Duality of generalized twisted Reed-Solomon codes and Hermitian self-dual MDS or NMDS codes

Guanmin Guo · **Ruihu Li** · **Yang Liu** · **Hao Song**

Abstract Self-dual MDS and NMDS codes over finite fields are linear codes with significant combinatorial and cryptographic applications. In this paper, firstly, we investigate the duality properties of generalized twisted Reed-Solomon (abbreviated GTRS) codes in some special cases. In what follows, a new systematic approach is proposed to draw Hermitian self-dual (+)-GTRS codes. The necessary and sufficient conditions of a Hermitian self-dual (+)-GTRS code are presented. With this method, several classes of Hermitian self-dual MDS and NMDS codes are constructed.

1 Introduction

Maximum distance separable (MDS) codes are optimal because they attain the maximal achievable minimum distance $d = n - k + 1$ of length n and dimension k, which have the largest error-correcting capability for given a code rate. The most famous family of MDS codes is (extended) generalized Reed-Solomon (for short GRS and EGRS) codes. There are, of course, other non-Reed-Solomon type MDS codes [1].

Guanmin Guo*
E-mail: gmguo_xjtukgd@yeah.net
Ruihu Li
E-mail: llzsy110@126.com
Yang Liu
E-mail: liu_yang10@163.com
Hao Song
E-mail: songhao_kgd@163.com

Fundamentals Department, Air Force Engineering University, Xi'an, Shaanxi 710051, P. R. China

Near MDS (i.e. NMDS) codes are introduced in [2] by slightly weakening the restrictive conditions in the definition of MDS codes, which are closely connected to interesting objects in finite geometry and have applications in combinatorics [2,3] and secret sharing scheme [4]. Similarly, because of their special algebraic structure, self-dual codes are another family of linear codes worth studying, and have important applications in cryptographic protocols [5,6]. For those reasons, constructing (Hermitian) self-dual MDS and NMDS codes is thus becoming a significant research topic in the theory of classical error-correcting codes. Analogous with the construction of (Hermitian) self-dual MDS codes, it is also challenging to determine the existence of a (Hermitian) self-dual NMDS code.

In recent years, researchers are trying to use different techniques to focus on investigating Euclidean and Hermitian self-dual MDS codes, especially for Euclidean case, via building-up construction method [7,8], and constacyclic codes [9,10], Glynn codes [11], rational function fields [12]. Especially recently, many Euclidean self-dual MDS codes have been presented by utilizing GRS codes [13,14,15,16,17]. In [8], Gulliver *et al.* also construct Euclidean self-dual NMDS codes of length $n = q-1$ (q is power of odd prime) derived from Reed-Solomon (i.e. RS) codes. In [18], some self-dual NMDS codes with length $n \leq 16$ were constructed over some small prime fields. Jin and Kan [19] make use of properties of elliptic curves to construct some self-dual NMDS codes. Consequently, constructing self-dual NMDS codes remains an open problem for a large range of parameters. As far as we know, however, there are few research results on Hermitian self-dual MDS and NMDS codes, for a few results, see [20,21].

In 2017, enlighten by the construction of twisted Gabidulin codes [22] in rank metric, Beelen *et al.* [23] introduce a new family of linear evaluation codes in Hamming metric: twisted Reed-Solomon (i.e. TRS) codes. The idea of TRS codes is based on RS codes, by adding further monomials, so called "twist", and selecting the evaluation points appropriately. Afterwards, Beelen *et al.* [24] also propose the generalization of the single-twist Reed-Solomon codes in [23] to the multi-twist composition. TRS codes are also shown to be largely distinct from GRS codes, which have much larger Schur squares dimension than a GRS code with the same parameters. Meanwhile, a subfamily of TRS codes are proposed as an alternative to Goppa codes for the McEliece cryptosystem [24,25], which is a public-key cryptosystem and one of the candidates for post-quantum cryptography, resulting in a potential reduction of key sizes. We call the extension of TRS codes by generalized TRS (i.e. GTRS) codes. For other recent studies on GTRS codes, please refer to [26,27,28]. In general, TRS codes are not MDS, nevertheless certain subclasses may be MDS or NMDS which are constructed by a suitable choice of the evaluation points and twist coefficients. What's more famous is that (+)-twisted Reed-Solomon codes [23], which is called (+)-TRS codes for simplicity. In [26], Huang *et al.* represent the form of check matrix of (+)-GTRS codes.

In this paper, we firstly prove that GTRS codes are also closed under Euclidean duality if we choose evaluation points which form a multiplicative group. In the following, we present the necessary and sufficient conditions of a (+)-GTRS code is Hermitian self-dual and give a new efficient construction method for self-dual (+)-GTRS

codes with respect to the Hermitian inner product. By applying the new method, we draw several classes of Hermitian self-dual MDS and NMDS codes, respectively.

The remainder of this paper is organized as follows. Basic notations and results about GTRS codes and NMDS codes are provided in Section II. The main contributions are presented in Section III. Some final remarks and hints for future works conclude the paper in Section IV.

2 Preliminaries

In this section, we recall some definitions and basic theory of Hermitian self-dual codes, GTRS codes, and NMDS codes.

2.1 Hermitian self-dual codes

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Assume that n and q are coprime, that is $\gcd(n, q) = 1, \mathbb{F}_{q^*} = \mathbb{F}_q \backslash \{0\}$. Let $\mathbb{F}_q^n$ denote the vector space of all n-tuples over the finite field $\mathbb{F}_q$. If C is a k-dimensional subspace of $\mathbb{F}_q^n$, then C will be called an $[n, k]$ linear code over $\mathbb{F}_q$. The linear code C has q^k codewords.

