum* of v. The vector $\mathbf{v}$ is related to its spectrum $\mathbf{V}$ by

$$v_i = \frac{1}{n} \sum_{j=0}^{n-1} V_j \omega^{-ij},$$

where n is interpreted as an integer of the field. Now, a Reed-Solomon code C of length n over F_q, with n a divisor of $q-1$, and designed minimum distance d is defined as the set of all words over F_q of length n whose discrete Fourier transform is equal to zero in a specified block of $d-1$ consecutive components, see [1, chap. 6].

The operator discrete fourier transform can be introduced in more general case using the concept of Hasse derivative. Let F_q be a finite field. For $j = 0, 1, 2, \ldots$ and $f(x) = \sum_{i=0}^{n} a_i x^i \in F_q[x]$, the jth Hasse derivative of f is defined as

$$f^{[j]}(x) = \sum_{i=0}^{n} \binom{i}{j} a_i x^{i-j}.$$

Here we use a standard convention for binomial coefficients: $\binom{i}{j} = 0$ for all $j > i$, which guarantees that the jth Hasse derivative be again a polynomial over F_q. Also, by $\binom{i}{j}$, i a negative integer, we mean $\binom{((i))}{j}$ where $((i))$ stands for i modulo n.

Just as in the case of formal derivatives in the fields with characteristic 0, Hasse derivatives in any field are related to repeated factors of a polynomial, as the following proposition states.

Proposition 2.1. *[5, Lemma 6.51]. Let f be a polynomial over the finite field F_q. Suppose $c \in F_q$ is a root of $f^{[j]}$ for $j = 0, 1, \ldots, M-1$. Then $(x-c)^M$ divides $f(x)$.*

3. Generalized Discrete Fourier Transform

Let $n = p^a m$, where $(m, p) = 1$. When $a \geq 1$, n is no longer relatively prime to p. Thus n is not a nonzero element of the field F_q with characteristic p and the inverse discrete Fourier transform does not exist. So the classical theory of discrete Fourier transform does not apply to $F_q[x]/\langle x^n - 1\rangle$. However, a generalized discrete Fourier transform (GDFT) has been introduced in the literature that deals with this situation [6].

Let $\mathbf{c} = \sum_{i=0}^{n-1} c_i x^i \in F_q[x]$, and let ζ be a primitive m-th root of unity in some (sufficiently large) extension of F_q. For each $0 \leq g \leq p^a - 1$ and $0 \leq h \leq m-1$, let

$$\widehat{c}_{g,h} = \sum_{i=0}^{n-1} \binom{i}{g} c_i \zeta^{h(i-g)}.$$

Note that $\widehat{c}_{g,h} = \mathbf{c}^{[g]}(\zeta^h)$. Then, the generalized Discrete Fourier transform of $\mathbf{c}$ can be described in terms of a matrix

$$\widehat{\mathbf{c}} = [\widehat{c}_{g,h}] = \begin{bmatrix} \widehat{c}_{0,0} & \widehat{c}_{0,1} & \cdots & \widehat{c}_{0,m-1} \\ \widehat{c}_{1,0} & \widehat{c}_{1,1} & \cdots & \widehat{c}_{1,m-1} \\ \vdots & & & \\ \widehat{c}_{p^a-1,0} & \widehat{c}_{p^a-1,1} & \cdots & \widehat{c}_{p^a-1,m-1} \end{bmatrix}.$$

We say that $\mathbf{c}$ and $\widehat{\mathbf{c}}$ is a GDFT pair and write $\mathbf{c} \leftrightarrow \widehat{\mathbf{c}}$. Just as DFT, the GDFT has many strong propertis [6]. One we need later, is the following proposition.

