Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2018) 42: 349 – 359
© TÜBİTAK
doi:10.3906/mat-1607-49

Two-dimensional generalized discrete Fourier transform and related quasi-cyclic Reed–Solomon codes

Majid MAZROOEI*, **Lale RAHIMI**, **Najme SAHAMI**
Department of Mathematics, University of Kashan, Kashan, Iran

Received: 19.07.2016 • **Accepted/Published Online:** 18.05.2017 • **Final Version:** 22.01.2018

Abstract: Using the concept of the partial Hasse derivative, we introduce a generalization of the classical 2-dimensional discrete Fourier transform, which will be called 2D-GDFT. Begining with the basic properties of 2D-GDFT, we proceed to study its computational aspects as well as the inverse transform, which necessitate the development of a faster way to calculate the 2D-GDFT. As an application, we will employ 2D-GDFT to construct a new family of quasi-cyclic linear codes that can be assumed to be a generalization of Reed–Solomon codes.

Key words: Discrete Fourier transform, partial Hasse derivative, Reed–Solomon codes

1. Introduction

The relationship between one- and two-dimensional Fourier transforms is similar in the discrete domain. Let ω be an nth root of unity in the Galois field F_q, where q is a prime power p^a. Recall that the discrete Fourier transform (DFT) of an n-bit vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1}) \in F_q^n$, n coprime with p, is defined as follows:

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

where $V_j = \sum_{i=0}^{n-1} v_i \omega^{ij}$, $j = 0, \cdots, n-1$. The vector $\mathbf{v}$ is related to its spectrum $\mathbf{V} = \mathcal{F}\{\mathbf{v}\}$ by

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

where n is interpreted as an integer of the field.

Two-dimensional Fourier transform of an $M \times N$-matrix $A = [a_{ij}] \in (F_q)^{M \times N}$, M and N relatively prime to p, is similarly defined as an $M \times N$-matrix $B = [b_{ij}]$ by

$$B_{kl} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} A_{ij} \alpha^{ik} \beta^{jl}, \quad k = 0, \cdots, M-1, \quad l = 0, \cdots, N-1,$$

where α and β are respectively an Mth root of unity and an Nth root of unity in some (sufficiently large)

*Correspondence: m.mazrooei@kashanu.ac.ir
2010 *AMS Mathematics Subject Classification:* Primary 42B10, 43A32; Secondary 94B05

extension of F_q. In this case, the inverse transform is given by

$$A_{ij} = \frac{1}{MN} \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} B_{kl} \alpha^{-ik} \beta^{-jl}.$$

The importance of two-dimensional DFT arises when we deal with the problem of evaluating the one-dimensional DFT of a vector $\mathbf{v}$ having a large number of elements, on the hypothesis that the working memory of the available processor is not sufficient to handle the vector as a whole. Such a situation can arise in several applications [1,4,5,12], such as Fourier transform spectroscopy or musical sound analysis. In this case it is convenient to fold $\mathbf{v}$ into a matrix A and apply the two-dimensional DFT on the corresponding matrix A.

Some generalizations of the concept of (one and two-dimensional) DFT were given by earlier authors. In [3], (one and two-dimensional) generalized DFT (GFT) was introduced and some basic properties were derived. In particular, it was shown that a given one-dimensional GFT on a vector $\mathbf{v}$ can be performed by means of an infinite number of two-dimensional GFTs on a matrix A whose elements are the elements of $\mathbf{v}$ properly ordered. In [6], multidimensional generalized DFT was introduced and its characteristics were investigated while some general results were derived that included as particular cases the properties previously given in [3].

Here, the key point is that previously introduced two-dimensional GFTs have an inverse only if the characteristic of the field structuring the alphabet was zero or coprime with both M and N, where M and N denote the number of rows and columns of input matrices, respectively. To relax that condition, we shall introduce a new kind of two-dimensional DFT, called the two-dimensional generalized DFT (2D-GDFT), which in turn relies on the concept of the partial Hasse derivative of two-variable polynomials. We will show that the 2D-GDFT enjoys all basic properties of DFT analogously. As an application, using the 2D-GDFT, we will construct a family of linear codes, called quasi-cyclic Reed–Solomon codes.

2. Preliminaries

2.1. Linear codes

Linear codes are widely studied because of their algebraic structure, which makes them easier to describe than nonlinear codes.

Let $q = p^a$ be a prime power and let F_q denote the finite field of order q. A linear code C of length n over F_q is an F_q-vector subspace of F_q^n. The (Hamming) weight of a vector $\mathbf{c} \in (F_q)^n$ is the number $w(\mathbf{c})$ of its nonzero coordinates. For a linear code C, the distance $d(C)$ is defined as the minimum weight of nonzero words. The distance of a code C is important to determine the error correction capability of C (that is, the number of errors that the code can correct) and its error detection capability (that is, the number of errors that the code can detect).