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^2}^n$, here we review that the Euclidean inner product of vectors $\mathbf{x}, \mathbf{y}$ is

$$\langle \mathbf{x}, \mathbf{y} \rangle_E = \sum_{i=1}^{n} x_i y_i. \tag{1}$$

The Euclidean dual code of C is defined as

$$C^{\perp_E} = \{\mathbf{x} \mid \mathbf{x} \in \mathbb{F}_{q^2}^n, \langle \mathbf{x}, \mathbf{y} \rangle_E = 0, \text{ for all } \mathbf{y} \in C\}. \tag{2}$$

It is always useful to consider another inner product, called the Hermitian inner product.

$$\langle \mathbf{x}, \mathbf{y} \rangle_H = \sum_{i=1}^{n} x_i y_i^q. \tag{3}$$

Analogous to (2), we can define the Hermitian dual of C as follows by using this inner product.

$$C^{\perp_H} = \{\mathbf{x} \mid \mathbf{x} \in \mathbb{F}_{q^2}^n, \langle \mathbf{x}, \mathbf{y} \rangle_H = 0, \text{ for all } \mathbf{y} \in C\}. \tag{4}$$

Namely, $C^{\perp_H}$ is the orthogonal subspace to C, with respect to the Hermitian inner product. We also have Hermitian self-orthogonality and Hermitian self-duality. If $C \subseteq C^{\perp_H}$, then $C^{\perp_H}$ is Hermitian self-orthogonal. Particularly, if $C^{\perp_H} = C$, then C is Hermitian self-dual.

2.2 GTRS codes and NMDS codes

The GTRS codes are formally defined as follows, for more details we refer to [23, 24].

Definition 1 Let $n, k, \ell \in \mathbb{N}$ be positive integers, where $k < n$, $\ell \leq n - k$. Choose a twist vector $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, \ldots, n-k\}^\ell$ such that the $t_i (1 \leq i \leq \ell)$ are distinct, and a hook vector $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{0, \ldots, k-1\}^\ell$ such that the $h_i (1 \leq i \leq \ell)$ are also distinct. Set $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_\ell) \in (\mathbb{F}_q^*)^\ell$. The set of $[k, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}]$-twisted polynomials over $\mathbb{F}_q$ is defined by

$$\mathcal{P}_{k,n}[\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}] = \left\{ f = \sum_{i=0}^{k-1} f_i x^i + \sum_{j=1}^{\ell} \eta_j f_{h_j} x^{k-1+t_j} : f_i \in \mathbb{F}_q \right\}. \tag{5}$$

Definition 2 Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ be pairwise distinct, $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q^*)^n$ and $1 \leq k \leq n$. Let $\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}$ and $\mathcal{P}_{k,n}[\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}]$ be defined as above. The $[\boldsymbol{\alpha}, \boldsymbol{v}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}]$-GTRS code of length n and dimension k is defined by

$$GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}] := \{[v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)] : f \in \mathcal{P}_{k,n}[\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}]\}. \tag{6}$$

The elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ are called the *code locators (evaluation points)* of $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}]$, and the elements $v_1, v_2, \ldots, v_n$ are called the *column multipliers*. The set of twisted polynomials $\mathcal{P}_{k,n}[\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}] \subseteq \mathbb{F}_q[x]$ forms a k-dimensional $\mathbb{F}_q$-linear subspace, so a GTRS code is linear code.

Let us recall the definition of NMDS codes as follows.

Definition 3 ([2]) A linear code with parameters of the form $[n, k, n-k]$ is said to be almost MDS (i.e. AMDS). Particularly, An AMDS code is an NMDS code if the dual code is also an AMDS code.

3 Main Results

3.1 Euclidean dual of GTRS codes

It is known that the dual code of a GRS code is also a GRS code. In contrast to GRS codes, GTRS also do not generally seem to be closed under duality. However, if we choose evaluation points which form a multiplicative group, this yields to the following results.

Firstly, denote the reversal matrix $\boldsymbol{J}_k \in \mathbb{F}_q^{k \times k}$ by the square matrix

$$\boldsymbol{J}_k = \begin{pmatrix} & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & \end{pmatrix}. \tag{7}$$

We denote by $V_n(\alpha)$ the $n \times n$ Vandermonde matrix over α, and Λ is the diagonal matrix $\text{diag}(v_1, v_2, \ldots, v_n)$, where

$$V_n(\alpha) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{pmatrix}. \tag{8}$$

Theorem 1 *Let C be an $[n, k]$ linear code with a generator matrix of the form*

$$G = \begin{bmatrix} I \mid L \end{bmatrix} \cdot (V_n(\alpha)\Lambda), \tag{9}$$

where $I \in \mathbb{F}_q^{k \times k}$ is the identity matrix, $L \in \mathbb{F}_q^{k \times (n-k)}$, and the entries of $\alpha \in \mathbb{F}_q^n$ are distinct and form a multiplicative group. Then the Euclidean dual code $C^{\perp_E}$ has generator matrix with the form

$$H = [I \mid J_{n-k}(-L^T)J_k] \cdot V_n(\alpha) \,\text{diag}(\alpha/n)\Lambda^{-1}. \tag{10}$$

Proof Since the entries of α form a multiplicative group, we have $\alpha_i^n = 1$, $1 \le i \le n$ and by [24], we obtain

$$(V^T)^{-1} = J \cdot V \cdot \text{diag}(\alpha/n). \tag{11}$$

Since H has rank $n - k$ so left is to show $G \cdot H^{\mathrm{T}} = 0$. Note that

$$\begin{aligned} &G \cdot H^T \\ &= [I \mid L](V\Lambda) \cdot ([I \mid J_{n-k}(-L^T)J_k] \cdot V \,\text{diag}(\alpha/n)\Lambda^{-1})^T \\ &= [I \mid L](V\Lambda) \cdot (J_{n-k}[-L^{\mathrm{T}} \mid I]J_n \cdot V \,\text{diag}(\alpha/n)\Lambda^{-1})^T \\ &= [I \mid L](V\Lambda) \cdot (J_{n-k}[-L^{\mathrm{T}} \mid I](V^{-1})^{\mathrm{T}}\Lambda^{-1})^T \\ &= [I \mid L][\begin{smallmatrix} -L \\ I \end{smallmatrix}]J_{n-k} \\ &= 0. \end{aligned}$$

So it is a parity-check matrix of C, and thus, a generator matrix of the dual code.