Proposition 3.1. *If* $\mathbf{c} = \sum_{i=0}^{n-1} c_i x^i \leftrightarrow \widehat{\mathbf{c}} = [\widehat{c}_{g,h}]$ *is a GDFT pair, then the following are also GDFT pairs:*

$$\sum_{i=0}^{n-1} \zeta^{il} c_i x^i \leftrightarrow [\zeta^{gl} \widehat{c}_{g,((l+h))}],$$

$$\sum_{i=0}^{n-1} c_{((i-l))} x^i \leftrightarrow [\sum_{k=0}^{l} \binom{l}{k} \zeta^{((l-k))h} \widehat{c}_{((g-k)),h}],$$

where $l \geq 0$ *is an integer and the double parentheses indicate modulo appropriate* b *(*$b \in \{n, m, p^a\}$*).*

Proof. Let $\mathbf{u} = \sum_{i=0}^{n-1} \zeta^{il} c_i x^i$. Then,

$$\begin{aligned} \widehat{u}_{g,h} &= \sum_{i=0}^{n-1} \binom{i}{g} \zeta^{il} c_i \zeta^{h(i-g)} \\ &= \zeta^{gl} \sum_{i=0}^{n-1} \binom{i}{g} c_i \zeta^{((h+l))(i-g)} \\ &= \zeta^{gl} \widehat{c}_{g,((h+l))}, \end{aligned}$$

which proves the first property. Next, let $\mathbf{v} = \sum_{i=0}^{n-1} c_{((i-l))} x^i$. Then,

$$\begin{aligned} \widehat{v}_{g,h} &= \sum_{i=0}^{n-1} \binom{i}{g} c_{((i-l))} \zeta^{h(i-g)} \\ &= \sum_{i=0}^{n-1} \left(\sum_{k=0}^{g} \binom{l}{k} \binom{i-l}{g-k} \right) c_{((i-l))} \zeta^{h(i-g)} \\ &= \sum_{k=0}^{g} \binom{l}{k} \left(\sum_{j=-l}^{n-l-1} \binom{((j))}{g-k} c_j \zeta^{h(((j))+l-g)} \right) \\ &= \sum_{k=0}^{g} \binom{l}{k} \left(\sum_{t=0}^{n-1} \binom{t}{g-k} c_t \zeta^{h(t-(g-k))} \right) \zeta^{h(l-k)} \\ &= \sum_{k=0}^{g} \binom{l}{k} \zeta^{h((l-k))} \widehat{c}_{((g-k)),h}, \end{aligned}$$

which shows that the second property holds. ■

Let $\mathbf{u} = (u_0, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, \ldots, v_{n-1})$ be vectors over F_q. The convolution vector $\mathbf{u} \star \mathbf{v}$ is defined as a vector $\mathbf{w} \in F_q^n$ whose $\mathbf{w_i} = \sum_{j=0}^{n-1} u_{((i-j))} v_j$ for each $0 \leq i \leq n-1$ (here, double parantheses means module n). The following theorem will be needed later.

Theorem 3.2. *If $\mathbf{u} \leftrightarrow \widehat{\mathbf{u}} = [\widehat{u}_{g,h}]$ and $\mathbf{v} \leftrightarrow \widehat{\mathbf{v}} = [\widehat{v}_{g,h}]$ are GDFT pairs, then $\mathbf{w} = \mathbf{u} \star \mathbf{v} \leftrightarrow \widehat{\mathbf{w}} = [\widehat{w}_{g,h}]$ is a GDFT pair, where for each $0 \leq g \leq p^a - 1$ and $0 \leq h \leq m-1$:*