We denote by T the standard shift operator on F_q^n. A (linear) code is said to be quasi-cyclic of index l or l-quasi-cyclic if and only if it is invariant under T^l.

2.2. (Partial) Hasse derivatives

Recall that the uth Hasse derivative ($u = 0, 1, \cdots$) of a polynomial $f(x) = \sum_i a_i x^i \in F_q[x]$ is defined as the polynomial $f^{[u]}(x) = \sum_i \binom{i}{u} a_i x^{i-u}$. Analogously, for a bivariate polynomial $f(x, y) = \sum_{i,j} a_{ij} x^i y^j \in F_q[x, y]$, the (u,v)th partial Hasse (partial mixed) derivative of f, denoted by $f^{[u,v]}(x,y)$, is defined by

$$f^{[u,v]}(x,y) = \sum_{i,j} \binom{i}{u}\binom{j}{v} a_{ij} x^{i-u} y^{j-v}.$$

Here we use a standard convention for binomial cofficients: $\binom{k}{l} = 0$ for all $l > k$, which guarantees that the (u,v)th Hasse derivative is again a polynomial over F_q.

3. Two-dimensional 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, so the classical theory of discrete Fourier transform does not apply to $F_q[x]/\langle x^n - 1\rangle$. However, Massey and Serconek [9] introduced a generalized discrete Fourier transform (GDFT) as follows.

Let $\mathbf{c} = \sum_{i=0}^{n-1} c_i x^i \in F_q[x]$, and let ζ be an mth 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

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

Note that $\hat{c}_{g,h} = \mathbf{c}^{[g]}(\zeta^h)$.

Then the GDFT of $\mathbf{c}$ can be described in terms of a matrix:

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

Motivated by the above definition, we give the following generalization of two-dimensional DFT.

Definition 3.1 *Let $m = p^a m'$ and $n = p^b n'$, m' and n' relatively prime to p, and assume that α and β are the m'th root of unity and n'th root of unity in some (sufficiently large) extension of F_q, respectively. Let $\mathbf{c} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j} x^i y^j \in F_q[x,y]$. The two-dimensional generalized discrete Fourier transform (2D-GDFT, for short) of the bivariate $\mathbf{c}(x,y)$ is a $p^{a+b} \times m'n'$-matrix $\hat{\mathbf{c}}$ whose the rows are indexed by all pairs (g,h), $0 \leq g \leq p^a - 1$ and $0 \leq h \leq p^b - 1$, the columns are indexed by all pairs (u,v), $0 \leq u \leq m' - 1$ and $0 \leq v \leq n' - 1$, and*

$$\begin{aligned} \hat{c}_{(g,h),(u,v)} &= \mathbf{c}^{[g,h]}(\alpha^u, \beta^v) \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \binom{i}{g}\binom{j}{h} c_{i,j} \alpha^{u(i-g)} \beta^{v(j-h)}. \end{aligned}$$

To be convenient, we assume that the rows and the columns of the matrix $\hat{\mathbf{c}}$ are ordered lexicographically.

Just as the DFT, the 2D-GDFT enjoys the modulation and translation properties as well as some other nice relations.

Proposition 3.2 *If* $\mathbf{c} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j}x^iy^j \leftrightarrow \hat{\mathbf{c}} = [\hat{c}_{(g,h),(u,v)}]$ *is a 2D-GDFT pair, then the following are 2D-GDFT pairs:*

$$(1)\quad \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha^{il}c_{i,j}x^iy^j \leftrightarrow [\alpha^{gl}\hat{c}_{(g,h),(l+u,v)}],$$

$$(2)\quad \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \beta^{jk}c_{i,j}x^iy^j \leftrightarrow [\beta^{hk}\hat{c}_{(g,h),(u,k+v)}],$$

$$(3)\quad \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j-l}x^iy^j \leftrightarrow [\sum_{k=0}^{l}\binom{l}{k}\beta^{v(l-k)}\hat{c}_{(g,h-k),(u,v)}],$$

$$(4)\quad \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i-l,j}x^iy^j \leftrightarrow [\sum_{k=0}^{l}\binom{l}{k}\alpha^{u(l-k)}\hat{c}_{(g-k,h),(u,v)}],$$

$$(5)\quad \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{l-i,j}x^iy^j \leftrightarrow [\sum_{k=0}^{l}\sum_{r=0}^{g-k-1}(-1)^{g-k}\binom{l}{k}\binom{g-k-1}{r}\alpha^{u(-2g+l+k)+r}\hat{c}_{(g-k-r,h),(-u,v)}],$$

where $k,l \geq 0$ *are integers and all indices are calculated modulo appropriate* $t \in \{m,n,p^a,p^b\}$.