Theorem 1 implies the following duality statement for GTRS codes with evaluation points forming a multiplicative group, analogy to TRS codes in [24].

Theorem 2 *Let $n, k, \alpha, v, t, h, \eta$ be chosen as in Definition 2 such that the entries of α form a multiplicative subgroup of $\mathbb{F}_q^*$. Then $GTRS_{k,n}[\alpha, v, t, h, \eta]^{\perp_E}$ twisted code is equivalent to a $GTRS_{n-k,n}[\alpha, v^{-1}, k - h, n - k - t, -\eta]$ -twisted code.*

Proof By definition, we claim that a generator matrix of $GTRS_{k,n}[\alpha, v, t, h, \eta]$ is given by $G = [I \mid L] \cdot (V\Lambda)$, where the entries of $L \in \mathbb{F}_q^{k \times (n-k)}$ are of the form

$$L_{ij} = \begin{cases} \eta_\mu, & \text{if } (i, j) = (h_\mu + 1, t_\mu), \\ 0, & \text{else} \end{cases} \tag{12}$$

With the analysis as Theorem 1, a parity check matrix for $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}]$ is:

$$\boldsymbol{H} = [\boldsymbol{I} \mid \boldsymbol{J}_{n-k}(-\boldsymbol{L}^T)\boldsymbol{J}_k] \cdot \boldsymbol{V}_n(\boldsymbol{\alpha}) \operatorname{diag}(\boldsymbol{\alpha}/n)\boldsymbol{\Lambda}^{-1}. \tag{13}$$

Hence it is equivalent to a code C' generated by $\left[\boldsymbol{I} \mid -\boldsymbol{J}_{n-k}\boldsymbol{L}^T\boldsymbol{J}_k\right] \cdot \boldsymbol{V}_n(\boldsymbol{\alpha})\boldsymbol{\Lambda}^{-1}$. As we already know, the entries of $-\boldsymbol{J}_{n-k}\boldsymbol{L}^T\boldsymbol{J}_k$ are of the form

$$(-\boldsymbol{J}_{n-k}\boldsymbol{L}^T\boldsymbol{J}_k)_{i,j} = \begin{cases} -\eta_\mu, & (i, j) = \left(n - k - t_\mu + 1, k - h_\mu\right), \\ 0, & \text{else.} \end{cases} \tag{14}$$

In other words, a twist $x^{h_\mu}+\eta_\mu x^{k-1+t_\mu}$ becomes the twist $x^{n-k-t_\mu}+\left(-\eta_\mu\right)x^{n-k-1+\left(k-h_\mu\right)}$ in the dual code. Therefore the code C' is a $[k-\boldsymbol{h}, n-k-\boldsymbol{t}, -\boldsymbol{\eta}]$-twisted code, which proves the claim.

3.2 (+)-generalized twisted Reed-Solomon codes

Taking $l = 1$, $(t, h) = (1, k - 1)$ in Definition 2, Beelen *et al.* obtain a family code as the (+)-twisted Reed-Solomon codes by employing additive subgroups of $\mathbb{F}_q$. We denote generalization of the class twisted code as $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k - 1, \eta]$.

Lemma 1 *([23]) Let $k \le n \le q$, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ be pairwise distinct, $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q^*)^n$, and $\eta \in \mathbb{F}_q^*$. Then the generalized twisted code $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k - 1, \eta]$ is MDS if and only if*

$$\eta \sum_{i \in \mathcal{I}} \alpha_i \neq -1, \quad \forall \mathcal{I} \subseteq \{1, \ldots, n\} \ s.t. \ |\mathcal{I}| = k. \tag{15}$$

Next, we present the sufficient and necessary conditions that (+)-GTRS code is an NMDS code. It is easy to conclude from the proof process of Lemma 1, so we omit the details.

Lemma 2 *Let $k, n, \boldsymbol{\alpha}, \boldsymbol{v}, \eta$ be chosen as above. Then $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$ is NMDS if and only if*

$$\eta \sum_{i \in \mathcal{I}} \alpha_i = -1, \quad \exists \mathcal{I} \subseteq \{1, \ldots, n\} \ s.t. \ |\mathcal{I}| = k. \tag{16}$$

Remark 1 It can be drawn that the code $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k - 1, \eta]$ is MDS if $-\eta^{-1}$ cannot be represented as the sum of any *k evaluation points*. Furthermore, $\forall \eta \in \mathbb{F}_q^*$, $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k - 1, \eta]$ is either MDS or NMDS.

3.3 Hermitian self-dual (+)-GTRS codes

From now on, we always assume that ω is a primitive element of $\mathbb{F}_{q^2}$, that is $\mathbb{F}_{q^2}^* = \langle\omega\rangle$, and label the elements of $\mathbb{F}_q$ as $\mathbb{F}_q = \left\{a_1, a_2, \ldots, a_q\right\}$.

Meanwhile, we also always denote $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, where

$$u_i := \prod_{1 \le j \le n, j \ne i} \left(\alpha_i - \alpha_j \right)^{-1}, \ 1 \le i \le n, \tag{17}$$

and

$$a = \sum_{i=1}^{n} \alpha_i. \tag{18}$$

Next according to the check matrix of $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$ in [26], we present the following lemma.