$$\widehat{w}_{g,h} = \sum_{k=0}^{g} \widehat{u}_{g-k,h} \widehat{v}_{k,h}.$$

Proof. By definition, we have

$$\begin{aligned}
\widehat{w}_{g,h} &= \sum_{i=0}^{n-1} \binom{i}{g} w_i \zeta^{h(i-g)} \\
&= \sum_{i=0}^{n-1} \binom{i}{g} \left(\sum_{j=0}^{n-1} u_{((i-j))} v_j \right) \zeta^{h(i-g)} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \binom{i}{g} u_{((i-j))} v_j \zeta^{h(i-g)} \\
&= \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \binom{i}{g} u_{((i-j))} \zeta^{h(i-g)} v_j \\
&= \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} \left(\sum_{k=0}^{g} \binom{j}{k} \binom{i-j}{g-k} \right) u_{((i-j))} \zeta^{h(i-g)} v_j \\
&= \sum_{j=0}^{n-1} \sum_{k=0}^{g} \binom{j}{k} \left(\sum_{i=0}^{n-1} \binom{i-j}{g-k} u_{((i-j))} \zeta^{h(i-j-g+k)} \right) \zeta^{h(j-k)} v_j \\
&= \sum_{j=0}^{n-1} \sum_{k=0}^{g} \binom{j}{k} \left(\sum_{t=-j}^{n-j-1} \binom{((t))}{g-k} u_{((t))} \zeta^{h(((t))-g+k)} \right) \zeta^{h(j-k)} v_j \\
&= \sum_{j=0}^{n-1} \sum_{k=0}^{g} \binom{j}{k} \widehat{u}_{g-k,h} \zeta^{h(j-k)} v_j \\
&= \sum_{k=0}^{g} \widehat{u}_{g-k,h} \left(\sum_{j=0}^{n-1} \binom{j}{k} \zeta^{h(j-k)} v_j \right) \\
&= \sum_{k=0}^{g} \widehat{u}_{g-k,h} \widehat{v}_{k,h},
\end{aligned}$$

as we claimed. ■

Description of the inverse GDFT is somewhat more involved than that of the classical DFT. As an explicit description of the inverse GDFT is necessary for obtaining the minimum distance of the generalized RS codes (which will be introduced in the next section), we recall some details of the inverse GDFT here.

For each $0 \leq i \leq p^a - 1$, let

$$\mathbf{c}_{(i)}(x) = c_i + c_{i+p^a} x + \ldots + c_{i+(m-1)p^a} x^{m-1}.$$

Let $\beta = \zeta^{p^a}$, so that β is again a primitive mth root of unity. By the classical DFT (with β as the chosen mth root of unity), one sees readily that

$$c_{i+jp^a} = \frac{1}{m}\sum_{i=0}^{m-1} \mathbf{c}_{(i)}(\beta^h)(\beta^{-j})^h.$$

Let $H(x)$ be the $p^a \times p^a$ matrix whose (i,j)th entry is $\binom{j}{i}x^{j-i}$, where the rows and columns are labelled from 0 to $p^a - 1$ (this is the ith Hasse derivative of the monomial x^j in $F_q[x]$). It is known that the inverse of $H(x)$ is $H(-x)$ (cf. [6, Lemma 6]). In particular, when q is even, $H(x)$ is self-inverse. It can then be verified (cf. [6, Eq. (4)]) that

$$\begin{bmatrix} \mathbf{c}_{(0)}(\beta^h) \\ \mathbf{c}_{(1)}(\beta^h) \\ \vdots \\ \mathbf{c}_{(p^a-1)}(\beta^h) \end{bmatrix} = H(-\zeta^h) \begin{bmatrix} \widehat{c}_{0,h} \\ \widehat{c}_{1,h} \\ \vdots \\ \widehat{c}_{p^a-1,h} \end{bmatrix}.$$

Consequently,

$$c_{i+jp^a} = \frac{1}{m}\sum_{h=0}^{m-1}\left(\sum_{g=0}^{p^a-1}\binom{g}{i}(-\zeta^h)^{g-i}\widehat{c}_{g,h}\right)(\beta^{-j})^h.$$

Hence the GDFT is invertible.

4. Generalized Reed-Solomon Codes

Recall that a Reed-Solomon code C of length n over F_q, with n a divisor of $q-1$ (and hence $(n,q) = 1$), and designed distance d is an $[n, n-d+1, d]$-cyclic code which is defined as the set of all words over F_q of length n whose discrete Fourier transform is equal to zero in a specified block of $d-1$ consecutive components.