Proof Let $\mathbf{c}' = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{il}c_{i,j}x^iy^j$. Then

$$\begin{aligned}
\hat{c'}_{(g,h),(u,v)} &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\binom{i}{g}\binom{j}{h}\alpha^{il}c_{i,j}\alpha^{u(i-g)}\beta^{v(j-h)} \\
&= \alpha^{gl}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\binom{i}{g}\binom{j}{h}c_{i,j}\alpha^{(u+l)(i-g)}\beta^{v(j-h)} \\
&= \alpha^{gl}\hat{c}_{(g,h),(u+l,v)}.
\end{aligned}$$

The proof of the second equality is similar to (1). To prove (3) (and similarly (4)), let $\mathbf{s} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}c_{i,j-l}x^iy^j$.

Then

$$\begin{aligned}
\hat{s}_{(g,h),(u,v)} &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\binom{i}{g}\binom{j}{h}c_{i,j-l}\alpha^{u(i-g)}\beta^{v(j-h)} \\
&= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\binom{i}{g}\left(\sum_{k=0}^{l}\binom{l}{k}\binom{j-l}{h-k}\right)c_{i,j-l}\alpha^{u(i-g)}\beta^{v(j-h)}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{k=0}^{l}\binom{l}{k}\left(\sum_{i=0}^{m-1}\sum_{r=0}^{n-1}\binom{i}{g}\binom{r}{h-k}c_{i,r}\alpha^{u(i-g)}\beta^{v(r+l-h)}\right)\\
&= \sum_{k=0}^{l}\binom{l}{k}\left(\sum_{i=0}^{m-1}\sum_{r=0}^{n-1}\binom{i}{g}\binom{r}{h-k}c_{i,r}\alpha^{u(i-g)}\beta^{v(r-(h-k))}\right)\beta^{v(l-k)}\\
&= \sum_{k=0}^{l}\binom{l}{k}\beta^{v(l-k)}\hat{c}_{(g,h-k),(u,v)},
\end{aligned}$$

showing that the translation property holds.

Finally, let $\mathbf{w} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{l-i,j}x^iy^j$. Then

$$\begin{aligned}
\hat{w}_{(g,h),(u,v)} &= \sum_{i,j}\binom{i}{g}\binom{j}{h}c_{l-i,j}\alpha^{u(i-g)}\beta^{v(j-h)}\\
&= \sum_{i,j}\binom{j}{h}(\sum_{k=0}^{l}\binom{l}{k}\binom{i-l}{g-k})c_{l-i,j}\alpha^{u(i-g)}\beta^{v(j-h)}\\
&= \sum_{k=0}^{l}\binom{l}{k}\sum_{i,j}\binom{i-l}{g-k}\binom{j}{h}c_{l-i,j}\alpha^{u(i-g)}\beta^{v(j-h)}\\
&= \sum_{k=0}^{l}\binom{l}{k}\sum_{s,j}\binom{-s}{g-k}\binom{j}{h}c_{s,j}\alpha^{u(l-s-g)}\beta^{v(j-h)}\\
&= \sum_{k=0}^{l}\binom{l}{k}\sum_{s,j}(-1)^{g-k}\binom{s+g-k-1}{g-k}\binom{j}{h}c_{s,j}\alpha^{u(l-s-g)}\beta^{v(j-h)}\\
&= \sum_{k=0}^{l}(-1)^{g-k}\binom{l}{k}\sum_{t,j}\binom{t}{g-k}\binom{j}{h}c_{t-g+k+1,j}\alpha^{u(l-t-k-1)}\beta^{v(j-h)}\\
&= \sum_{k=0}^{l}(-1)^{g-k}\binom{l}{k}\alpha^{u(l-g-1)}\sum_{t,j}\binom{t}{g-k}\binom{j}{h}c_{t-g+k+1,j}\alpha^{-u(t-g+k)}\beta^{v(j-h)}\\
&= \sum_{k=0}^{l}(-1)^{g-k}\binom{l}{k}\alpha^{u(l-g-1)}\sum_{r=0}^{g-k-1}\binom{g-k-1}{r}\alpha^{-u(g-k-1-r)}\hat{c}_{(g-k-r,h),(-u,v)}\\
&= \sum_{k=0}^{l}\sum_{r=0}^{g-k-1}(-1)^{g-k}\binom{l}{k}\binom{g-k-1}{r}\alpha^{u(-2g+l+k)+r}\hat{c}_{(g-k-r,h),(-u,v)},
\end{aligned}$$

which proves (5). □

Corollary 3.3 *If* $\mathbf{c} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j}x^iy^j \leftrightarrow \hat{\mathbf{c}} = [\hat{c}_{(g,h),(u,v)}]$ *is a 2D-GDFT pair, then, for any* $l,k \geq 0$*, the following is a 2D-GDFT pair:*