Lemma 3 *Let $k \le n \le q^2$, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^2}^n$ be pairwise distinct, $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^2}^*)^n$, and $\eta \in \mathbb{F}_{q^2}^*$. Then the Euclidean dual of twisted code $GTRS_{k,n}$ $[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta](\eta \ne -a^{-1})$ is represented as follows.*

$$GTRS_{k,n}^{\perp_E}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$$
$$= GTRS_{n-k,n}[\boldsymbol{\alpha}, \boldsymbol{u}\boldsymbol{v}^{-1}, 1, n-k-1, -\frac{\eta}{1+a\eta}].$$

Remark 2 In Theorem 2, suppose that $\boldsymbol{\alpha}$ form a multiplicative subgroup of $\mathbb{F}_{q^2}$, then $a = \sum_{i=1}^{n} \alpha_i = 0$, and set $l = 1$, $(t, h) = (1, k-1)$, then $GTRS_{k,n}^{\perp_E}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta] = GTRS_{n-k,n}[\boldsymbol{\alpha}, \boldsymbol{u}\boldsymbol{v}^{-1}, 1, n-k-1, -\eta]$. Thus the result of Lemma 3 is a special case of Theorem 2 and vice versa.

According to Lemma 3, we obtain the corollary as follows.

Corollary 3 *Let $\boldsymbol{1}$ be all-one word of length n. Then the Euclidean dual code of $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{1}, 1, k-1, \eta](\eta \ne -a^{-1})$ is*

$$GTRS_{k,n}^{\perp_E}[\boldsymbol{\alpha}, \boldsymbol{1}, 1, k-1, \eta]$$
$$= GTRS_{n-k,n}[\boldsymbol{\alpha}, \boldsymbol{u}, 1, n-k-1, -\frac{\eta}{1+a\eta}]$$
$$= \{(u_1 g(\alpha_1), \ldots, u_n g(\alpha_n)) | g(x) \in \mathbb{F}_{q^2}[x]\},$$

where $g(x) = \sum_{i=0}^{n-k-2} g_i x^i + g_{n-k-1}(x^{n-k-1} - \frac{\eta}{1+a\eta} x^{n-k})$, $g_i \in \mathbb{F}_{q^2}, 0 \le i \le n-k-1$ with $g_{n-k-1} \ne 0$.

In the following, we show that the necessary and sufficient conditions for (+)-GTRS codes being Hermitian self-dual.

Theorem 4 *Keep the above notations, let $n = 2k$, then $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta](\eta \ne -a^{-1})$ over $\mathbb{F}_{q^2}$ is Hermitian self-dual if and only if there exists a polynomial $g(x) = \sum_{i=0}^{k-2} g_i x^i + g_{k-1}(x^{k-1} - \frac{\eta}{1+a\eta} x^k)$, $g_i \in \mathbb{F}_{q^2}, 0 \le i \le k-1$ with $g_{k-1} \ne 0$ such that*

$$v_i^{q+1} f^q(\alpha_i) = u_i g(\alpha_i), 1 \le i \le n. \tag{19}$$

Proof Note that $GTRS_{k,n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$ has a generator matrix given by $G_k(\boldsymbol{\alpha}, \boldsymbol{v}, \eta)$. Clearly, we have $G_k(\boldsymbol{\alpha}, \boldsymbol{v}, \eta) = G_k(\boldsymbol{\alpha}, \mathbf{1}, \eta)\Lambda$, where

$$
G_k(\boldsymbol{\alpha}, \mathbf{1}, \eta) = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
\alpha_1 & \alpha_2 & \cdots & \alpha_n \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1^{k-2} & \alpha_2^{k-2} & \cdots & \alpha_n^{k-2} \\
\alpha_1^{k-1} + \eta\alpha_1^k & \alpha_2^{k-1} + \eta\alpha_2^k & \cdots & \alpha_n^{k-1} + \eta\alpha_n^k
\end{pmatrix},
$$

and Λ is the diagonal matrix $\operatorname{diag}(v_1, v_2, \ldots, v_n)$. It follows that $GTRS_{\frac{n}{2},n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$ over $\mathbb{F}_{q^2}$ is Hermitian self-dual if and only if for any codeword $\mathbf{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n))$ of $GTRS_{\frac{n}{2},n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$,

$$
\begin{aligned}
&\mathbf{c}^q \cdot G_{\frac{n}{2}}(\boldsymbol{\alpha}, \boldsymbol{v}, \eta)^T \\
={} &\mathbf{c}^q \cdot (G_{\frac{n}{2}}(\boldsymbol{\alpha}, \mathbf{1}, \eta)\Lambda)^T \\
={} &(v_1^{q+1} f^q(\alpha_1), \ldots, v_n^{q+1} f^q(\alpha_n)) \cdot G_{\frac{n}{2}}(\boldsymbol{\alpha}, \mathbf{1}, \eta)^T \\
={} &\mathbf{0} \\
\Leftrightarrow{} &(v_1^{q+1} f^q(\alpha_1), \ldots, v_n^{q+1} f^q(\alpha_n)) \in GTRS_{\frac{n}{2},n}^{\perp_E}[\boldsymbol{\alpha}, \mathbf{1}, 1, k-1, \eta].
\end{aligned}
$$

Recall that the Euclidean dual of $GTRS_{\frac{n}{2},n}[\boldsymbol{\alpha}, \mathbf{1}, 1, k-1, \eta]$ is $GTRS_{\frac{n}{2},n}[\boldsymbol{\alpha}, \boldsymbol{u}, 1, k-1, -\frac{\eta}{1+a\eta}]$, now the desired result follows immediately from Corollary 3. $\square$

3.4 Hermitian self-dual MDS and NMDS codes

In this section, we mainly present our contribution to construct several classes of Hermitian self-dual MDS and NMDS codes. To do that, we consider the Hermitian self-dual (+)-GTRS codes in Theorem 4. We first give the following basic lemmas from [30].