In this section, we introduce a generalization of Reed-Solomon codes of length n not neccessarily coprime to q.

Definition 4.1. Let $d \geq 2$ and $n = p^a m$ where $a \geq 0$ is an integer and $(m,p) = 1$. A generalized Reed-Solomon code with parameters n and d over F_q, denoted $\mathrm{GRS}_{n,d}$, is the set of all words over F_q of length n whose generalized discrete Fourier transform is equal to zero in a specified block of $d-1$ consecutive columns, denoted $\{j_0, j_0+1, \ldots, j_0+d-2\}$, i.e

$$\mathrm{GRS}_{n,d} = \{\mathbf{c} \mid \widehat{c}_{g,h} = 0,\ \forall\ 0 \leq g \leq p^a - 1,\ \forall\ j_0 \leq h \leq j_0 + d - 2\}.$$

By definition, it is easy to see that $\mathrm{GRS}_{n,d}$ is an $[n, n - p^a(d-1)]$-linear code.

Example 4.2. Let $q = 9$, $n = 6$ and $d = 2$. Using $\zeta = 2 \in F_9$ as a 2th root of unity, the GDFT of a vector $\mathbf{c} \in (F_9)^6$ is given by the (3×2)-matrix $\widehat{\mathbf{c}}$ such that

$$\widehat{c}_{g,h} = \sum_{i=0}^{5} \binom{i}{g} c_i 2^{h(i-g)}.$$

Now, $\mathrm{GRS}_{6,2}$ consists of all words $\mathbf{c} \in (F_9)^6$ whose the first column of $\widehat{\mathbf{c}}$ is zero, i.e. $\widehat{c}_{0,0} = \widehat{c}_{1,0} = \widehat{c}_{2,0} = 0$. Thus,

$$\begin{cases} c_0 + c_1 + c_2 + c_3 + c_4 + c_5 = 0 \\ c_1 + 2(c_2 + c_5) + c_4 = 0 \\ c_2 + c_5 = 0 \end{cases},$$

which shows

$$c_0 + c_1 + c_2 + c_3 + c_4 + c_5 = c_2 + c_5 = c_1 + c_4 = 0.$$

This code has dimension $k = 3$ and $d(\mathrm{GRS}_{6,2}) = 2$.

As we mentioned, classical RS codes are cyclic. The following proposition states a similar result for GRS codes.

Proposition 4.3. *All generalized Reed-Solomon codes $GRS_{n,d}$ are cyclic.*

Proof. Suppose that $\mathbf{c} = \sum_{i=0}^{n-1} c_i x^i$ is a word of $\mathrm{GRS}_{n,d}$. Hence, $\widehat{c}_{g,h} = 0$ for all g and for each $j_0 \le h \le j_0 + d - 2$. Thus $\sum_{k=0}^{l} \binom{l}{k} \zeta^{((l-k))h} \widehat{c}_{((g-k)),h} = 0$ $(0 \le g \le p^a - 1,\ j_0 \le h \le j_0 + d - 2)$. Therefore, by proposition 3.1, the GDFT of the vector $\sum_{i=0}^{n-1} c_{((i-l))} x^i$ is equal to zero in the columns $j_0, j_0 + 1, \ldots, j_0 + d - 2$, proving that $\sum_{i=0}^{n-1} c_{((i-l))} x^i$ is a word of $\mathrm{GRS}_{n,d}$, as desired. ■

Because a generalized Reed-Solomon code is a cyclic code, it has a generator polynomial, $g_{n,d}(x)$, that can be calculated.

Proposition 4.4. *Let*

$$g_{n,d}(x) = (x - \zeta^{j_0})^{p^a} (x - \zeta^{j_0+1})^{p^a} \ldots (x - \zeta^{j_0+d-2})^{p^a}.$$

Then $g_{n,d}(x)$ is the generator polynomial of the code $GRS_{n,d}$.