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i-l,j-k}x^i y^j \leftrightarrow [\sum_{r=0}^{l}\sum_{s=0}^{k}\binom{l}{r}\binom{k}{s}\alpha^{u(l-r)}\beta^{v(k-s)}\hat{c}_{(g-r,h-s),(u,v)}].$$

Let $A=[a_{ij}]$ and $B=[b_{ij}]$ be $m\times n$-matrices over F_q. The convolution product $A\star B$ is defined as an $m\times n$-matrix C whose

$$C_{i,j}=\sum_{l=0}^{m-1}\sum_{k=0}^{n-1}A_{i-l,j-k}B_{lk},$$

where the indices are calculated modulo appropriate $t\in\{m,n\}$. The following theorem describes what the 2D-GDFT will do with the convolution product.

Theorem 3.4 *If $\mathbf{c}\leftrightarrow\hat{\mathbf{c}}$ and $\mathbf{d}\leftrightarrow\hat{\mathbf{d}}$ are 2D-GDFT pairs, then $\mathbf{e}=\mathbf{c}\star\mathbf{d}\leftrightarrow\hat{\mathbf{e}}$ is a 2D-GDFT pair, where for each $0\le g\le p^a-1$, $0\le h\le p^b-1$, $0\le u\le m'-1$, and $0\le v\le n'-1$,*

$$\hat{e}_{(g,h),(u,v)}=\sum_{r=0}^{g}\sum_{s=0}^{h}\hat{c}_{(g-r,h-s),(u,v)}\hat{d}_{(r,s),(u,v)}.$$

Proof By definition, we have

$$\begin{aligned}
\hat{e}_{(g,h),(u,v)} &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\binom{i}{g}\binom{j}{h}e_{i,j}\alpha^{u(i-g)}\beta^{v(j-h)}\\
&= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\binom{i}{g}\binom{j}{h}\left(\sum_{l=0}^{m-1}\sum_{k=0}^{n-1}c_{i-l,j-k}d_{l,k}\right)\alpha^{u(i-g)}\beta^{v(j-h)}\\
&= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\sum_{l=0}^{m-1}\sum_{k=0}^{n-1}\binom{i}{g}\binom{j}{h}c_{i-l,j-k}d_{l,k}\alpha^{u(i-g)}\beta^{v(j-h)}\\
&= \sum_{i,j,l,k}\left(\sum_{r=0}^{g}\binom{l}{r}\binom{i-l}{g-r}\right)\left(\sum_{s=0}^{h}\binom{k}{s}\binom{j-k}{h-s}\right)c_{i-l,j-k}d_{l,k}\alpha^{u(i-g)}\beta^{v(j-h)}
\end{aligned}$$

$$=\sum_{l,k}\sum_{r,s}\binom{l}{r}\binom{k}{s}\left(\sum_{i,j}\binom{i-l}{g-r}\binom{j-k}{h-s}c_{i-l,j-k}\alpha^{u(i-l-g+r)}\beta^{v(j-k+s-h)}\right)d_{l,k}\alpha^{u(l-r)}\beta^{v(k-s)}$$

$$\begin{aligned}
&= \sum_{l=0}^{m-1}\sum_{r=0}^{g}\sum_{k=0}^{n-1}\sum_{s=0}^{h}\binom{l}{r}\binom{k}{s}\hat{c}_{(g-r,h-s),(u,v)}d_{l,k}\alpha^{u(l-r)}\beta^{v(k-s)}\\
&= \sum_{r=0}^{g}\sum_{s=0}^{h}\hat{c}_{(g-r,h-s),(u,v)}\hat{d}_{(r,s),(u,v)},
\end{aligned}$$

as we claimed. □

4. 2D-GDFT is invertible

In this section, we are going to describe the inverse 2D-GDFT clearly. For each $0 \leq i \leq p^a-1$ and $0 \leq g \leq p^b-1$, let

$$\mathbf{c}_{(i,g)}(x,y) = \sum_{r=0}^{m'-1}\sum_{s=0}^{n'-1} c_{i+rp^a,g+sp^b}X^rY^s.$$