Lemma 4 *If ω is a primitive element of $\mathbb{F}_{q^2}$, then there exists a $\xi \in \mathbb{F}_{q^2}$ such that $\omega^q + \omega = \xi^{q+1}$, that is $\omega^q + \omega \in \mathbb{F}_q$.*

Proof Since $(\omega^q + \omega)^q = \omega^{q^2} + \omega^q = \omega + \omega^q$, that is $(\omega^q + \omega)^{q-1} = 1$, then it is a straight-forward fact that $\omega^q + \omega \in \mathbb{F}_q$. $\square$

Lemma 5 *The equation $\zeta^q + \zeta^{q-1} + 1 = 0$ with regard to ζ has q distinct nonzero roots over the finite field $\mathbb{F}_{q^2}$.*

Next, we present our discussions according to two classes different values of *code locators $\boldsymbol{\alpha}$*.

(I) Fix $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. $\forall\ 1 \le l \le q$, set

$$
A_l = a_l\beta + \mathbb{F}_q := \{a_l\beta + x : x \in \mathbb{F}_q\}. \tag{20}
$$

In general, here we always set $\beta = \omega$.

Theorem 5 *Let q be a prime power, $n = 2k, n \le q$, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in A_l^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct elements. If $a = 0$ and $q = 2^s$ are not met at the same time, then there exists a vector $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^2}^*)^n$, and $\eta \in \mathbb{F}_{q^2}^*$ such that GTRS$_{\frac{n}{2},n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$ is an $\left[n, \frac{n}{2}, \frac{n}{2} + 1\right]$ Hermitian self-dual GTRS code over $\mathbb{F}_{q^2}$.*

Proof As can be seen, $|A_l| = q$. Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in A_l^n$, then it is a straightforward fact that

$$u_i = \prod_{1 \le j \le n, j \ne i} \left(x_i - x_j\right)^{-1}. \tag{21}$$

It is obvious that $u_i \in \mathbb{F}_q^*$, thus there exists $v_i \in \mathbb{F}_{q^2}^*$ such that $v_i^{q+1} = u_i$. Set $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$.

Let $\omega^q + \omega = \xi^{q+1}$, then

$$
\begin{aligned}
\alpha_i^q &= (a_l\omega + x_i)^q \\
&= a_l^q\omega^q + x_i^q \\
&= a_l(\xi^{q+1} - \omega) + x_i \\
&= (a_l\omega + x_i) + (\xi^{q+1} - 2\omega)a_l \\
&= \alpha_i + (\xi^{q+1} - 2\omega)a_l.
\end{aligned}
$$

For all $f(x) \in \mathbb{F}_{q^2}[x]$ with form $f(x) = \sum_{i=0}^{k-2} f_i x^i + f_{k-1}(x^{k-1} + \eta x^k), f_{k-1} \ne 0$, we will discuss it in two ways.

(1) In the case of $a = 0$ and $q \ne 2^s$, set $\eta^q = -\eta$, and $h(x) = \sum_{i=0}^{k-2} f_i^q x^i + f_{k-1}^q(x^{k-1} - \eta x^k)$. By $\alpha_i^q = \alpha_i + (\xi^{q+1} - 2\omega)a_l$, therefore

$$
\begin{aligned}
f^q(\alpha_i) &= \sum_{j=0}^{k-2} f_j^q(\alpha_i^q)^j + f_{k-1}^q((\alpha_i^q)^{k-1} + \eta^q(\alpha_i^q)^k) \\
&= h(\alpha_i + (\xi^{q+1} - 2\omega)a_l).
\end{aligned}
$$

Set $g(x) = h(x + (\xi^{q+1} - 2\omega)a_l)$, then there exists $g(x) = \sum_{i=0}^{k-2} g_i x^i + g_{k-1}(x^{k-1} - \eta x^k) \in \mathbb{F}_{q^2}[x]$ with $g_{k-1} \ne 0$ such that $f^q(\alpha_i) = g(\alpha_i), 1 \le i \le n$. Therefore, there exists a $g(x)$ such that $v_i^{q+1} f^q(\alpha_i) = u_i g(\alpha_i), 1 \le i \le n$. By Theorem 4, GTRS$_{\frac{n}{2},n}[\boldsymbol{\alpha}, \boldsymbol{v}, 1, k-1, \eta]$ is a Hermitian self-dual GTRS code.

(2) In the case of $a \ne 0$, set $\eta^q = \mu\eta, \mu \in \mathbb{F}_{q^2}$ and $h(x) = \sum_{i=0}^{k-2} f_i^q x^i + f_{k-1}^q(x^{k-1} + \mu\eta x^k)$. By $\alpha_i^q = \alpha_i + (\xi^{q+1} - 2\omega)a_l$, therefore $f^q(\alpha_i) = h(\alpha_i + (\xi^{q+1} - 2\omega)a_l)$.

Set $g(x) = h(x + (\xi^{q+1} - 2\omega)a_l)$, to make $g(x)$ has form $g(x) = \sum_{i=0}^{k-2} g_i x^i + g_{k-1}(x^{k-1} - \frac{\eta}{1+a\eta} x^k) \in \mathbb{F}_{q^2}[x]$ with $g_{k-1} \ne 0$, by analyzing the coefficient of x^{k-1} and x^k on both sides, then

$$\frac{\mu\eta}{k(\xi^{q+1} - 2\omega)a_l\mu\eta + 1} = -\frac{\eta}{1 + a\eta}. \tag{22}$$

Combining with $\eta^q = \mu\eta$ and Equation (22), then

$$[k(\xi^{q+1} - 2\omega)a_l + a]\eta^q + \eta^{q-1} + 1 = 0. \tag{23}$$

It is easy to prove that $A \triangleq k(\xi^{q+1} - 2\omega)a_l + a = \sum_{i=1}^{n} x_i + k\xi^{q+1}a_l \in \mathbb{F}_q$. Setting $\zeta = A\eta$ transforms Equation (23) to $\zeta^q + \zeta^{q-1} + A^{q-1} = 0$, that is $\zeta^q + \zeta^{q-1} + 1 = 0$. By Lemma

5, Equation (23) has q distinct nonzero roots in $\mathbb{F}_{q^2}$. Then there exists a $g(x)$ such that $f^q(\alpha_i) = g(\alpha_i), 1 \le i \le n$. Therefore, there exists a $g(x)$ such that $v_i^{q+1} f^q(\alpha_i) = u_i g(\alpha_i), 1 \le i \le n$. By Theorem 4, $GTRS_{\frac{n}{2},n}[\alpha, v, 1, k-1, \eta]$ is a Hermitian self-dual GTRS code, which proves the claim.