Proof. First, note that $g_{n,d}^{[j]}(\zeta^h) = 0$ for each $0 \le j \le p^a - 1$ and $j_0 \le h \le j_0 + d - 2$. Hence $g_{n,d}(x) \in \mathrm{GRS}_{n,d}$. On the other hand, if $\mathbf{c} = \sum_{i=0}^{n-1} c_i x^i \in \mathrm{GRS}_{n,d}$ then $\mathbf{c}^{[j]}(\zeta^h) = 0$ $(j = 0, \ldots, p^a - 1,\ h = j_0, \ldots, j_0 + d - 2)$. By proposition 2.1, $(x - \zeta^h)^{p^a}$ divides $\mathbf{c}(x)$ for

$h = j_0, \ldots, j_0 + d - 2$. Thus $g_{n,d}(x)$ divides $\mathbf{c}(x)$. These arguments shows that $g_{n,d}(x)$ is the generator polynomial of the code $\mathrm{GRS}_{n,d}$. ■

Next, we are going to discuss the minimum distance of the code $\mathrm{GRS}_{n,d}$.

Theorem 4.5. *The minimum distance of the code $GRS_{n,d}$, $d(\mathrm{GRS}_{n,d})$, satisfies*

$$d \leq d(\mathrm{GRS}_{n,d}) \leq p^a(d-1) + 1.$$

Proof. Without loss of generality, we may assume that $j_0 = m - d + 1$, i.e $\mathrm{GRS}_{n,d}$ is the set of all words over F_q of length n whose generalized discrete Fourier transform is equal to zero in the last $d - 1$ columns. For any $0 \leq i \leq p^a - 1$, let

$$C_{(i)}(x) = \sum_{j=0}^{m-1} \mathbf{c}_{(i)}(\beta^j) x^j,$$

where $\mathbf{c}_{(i)}$ and β are defined as in the section 2.3. Recall that

$$\mathbf{c}_{(i)}(\beta^h) = \sum_{j=0}^{p^a-1} \binom{j}{i} (-\zeta^h)^{j-i} \widehat{c}_{j,h}.$$

On the other hand, $\widehat{c}_{j,h} = 0$ for all $0 \leq j \leq p^a - 1$ and $m - d + 1 \leq h \leq m - 1$, showing that $\mathbf{c}_{(i)}(\beta^h) = 0$ for $h = m-d+1, \ldots, m-1$. Therefore the polynomial $C_{(i)}(x)$ is either zero or has degree at most $m - d$. The corresponding codeword $\mathbf{c}$ has components $c_{i+jp^a} = \frac{1}{m} C_{(i)}(\beta^{-j})$. Because $C_{(i)}(x)$ is a polynomial of degree at most $m-d$, it can have at most $m-d$ zeros. Hence, unless it is identically zero, there will be at least d index j such that $c_{i+jp^a} \neq 0$. Consequently, $d(\mathrm{GRS}_{n,d}) \geq td$ where t is the number of those i whose $C_i(x) \neq 0$. Thus $d(\mathrm{GRS}_{n,d}) \geq d$. On the other hand, $d(\mathrm{GRS}_{n,d}) \leq n - k + 1 = p^a(d-1) + 1$. This completes the proof. ■

The following theorem shows that the dual code of a generalized Reed-Solomon code is a generalized Reed-Solomon code.

Theorem 4.6. *The dual code of $GRS_{n,d}$ is a generalized Reed-Solomon code.*

Proof. Without loss of generality, we may assume that $j_0 = 0$. We show that

$$\mathrm{GRS}_{n,d}^{\perp} = \{\mathbf{u} \in F_q^n \mid \widehat{u}_{g,h} = 0,\ g = 0, \ldots, p^a - 1,\ h = d-1, \ldots, m-1\}.$$