Let $\lambda = \alpha^{p^a}$ and $\mu = \beta^{p^b}$, so that λ and μ are again m'th and n'th roots of unity, respectively. By the classical two-dimensional DFT (with λ and μ as the chosen m'th and n'th roots of unity), we have

$$c_{i+rp^a,g+sp^b} = \frac{1}{m'n'}\sum_{u=0}^{m'-1}\sum_{v=0}^{n'-1}\mathbf{c}_{(i,g)}(\lambda^u,\mu^v)(\lambda^{-r})^u(\mu^{-s})^v.$$

Definition 4.1 *The partial Hasse matrix $H(X,Y)$ is the $p^{a+b}\times p^{a+b}$-matrix whose rows and columns are indexed (and ordered lexicographically) by all pairs (r,s), $0 \leq r \leq p^a-1$ and $0 \leq s \leq p^b-1$, and the $(i,g),(j,h)$th entry is $\binom{j}{i}\binom{h}{g}X^{j-i}Y^{h-g}$ (this is the (i,g)th partial Hasse derivative of the monomial X^jY^h in $F_q[X,Y]$).*

By definition, we have

$$\begin{aligned}\Bigg(H(X,Y)H(-X,-Y)\Bigg)_{(i,g),(j,h)} &= \sum_{k=0}^{p^a-1}\sum_{l=0}^{p^b-1}\binom{k}{i}\binom{l}{g}X^{k-i}Y^{l-g}\binom{j}{k}\binom{h}{l}(-X)^{j-k}(-Y)^{h-l}\\ &= X^{j-i}Y^{h-g}(\sum_k\binom{k}{i}\binom{j}{k}(-1)^{j-k})(\sum_l\binom{l}{g}\binom{h}{l}(-1)^{h-l})\end{aligned}$$

$$= \binom{j}{i}\binom{h}{g}X^{j-i}Y^{h-g}(\sum_k(-1)^{j-k}\binom{j-i}{j-k})(\sum_l(-1)^{h-l}\binom{h-g}{h-l}).$$

Now, from the binomial expansion

$$(1-1)^w = \sum_{u\leq v}\binom{w}{u}(-1)^u = 0,$$

applied to the off-diagonal terms in the product $H(X,Y)H(-X,-Y)$, we see that the inverse of the partial Hasse matrix $H(X,Y)$ is $H(-X,-Y)$.

Before going on, we need the following simple lemma.

Lemma 4.2 *Let $q = p^m$ be a prime power and F_q be a field of order q. For each $i,a,b,c \geq 0$ we have*

$$\binom{a}{i} = \binom{a+bp^c}{i},$$

where $\binom{a}{i}$ and $\binom{a+bp^c}{i}$ are interpreted as integers of the field F_q.

Proof Just note that the field F_q has characteristics p. Hence, $a + bp^c$ equals a when all the quantities involved are integers. Thus, the result is obvious. □

Using the previous lemma, we can write

$$\begin{aligned}
\sum_{j,h} \binom{j}{i}\binom{h}{g} \alpha^{u(j-i)} \beta^{v(h-g)} \mathbf{c}_{(j,h)}(\lambda^u, \mu^v) &= \sum_{j,h}\sum_{r,s} \binom{j}{i}\binom{h}{g} c_{j+rp^a, h+sp^b} \alpha^{u(j+rp^a-i)} \beta^{v(h+sp^b-g)} \\
&= \sum_{h,s} \left(\sum_{j,r} \binom{j+rp^a}{i} c_{j+rp^a, h+sp^b} \alpha^{u(j+rp^a-i)} \right) \binom{h}{g} \beta^{v(h+sp^b-g)} \\
&= \sum_{h,s} \left(\sum_{k=0}^{m-1} \binom{k}{i} c_{k, h+sp^b} \alpha^{u(k-i)} \right) \binom{h}{g} \beta^{v(h+sp^b-g)} \\
&= \sum_{k=0}^{m-1} \binom{k}{i} \alpha^{u(k-i)} \left(\sum_{h,s} \binom{h+sp^b}{g} c_{k,h+sp^b} \beta^{v(h+sp^b-g)} \right) \\
&= \sum_{k=0}^{m-1} \binom{k}{i} \alpha^{u(k-i)} \left(\sum_{l=0}^{n-1} \binom{l}{g} c_{k,l} \beta^{v(l-g)} \right) \\
&= \sum_{k=0}^{m-1}\sum_{l=0}^{n-1} \binom{k}{i}\binom{l}{g} c_{k,l} \alpha^{u(k-i)} \beta^{v(l-g)} \\
&= \hat{c}_{(i,g),(u,v)}.
\end{aligned}$$