(II) Let $\beta_m = \omega^m, 1 \le m \le q, \forall 1 \le l \le q$, denote

$$A_{l,m} = a_l + \mathbb{F}_q \cdot \beta_m := \{a_l + \beta_m x : x \in \mathbb{F}_q\}. \tag{24}$$

Theorem 6 *Let q be a prime power, $n = 2k, n \le q$, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in A_{l,m}^n$ with $\alpha_1, \alpha_2, \ldots, \alpha_n$ distinct elements. If $a = 0$ and $q = 2^s$ are not met at the same time, then there exists a vector $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^2}^*)^n$, and $\eta \in \mathbb{F}_{q^2}^*$ such that $GTRS_{\frac{n}{2},n}[\alpha, v, 1, k-1, \eta]$ is an $\left[n, \frac{n}{2}, \frac{n}{2}+1\right]$ Hermitian self-dual GTRS code over $\mathbb{F}_{q^2}$.*

Proof As can be seen, $|A_{l,m}| = q$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in A_{l,m}^n$, then it can be shown that

$$u_i = \beta_m^{-(n-1)} \prod_{1 \le j \le n, j \ne i} \left(x_i - x_j\right)^{-1}. \tag{25}$$

Let $\lambda = \beta_m^{n-1} = \omega^{m(n-1)} \in \mathbb{F}_{q^2}^*$, thus there exists $v_i \in \mathbb{F}_{q^2}^*$ such that $v_i^{q+1} = \lambda u_i$. It turns out that $\alpha_i^q = \beta_m^{q-1} \alpha_i + (1 - \beta_m^{q-1}) a_l$. For all $f(x) \in \mathbb{F}_{q^2}[x]$ with form $f(x) = \sum_{i=0}^{k-2} f_i x^i + f_{k-1}(x^{k-1} + \eta x^k), f_{k-1} \ne 0$, set $h(x) = \sum_{i=0}^{k-2} f_i^q x^i + f_{k-1}^q(x^{k-1} + \mu\eta x^k)$, and $\eta^q = \mu\eta$. By $\alpha_i^q = \beta_m^{q-1} \alpha_i + (1 - \beta_m^{q-1}) a_l$, then

$$f^q(\alpha_i) = \sum_{j=0}^{k-2} f_j^q(\alpha_i^q)^j + f_{k-1}^q((\alpha_i^q)^{k-1} + \eta^q(\alpha_i^q)^k)$$

$$= h(\beta_m^{q-1} \alpha_i + (1 - \beta_m^{q-1}) a_l).$$

Set $g(x) = \lambda h(\beta_m^{q-1} x + (1 - \beta_m^{q-1}) a_l)$, we also consider the following two cases.

(1) In the case of $a = 0$ and $q \ne 2^s$, to make $g(x)$ has the form $g(x) = \sum_{i=0}^{k-2} g_i x^i + g_{k-1}(x^{k-1} - \eta x^k) \in \mathbb{F}_{q^2}[x]$ with $g_{k-1} \ne 0$, then by considering the coefficient of x^{k-1} and x^k on both sides, then

$$\lambda\mu\eta(\beta_m^{q-1})^k = -\lambda\eta(\beta_m^{q-1})^{k-1}. \tag{26}$$

that is

$$\mu\beta_m^{q-1} = -1. \tag{27}$$

Combining with $\eta^q = \mu\eta$ and Equation (27), then

$$\eta^{q-1} = -\beta_m^{-(q-1)}. \tag{28}$$

Obviously, Equation (28) has $q-1$ distinct nonzero roots in $\mathbb{F}_{q^2}$.

(2) In the case of $a \ne 0$, to make $g(x)$ has form $g(x) = \sum_{i=0}^{k-2} g_i x^i + g_{k-1}(x^{k-1} - \frac{\eta}{1+a\eta} x^k) \in \mathbb{F}_{q^2}[x]$ with $g_{k-1} \ne 0$, by analyzing the coefficient of x^{k-1} and x^k on both sides, then

$$\frac{\mu\eta\beta_m^{q-1}}{1 + k\mu\eta(1 - \beta_m^{q-1})a_l} = -\frac{\eta}{1 + a\eta}. \tag{29}$$

Table 1 Some Hermitian self-dual $GTRS_{3,6}[\alpha, v, 1, 2, \eta]$ with parameters $[6, 3, 4]$ or $[6, 3, 3]$ over $\mathbb{F}_{7^2}$.