Note that the right hand of the above equality is just $\mathrm{GRS}_{n,m-d+2}$. Let $\mathbf{v} \in \mathrm{GRS}_{n,d}^{\perp}$ and $\mathbf{u} \in \mathrm{GRS}_{n,d}$. Then, for each $0 \leq i \leq n-1$, $\sum_{j=0}^{n-1} u_{((i-j))} v_j = 0$ because $\mathbf{v} \in \mathrm{GRS}_{n,d}^{\perp}$ and $\mathbf{x} = (u_{((i-j))}) \in C$ (recall that C is a cyclic code). This shows that $\mathbf{u} \star \mathbf{v} = \mathbf{0}$, and hence, for each $0 \leq g \leq p^a - 1$ and $0 \leq h \leq m-1$, $\sum_{k=0}^{g} \widehat{u}_{g-k,h} \widehat{v}_{k,h} = 0$ (see proposition 3.2). Let $E(a,b)$

denote the $(p^a \times m)$-matrix whose only nonzero entry is 1 in the ath row and bth column and let $\mathbf{u}(a,b) = \mathrm{GDFT}^{-1}(E(a,b))$. Then for each $d-1 \leq h \leq m-1$ we have $\mathbf{u}(0,h) \in \mathrm{GRS}_{n,d}$. Thus, for each $0 \leq g \leq p^a-1$ and $d-1 \leq h \leq m-1$, $0 = \sum_{k=0}^{g} (\widehat{u}(0,h))_{g-k,h}\widehat{v}_{k,h} = \sum_{k=0}^{g} E(0,h)_{g-k,h}\widehat{v}_{k,h} = \widehat{v}_{g,h}$. Therefore, $\mathbf{v} \in \mathrm{GRS}_{n,m-d+2}$. So, we proved that $\mathrm{GRS}_{n,d}^{\perp} \subseteq \mathrm{GRS}_{n,m-d+2}$. But both $\mathrm{GRS}_{n,d}^{\perp}$ and $\mathrm{GRS}_{n,m-d+2}$ have dimension $p^a(d-1)$ which implies $\mathrm{GRS}_{n,d}^{\perp} = \mathrm{GRS}_{n,m-d+2}$, as desired. ■

5. Acknowledgments

The second author is partially supported by the University of Kashan under grant number 682474. The authors also wish to sincerely thank the referees for several useful comments.

References

[1] R. E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, Cambridge, 2003.

[2] S. Gao, *A new algorithm for decoding Reed-Solomon codes*, Communications, Information and Network Security, edited by V. K. Bhargava, H. V. Poor, V. Tarokh and Yoon Seokho, Kluwer (2002) 55-68.

[3] V. Guruswami, *List decoding of error-correcting codes*, Lecture notes in computer science, Springer, 2004.

[4] J. Justesen, *On the complexity of decoding Reed-Solomon codes*, IEEE Trans. Inform. Theory **22** (1976), 237-238.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[6] J. L. Massey and S. Serconek, *Linear complexity of peridic sequences: A general theory*, Advances in Cryptology-CRYPTO' 96, edited by N. Koblitz, Kluwer (1996), 358-371.

[7] G. Quintin, M. Barbier and C. Chabot, *On generalized Reed-Solomon codes over commutative and non-commutative rings*, IEEE Trans. Inform. Theory **59**(9) (2013), 5882-5897.

[8] I. S. Reed and G. Solomon, *Polynomial codes over certain finite fields*, J. Soc. Ind. Appl. Math. **8**(2) (1960), 300-304.

[9] A. Shokrollahi, *A class of generalized RS-codes with faster encoding and decoding algorithms*, ITA (2013), 1-10.

[10] M. Sudan, *Decoding of Reed-Solomon codes beyond the error-correction diameter*, Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing, University of Illions at Urbana-Champaign (1997), 215-224.

[11] S. B. Wicker and V. K. Bhargava, Reed-Solomon codes and their applications, IEEE Press, 1994.

Najme Sahami
Department of mathematical sciences
University of Kashan, Kashan
Isfahan, Iran.
n.sahami79@gmail.com

Majid Mazrooei

Department of mathematical sciences

University of Kashan, Kashan

Isfahan, Iran.

m.mazrooei@kashanu.ac.ir