Hence, we have

$$H(\alpha^u, \beta^v) \begin{bmatrix} \mathbf{c}_{(0,0)}(\lambda^u, \mu^v) \\ \mathbf{c}_{(0,1)}(\lambda^u, \mu^v) \\ \vdots \\ \mathbf{c}_{(0,p^b-1)}(\lambda^u, \mu^v) \\ \mathbf{c}_{(1,0)}(\lambda^u, \mu^v) \\ \mathbf{c}_{(1,1)}(\lambda^u, \mu^v) \\ \vdots \\ \mathbf{c}_{(1,p^b-1)}(\lambda^u, \mu^v) \\ \vdots \\ \mathbf{c}_{(p^a-1,0)}(\lambda^u, \mu^v) \\ \mathbf{c}_{(p^a-1,1)}(\lambda^u, \mu^v) \\ \vdots \\ \mathbf{c}_{(p^a-1,p^b-1)}(\lambda^u, \mu^v) \end{bmatrix} = \begin{bmatrix} \hat{c}_{(0,0),(u,v)} \\ \hat{c}_{(0,1),(u,v)} \\ \vdots \\ \hat{c}_{(0,p^b-1),(u,v)} \\ \hat{c}_{(1,0),(u,v)} \\ \vdots \\ \hat{c}_{(1,p^b-1),(u,v)} \\ \vdots \\ \hat{c}_{(p^a-1,0),(u,v)} \\ \hat{c}_{(p^a-1,1),(u,v)} \\ \vdots \\ \hat{c}_{(p^a-1,p^b-1),(u,v)} \end{bmatrix}.$$

Since the partial Hasse matrix is invertible, the above equality can be rewritten as

$$\begin{bmatrix} \mathbf{c}_{(0,0)}(\lambda^u,\mu^v) \\ \mathbf{c}_{(0,1)}(\lambda^u,\mu^v) \\ \vdots \\ \mathbf{c}_{(0,p^b-1)}(\lambda^u,\mu^v) \\ \mathbf{c}_{(1,0)}(\lambda^u,\mu^v) \\ \mathbf{c}_{(1,1)}(\lambda^u,\mu^v) \\ \vdots \\ \mathbf{c}_{(1,p^b-1)}(\lambda^u,\mu^v) \\ \vdots \\ \mathbf{c}_{(p^a-1,0)}(\lambda^u,\mu^v) \\ \mathbf{c}_{(p^a-1,1)}(\lambda^u,\mu^v) \\ \vdots \\ \mathbf{c}_{(p^a-1,p^b-1)}(\lambda^u,\mu^v) \end{bmatrix} = H(-\alpha^u,-\beta^v) \begin{bmatrix} \hat{c}_{(0,0),(u,v)} \\ \hat{c}_{(0,1),(u,v)} \\ \vdots \\ \hat{c}_{(0,p^b-1),(u,v)} \\ \hat{c}_{(1,0),(u,v)} \\ \vdots \\ \hat{c}_{(1,p^b-1),(u,v)} \\ \vdots \\ \hat{c}_{(p^a-1,0),(u,v)} \\ \hat{c}_{(p^a-1,1),(u,v)} \\ \vdots \\ \hat{c}_{(p^a-1,p^b-1),(u,v)} \end{bmatrix}.$$

Consequently,

$$c_{i+rp^a,g+sp^b} = \frac{1}{m'n'} \sum_{u=0}^{m'-1} \sum_{v=0}^{n'-1} \left(\sum_{j=0}^{p^a-1} \sum_{h=0}^{p^b-1} \binom{j}{i} \binom{h}{g} (-\alpha^u)^{j-i} (-\beta^v)^{h-g} \hat{c}_{(j,h),(u,v)} \right) (\lambda^{-r})^u (\mu^{-s})^v.$$

Therefore, the 2D-GDFT is invertible.

5. A family of quasi-cyclic codes

Reed–Solomon codes (RS codes) are a class of error-correcting cyclic codes proposed by Reed and Solomon in their original paper [10]. RS codes have optimal parameters and can be efficiently decoded [7,11,13].

Considering a vector space of polynomials f such that $f(m)=0$ for all m in the set $B=\{\alpha^{r_0},\alpha^{r_0+1},\cdots,\alpha^{r_0+n-k-1}\}$, we can define an RS code of length n and dimension k over the finite field F_q. Here α can be any element in F_q of multiplicative order at least n where n is a divisor of $q-1$. The key point here is that we can construct the RS codes from another fruitful method, the DFT approach ([2], Section 6), which enables us to introduce our generalization of such codes.