Class	a	Para.	α	v	η
(I)	$a = 0$	$[6, 3, 4]$	$(1, 2, 3, 4, 5, 6)$	$(\omega^4, 1, \omega^{11}, 3, \omega^9, \omega)$	$\{\omega^4, \omega^{12}, \omega^{20}, \omega^{28}, \omega^{36}, \omega^{44}\}$
(I)	$a \neq 0$	$[6, 3, 4]$	$(\omega, \omega^2, \omega^5, \omega^{11}, \omega^{31}, \omega^{36})$	$(\omega^2, \omega^5, \omega^6, \omega^{10}, \omega, \omega^3)$	$\{\omega^{17}, \omega^{23}, \omega^{27}, \omega^{38}, 5, \omega^{45}\}$
(I)	$a \neq 0$	$[6, 3, 3]$	$(\omega, \omega^2, \omega^5, \omega^{11}, \omega^{31}, \omega^{36})$	$(\omega^2, \omega^5, \omega^6, \omega^{10}, \omega, \omega^3)$	$\{\omega^{26}\}$
(II)	$a = 0$	$[6, 3, 4]$	$(\omega^4, \omega^{28}, \omega^{20}, \omega^{44}, \omega^{12}, \omega^{36})$	$(\omega, \omega^{10}, \omega^3, 1, \omega^2, \omega^{11})$	$\{1, 2, 3, 4, 5, 6\}$
(II)	$a \neq 0$	$[6, 3, 4]$	$(\omega, \omega^{25}, 0, \omega^{17}, \omega^{41}, \omega^9)$	$(\omega^2, 1, \omega^5, \omega^3, \omega^4, \omega)$	$\{3, \omega^{14}, \omega^{17}, \omega^{18}, \omega^{29}, \omega^{36}\}$
(II)	$a \neq 0$	$[6, 3, 3]$	$(\omega, \omega^{25}, 0, \omega^{17}, \omega^{41}, \omega^9)$	$(\omega^2, 1, \omega^5, \omega^3, \omega^4, \omega)$	$\{\omega^{31}\}$

Combining with $\eta^q = \mu\eta$ and Equation (29), then

$$[k(1 - \beta_m^{q-1})a_l + a\beta_m^{q-1}]\eta^q + \beta_m^{q-1}\eta^{q-1} + 1 = 0. \tag{30}$$

Denoting $B \triangleq \frac{k(1-\beta_m^{q-1})a_l + a\beta_m^{q-1}}{\beta_m^{q-1}}$, and setting $\zeta = B\eta$ transforms Equation (30) to $\zeta^q + \zeta^{q-1} + (B\beta_m^{-1})^{q-1} = 0$, it is easy to know $B\beta_m^{-1} \in \mathbb{F}_q$, that is $\zeta^q + \zeta^{q-1} + 1 = 0$. By Lemma 5, Equation (30) has q distinct nonzero roots in $\mathbb{F}_{q^2}$.

From the above discussions, it follows that there exists a $g(x)$ such that $f^q(\alpha_i) = \lambda^{-1}g(\alpha_i), 1 \leq i \leq n$. Therefore, there exists a $g(x)$ such that $v_i^{q+1}f^q(\alpha_i) = u_i g(\alpha_i), 1 \leq i \leq n$. By Theorem 4, the conclusion is established.

Remark 3 In the light of Theorem 2.5 in [26], suppose that $a = 0$, then $GTRS_{\frac{n}{2},n}[\alpha, v, 1, k-1, \eta]$ can not be a Euclidean self-dual MDS code, however, it can be a Hermitian self-dual MDS code.

Building on Theorems 5 and 6, and by Lemmas 1 and 2, we derive two striking conclusions.

Corollary 7 *In Theorems 5 and 6, if $a = 0$, then a Hermitian self-dual GTRS code $GTRS_{\frac{n}{2},n}[\alpha, v, 1, k-1, \eta]$ is a MDS code over $\mathbb{F}_{q^2}$.*

Corollary 8 *In Theorems 5 and 6, if $a\eta + 2 = 0$, then a Hermitian self-dual GTRS code $GTRS_{\frac{n}{2},n}[\alpha, v, 1, k-1, \eta]$ is NMDS. Otherwise, $GTRS_{\frac{n}{2},n}[\alpha, v, 1, k-1, \eta]$ is a MDS code over $\mathbb{F}_{q^2}$.*

Example 1 To be more precise, let $q = 7$, we present some examples of Hermitian self-dual GTRS codes $GTRS_{3,6}[\alpha, v, 1, 2, \eta]$ over $\mathbb{F}_{7^2}$ in Table 1.

Remark 4 As a potential application in McEliece cryptosystem, GTRS codes play an important role in reducing the public key size for a given security level. In addition, according to [31], some choices of the system parameters can avoid the mentioned attack, e.g. using codes with rate $R \simeq \frac{1}{2}$. We know a self-dual code have rate $R = \frac{1}{2}$. On the other hand, people begin to construct cryptosystem by using variant codes of original GRS and GTRS codes, It is worth noting that TRS codes are also subcodes of GRS codes. We know the generator matrix and dimension of subfield subcodes of GRS and GTRS codes are not guaranteed and depends on the actual choice of code

locators $\mathbf{a}$, column multipliers $\mathbf{v}$ and variable η [32]. Our investigation on determining Hermitian self-dual GTRS codes with pairs of $(\mathbf{a}, \mathbf{v}, \eta)$, which are expected that these codes and their subcodes can be used for constructing McEliece code-based cryptosystems with resisting some more known structural attacks.

4 Conclusion and discussion

In this paper, we mainly propose a systematical approach to construct Hermitian self-dual (+)-GTRS codes for the first time. Finally, we obtain several classes of q^2-ary Hermitian self-dual MDS and NMDS codes derived from these GTRS codes. Further, the techniques developed in this paper can be also applied for these MDS codes in [33] to obtain new Hermitian self-dual MDS codes. Meanwhile it is also a worthy research topic to construct Hermitian self-orthogonal (especially almost self-dual) and Hermitian LCD MDS and NMDS codes through GTRS codes applying this method.