Definition 5.1 *Let $d \geq 2$, $m=p^a m'$, and $n=p^b n'$, where $a,b \geq 0$ are integers and m',n' are relatively prime to p. Consider the subspace $C^\star$ consisting of all matrices $\mathbf{c} \in (F_q)^{m\times n}$ whose $\hat{c}_{(g,h),(u,v)}=0$ for all pairs (g,h) and (u,v) in which $0 \leq v \leq n'-2$. A generalized RS code C of block length mn over F_q, denoted $GRS_{m,n,d}$, will be defined as the set of all words $\mathbf{c} \in C^\star$ whose $\hat{c}_{(g,h),(u,n'-1)}=0$ for all pairs (g,h) and all pairs $(u,n'-1)$ in which u belongs to a specified block of $d-1$ consecutive integers, denoted $\{z_0,z_0+1,...,z_0+d-2\}$, i.e. $0 \leq z_0 \leq u \leq z_0+d-2 \leq m'-1$.*

Note that, by definition, we obtain a code whose elements are matrices, which can be viewed as vectors of length mn, by reading them column by column. It is easy to verify that $\mathrm{GRS}_{m,n,d}$ is an $[mn, p^{a+b}(m'-d+1)]$-linear code.

In the following, $\mathfrak{B}_{z_0,d}$ stands for the set

$$\{(u,n'-1) \mid z_0 \leq u \leq z_0+d-2\} \cup \{(u,v) \mid 0 \leq u \leq m'-1\ ,\ 0 \leq v \leq n'-2\}$$

and will be called the defining set of the code $\mathrm{GRS}_{m,n,d}$.

Proposition 5.2 *The code $GRS_{m,n,d}$ is a quasi-cyclic code of index m.*

Proof Suppose that $\mathbf{c} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j}x^i y^j$ is a word of $\mathrm{GRS}_{m,n,d}$. Hence, $\hat{c}_{(g,h),(u,v)} = 0$ for all pairs (g,h) and for each pair $(u,v) \in \mathfrak{B}_d$. Thus,

$$\sum_{k=0}^{n-1}\binom{n-1}{k}\beta^{v(n-1-k)}\hat{c}_{(g,h-k),(u,v)} = 0$$

for all pairs (g,h) and for each pair $(u,v) \in \mathfrak{B}_d$. Therefore, by proposition 3.2(3), the 2D-GDFT of the word $\mathbf{c}' = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j-1}x^i y^j$ is equal to zero in those columns (u,v) in which $(u,v) \in \mathfrak{B}_d$, proving that $\mathbf{c}'$ is a word of $\mathrm{GRS}_{m,n,d}$, as desired. □

Next, the minimum distance of the code $\mathrm{GRS}_{m,n,d}$ is going to be discussed.

Proposition 5.3 *The minimum distance of the code $GRS_{m,n,d}$ satisfies*

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

Proof Without loss of generality, we can suppose $z_0 = m' - d + 1$. Otherwise, use proposition 3.2(1) to translate the defining set $\mathfrak{B}_{z_0,d}$ to $\mathfrak{B}_{m'-d+1,d}$, thereby multiplying each codeword component by a power of α, which does not change the weight of a codeword because components that were nonzero remain nonzero. Suppose that $\mathbf{c} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j}x^i y^j$ is a nonzero word of $\mathrm{GRS}_{m,n,d}$. For any $0 \leq i \leq p^a - 1$ and $0 \leq g \leq p^b - 1$, let

$$C_{(i,g)}(x) = \sum_{u=0}^{m'-1} \mathbf{c}_{(i,g)}(\lambda^u, \mu^{n'-1})x^u,$$

where $\mathbf{c}_{(i,g)}$, λ, and μ are defined as in Section 4. Recall that

$$\mathbf{c}_{(i,g)}(\lambda^u, \mu^v) = \sum_{k=0}^{p^a-1}\sum_{l=0}^{p^b-1}\binom{k}{i}\binom{l}{g}(-\alpha^u)^{k-i}(-\beta^v)^{l-g}\hat{c}_{(k,l),(u,v)}.$$