References

1. Roth, R. M., Lempel, A.: A construction of non-Reed-Solomon type MDS codes. IEEE Trans. Inf. Theory **35**(3), 655-657 (1989)
2. Dodunekov, S., Landgev, I.: On near-MDS codes. J. Geometry **54**, 30-43 (1995)
3. Landjev, I., Rousseva, A.: The main conjecture for near-MDS codes. Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich. WCC2015-9th International Workshop on Coding and Cryptography (2015)
4. Zhou, Y., Wang, F., Xin, Y., Luo, S., Qing, S., Yang, Y.: A secret sharing scheme based on near-MDS codes. In Proc. IC-NIDC, 833-836 (2009)
5. Dougherty, S. T., Mesnager, S., Sole, P.: Secret-sharing schemes based on self-dual code. In Proc. Inf. Theory Workshop, 338-342 (2008)
6. Massey, J.: Some applications of coding theory in cryptography. In Proc. 4th IMA Conf. Cryptogr. Coding, 33-47 (1995)
7. Kim, J. L., Lee, Y.: Euclidean and Hermitian self-dual MDS codes over large finite fields. J. Comb. Theory Ser. A **105**(1), 79-95 (2006)
8. Gulliver, T. A., Kim, J. L., Lee, Y.: New MDS or near-MDS self-dual codes. IEEE Trans. Inf. Theory **54**(9), 4354-4360 (2008)
9. Guenda, K.: New MDS self-dual codes over finite fields. Des. Codes Cryptogr. **62**(1), 31-42 (2012)
10. Tong, H., Wang, X. New MDS Euclidean and Hermitian self-dual codes over finite fields. Adv. Pure Math. **7**(5), 325-333 (2017)
11. Baicheva, T., Bouyukliev, I., Dodunekov, S., Willems, W.: On the $[10, 5, 6]_9$ Reed-Solomon and Glynn codes. Mathematica Balkanica, New Series **18**, 67-78 (2004)
12. Sok, L.: Explicit constructions of MDS self-dual codes. IEEE Trans. Inf. Theory **66**(6), 3603-3615 (2020)
13. Jin, L., Xing, C.: New MDS self-dual codes from generalized Reed-Solomon codes. IEEE Trans. Inf. Theory **63**(3), 1434-1438 (2017)
14. Fang, W., Fu, F.-W.: New constructions of MDS Euclidean self-dual codes from GRS codes and extended GRS codes. IEEE Trans. Inf. Theory **65**(9), 5574-5579 (2019)
15. Fang, X., Labad, K., Liu, H., Luo, J.: New MDS self-dual codes over finite fields of odd characteristic. Des. Codes Cryptogr. **88**(6), 1127-1138 (2020)
16. Fang, W., Zhang, J., Xia, S.-T., Fu, F.-W.: A note on self-dual generalized Reed-Solomon codes. arXiv:2005.11732, [online] (2020)
17. Zhang, A., Feng, K.: A unified approach to construct MDS self-dual codes via Reed-Solomon codes. IEEE Trans. Inf. Theory **66**(6), 3650-3656 (2020)
18. Kotsireas, I. S., Koukouvinos, C., Simos, D. E.: MDS and near-MDS self-dual codes over large prime fields. Advances in Mathematics of Communications **3**(4), 349-361 (2009)

19. Jin, L., Kan, H.: Self-dual near MDS codes from elliptic curves. IEEE Trans. Inform. Theory **65**(4), 2166-2170 (2019)
20. Guo, G., Li, R.: Hermitian self-Dual GRS and extended GRS codes. IEEE Commun. Lett. **25**(4), 1062-1065 (2021)
21. Niu, Y., Yue, Q., Wu, Y., Hu, L.: Hermitian self-dual, MDS, and generalized Reed-Solomon codes. IEEE Commun. Lett. **23**(5), 781-784 (2019)
22. Sheekey, J.: A new family of linear maximum rank distance codes. Adv. Math. Commun. **10**, 475-488 (2016)
23. Beelen, P., Puchinger, S., Rosenkilde, né N. J.: Twisted Reed-Solomon codes. In IEEE Int. Symp. Inf. Theory (ISIT), 336-340 (2017)
24. Beelen, P., Bossert, M., Puchinger, S., Rosenkilde, né N. J.: Structural properties of twisted Reed-Solomon codes with applications to code-based cryptography. In IEEE Int. Symp. Inf. Theory (ISIT), 946-950 (2018)
25. Lavauzelle, J., Renner, J.: Cryptanalysis of a system based on twisted Reed-Solomon codes. Designs, Codes and Cryptography **88**(7), 1285-1300 (2020)
26. Huang, D., Yue, Q., Niu, Y., Li, X.: MDS or NMDS self-dual codes from twisted generalized Reed-Solomon codes. Des. Codes Cryptogr. 89, 2195-2209 (2021)
27. Wu, Y. Twisted Reed-Solomon codes with one-dimensional Hull. IEEE Commun. Lett. **25**(2), 383-386 (2021)
28. Wu, Y., Hyun, J. Y., Lee, Y.: New LCD MDS codes of non-Reed-Solomon type. IEEE Trans. Inf. Theory 67, 5069-5078 (2021)
29. Liu, H., Liu, S.: New constructions of MDS twisted Reed-Solomon codes and LCD MDS codes. Des. Codes Cryptogr. 89, 2051-2065 (2021)
30. Mullen, G. L., Panario, D.: Handbook of finite fields. Discrete Mathematics and its Applications. Boca Raton, FL, USA: CRC Press (2013)
31. Baldi, M., Chiaraluce, F., Rosenthal, J., Santini, P., Schipani, D.: Security of generalized Reed-Solomon code-based cryptosystems. IET Information Security 13, 404-410 (2019)
32. Senger, C., Bohara, R.: A linear algebraic approach to subfield subcodes of GRS codes. In Proc. IEEE Int. Symp. Inf. Theory (ISIT), 6-10 (2018)
33. Neri, A.: Twisted linearized Reed-Solomon codes: A skew polynomial framework, arXiv:2105.10451, [online] (2021)