On the other hand, $\hat{c}_{(k,l),(u,v)} = 0$ for all $0 \leq k \leq p^a - 1$, $0 \leq l \leq p^b - 1$, and $(u,v) \in \mathfrak{B}_{m'-d+1,d}$, showing that $\mathbf{c}_{(i,g)}(\lambda^u, \mu^v) = 0$ for each pair $(u,v) \in \mathfrak{B}_{m'-d+1,d}$. Therefore, the polynomial $C_{(i,g)}(x)$ is either zero or has degree at most $m' - d$. Since $\mathbf{c} \neq 0$, we can find a nonzero polynomial $C_{(i,g)}(x)$ for some $0 \leq i \leq p^a - 1$ and $0 \leq g \leq p^b - 1$. Some of the components of the codeword $\mathbf{c}$ are $c_{i+rp^a, g+sp^b} = \frac{(\mu^{-s})^{n'-1}}{m'n'}C_{(i,g)}(\lambda^{-r})$, $r = 0, \cdots, m' - 1$, and $s = 0, \cdots, n' - 1$. Since $C_{(i,g)}(x)$ is a polynomial of degree at most $m' - d$, it can have at most $m' - d$ zeros. Hence, for any $0 \leq s \leq n' - 1$, there will be at least d index r such that $c_{i+rp^a, g+sp^b} \neq 0$. Consequently, $w(\mathbf{c}) \geq td$ where t is the number of those pairs (i,g) whose $C_{(i,g)}(x) \neq 0$. Thus, $d_{\min}(\mathrm{GRS}_{m,n,d}) \geq m'n' - (m' - d)n' = n'd$. The right side of the inequality will be obtained from the Singleton bound for linear codes. This completes the proof. □

Example 5.4 *Let $q = 4$, $m = 6$, and $n = 5$. Choosing α^5 and α^3 as the fifth and third roots of unity in the Galois field $F_4 = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in F_2,\ \alpha^4 = \alpha + 1\}$, the 2D-GDFT of a bivariate polynomial $\mathbf{c} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{i,j}x^iy^j$ is given by the matrix $\hat{\mathbf{c}}$ whose*

$$\begin{aligned}\hat{c}_{(g,h),(u,v)} &= \mathbf{c}^{[g,h]}(\alpha^{5u}, \alpha^{3v}) \\ &= \sum_{i=0}^{5}\sum_{j=0}^{4}\binom{i}{g}\binom{j}{h}c_{i,j}\alpha^{5u(i-g)+3v(j-h)}.\end{aligned}$$

Now, let $d = 1$. Then the code $GRS_{6,5,1}$ is a linear $[30, 9]$-quasi-cyclic code of minimum distance 16 (http://www.codetables.de). This shows that good quasi-cyclic codes can be constructed via our algebraic approach, as in [9], where such codes have been constructed using integer linear programming and a heuristic combinatorial optimization algorithm based on a greedy local search.

6. Conclusion

We generalized and studied the 2D-GDFT, which enables us to apply the powerful concept of 2D-DFT on data matrices for which the number of rows or columns is not necessarily coprime with the field characteristic. Our generalized 2D-DFT enjoys the basic properties of the original one. As an application, we introduced a family of quasi-cyclic linear codes, denoted by $\mathrm{GRS}_{m,n,d}$, which are a natural generalization of the classical Reed–Solomon codes, and the code parameters were described.

References

[1] Arazi B. Two-dimensional digital processing of one-dimensional signal. IEEE T Acoust Speech 1974; 22: 31-36.

[2] Blahut RE. Algebraic Codes for Data Transmission. New York, NY, USA: Cambridge University Press, 2003.

[3] Bongiovanni G, Corsini P, Frosini G. One-dimensional and two-dimensional generalized discrete Fourier transforms. IEEE T Acoust Speech 1974; 24: 97-99.

[4] Brenner NM. Fast Fourier transform of externally stored data. IEEE T Acoust Speech 1963; 17: 128-132.

[5] Buijs HL. Fast Fourier transformation of large arrays of data. Appl Optimizat 1963; 8: 211-212.

[6] Corsini P, Frosini G. Properties of the multidimensional generalized discrete Fourier transform. IEEE T Comput 1979; C-28: 819-830.

[7] Gao S. A new algorithm for decoding Reed-Solomon codes. In: Bhargava VK, Poor HV, Tarokh V, Yoon S, editors. Communications, Information and Network Security. The Springer International Series in Engineering and Computer Science (Communications and Information Theory), Vol. 712. Boston, MA, USA: Springer, pp. 55-68.

[8] Gulliver TA, Bhargava VK. New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes. Design Code Cryptogr 1996; 7: 223-233.

[9] Massey JL, Serconek S. Linear complexity of periodic sequences: a general theory. Lect Notes Comput Sc 1996; 1109: 358-371.

[10] Reed IS, Solomon G. Polynomial codes over certain finite fields. Siam J Appl Math 1960; 8: 300-304.

[11] Sarwate D, Shanbhag N. High-speed architectures for Reed-Solomon decoders. IEEE T VLSI Syst 2001; 9: 641-655.

[12] Singleton RC. A method for computing the fast Fourier transform with auxiliary memory and limited high-speed storage. IEEE T Acoust Speech 1967; 16: 91-98.

[13] Wicker SB, Bhargava VK. Reed-Solomon Codes and Their Applications. New York, NY, USA: IEEE Press, 1994.