Information Processing Letters 115 (2015) 779–785

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

On commutativity of Discrete Fourier Transform

Mrinal Nandi

Department of Statistics, West Bengal State University, Barasat, West Bengal, India

ARTICLE INFO

Article history:
Received 4 July 2013
Received in revised form 2 April 2015
Accepted 9 April 2015
Available online 14 May 2015
Communicated by Ł. Kowalik

Keywords:
DFT matrix
Theory of computation
Commutativity of matrices

ABSTRACT

In this paper we have studied the commutative properties of general Discrete Fourier Transform (DFT) matrices U_n. The problem is to characterize matrices A_n that commute with U_n. We find complete solutions for A_n up to $n = 5$ theoretically. We also provide a major result towards the complete solutions for general n. To find A_n which commutes with U_n one needs to solve a system of n^2 linear equations of n^2 variables. We reduced this problem into solving two different systems of linear equations of more or less $n^2/4$ many variables and same number of equations. To do this reduction we use the idea of symmetric, skew symmetric matrices as well as we consider the set of matrices as a vector space and use direct sum of subspaces.

1. Introduction

The Discrete Fourier Transform (DFT) is one of the most important discrete transform, used to perform Fourier analysis in many practical applications. In digital signal processing, the function is any quantity or signal that varies over time, such as the pressure of a sound wave, a radio signal, or daily temperature readings, sampled over a finite time interval (often defined by a window function). In image processing, the samples can be the values of pixels along a row or column of a raster image. The DFT is also used to solve partial differential equations, and to perform other operations such as convolutions or multiplying large integers.

Quantum Fourier Transform (QFT) is the quantum analogue of the Discrete Fourier Transform (DFT). QFT has applications in quantum computation and information, see [3,4] for a detailed discussion in this area. The QFT can be seen as a linear transformation on quantum bits. Fourier transformation has applications in quantum phase estimation and hidden subgroup problem. QFT also performs efficiently on quantum computational framework. Shor's famous algorithm [9] for polynomial time factoring and discrete logarithm are based on Fourier transform, which is a generalization of the Hadamard transform in higher dimension. One important quantum gate in communication science is the Hadamard gate [3,4].

One cannot design a universal Hadamard gate for an arbitrary unknown quantum bit (qubit) because linearity does not allow linear superposition of an unknown state $|\psi\rangle$ with its orthogonal complement $|\psi'\rangle$ [8]. Maitra and Parashar have shown how one can construct a certain class of qubit states, for which the Hadamard gate works as it is [6]. Maitra and Sarkar identified that the result in [6] is not a complete characterization of such qubits and they do more work on that [5].

The qubits can be represented as the superposition of $|0\rangle$ and $|1\rangle$ in the form $|\psi\rangle = a|0\rangle + b|0\rangle$, where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$. The qubits of higher dimensions are called qudits. An n-dimensional qudit can be represented as $|\psi_t\rangle = a_{t,0}|0\rangle + a_{t,1}|1\rangle + \cdots + a_{t,n-1}|n-1\rangle$, where $a_{t,0}, a_{t,1}, \ldots, a_{t,n-1}$ are all complex numbers and $\sum_{j=0}^{n-1} |a_{t,j}|^2 = 1$.

The Discrete Fourier Transform is described as transforming a set $x_0, \ldots, x_{n-1}$ of n complex numbers into a set of complex numbers $y_0, \ldots, y_{n-1}$ defined by $y_j = U_n(x_j) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{\frac{2\pi ijk}{n}} x_k$. The Quantum Fourier Trans-

E-mail address: mrinal.nandi1@gmail.com.

http://dx.doi.org/10.1016/j.ipl.2015.04.011
0020-0190/

form (QFT) is the counterpart of this transformation and is defined as follows.

$$U_n(|j\rangle) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{\frac{2\pi ijk}{n}} |k\rangle. \quad (1)$$

The DFT/QFT matrix can be expressed in terms of an $n \times n$ matrix U_n defined as follows,

$$U_n = \frac{1}{\sqrt{n}}((\omega_n^{i\cdot j}))_{i,j=0,1,2,\ldots,n-1} = \begin{bmatrix} \omega_n^{0\cdot 0} & \omega_n^{0\cdot 1} & \ldots & \omega_n^{0\cdot(n-1)} \\ \omega_n^{1\cdot 0} & \omega_n^{1\cdot 1} & \ldots & \omega_n^{1\cdot(n-1)} \\ \ldots & \ldots & \ldots & \ldots \\ \omega_n^{(n-1)\cdot 0} & \omega_n^{(n-1)\cdot 1} & \ldots & \omega_n^{(n-1)\cdot(n-1)} \end{bmatrix},$$

where $\omega_n = e^{\frac{2\pi i}{n}}$.

Thus DFT/QFT is a unitary transformation expressed by the unitary matrix U_n. Given a set of qudits $\psi_0, \psi_1, \ldots, \psi_{n-1}$, after application of QFT, one can get another set of qudits $\psi'_0, \psi'_1, \ldots, \psi'_{n-1}$. From the Plancherel theorem [10] it is known that the dot product of two vectors is preserved under a unitary DFT/QFT transformation. Thus if ψ_u and ψ_v are orthogonal then ψ'_u and ψ'_v will be orthogonal too.

One application of such states is available other than the much used computational bases, less restriction can be provided on the sources producing qubits, qutrits or qudits in general. As an example, one can look at the traditional BB84 protocol [1]. A variant of the BB84 protocol with three-dimensional quantum states or qutrits has been studied in [2] for further security against symmetric attacks. All the applications are in two or three dimensions. If we want to generalized these applications to higher dimensions, we need following generalization:

Consider an n-dimensional qudit can be represented as $|\psi_t\rangle = a_{t,0}|0\rangle + a_{t,1}|1\rangle + a_{t,2}|2\rangle + \ldots + a_{t,n-1}|n-1\rangle$, where $a_{t,0}, a_{t,1}, a_{t,2}, \ldots, a_{t,n-1}$ are all complex numbers and $\sum_{j=0}^{n-1} |a_{t,j}|^2 = 1$. We want to characterize the qudits $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle$ such that

$$U_n(|\psi_j\rangle) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{\frac{2\pi ijk}{n}} |\psi_k\rangle. \quad (2)$$

This is true when $|\psi_0\rangle = |0\rangle$, $|\psi_1\rangle = |1\rangle, \ldots, |\psi_{n-1}\rangle = |n-1\rangle$. However, it is not true in general. Thus, it is an important theoretical question to characterize such ensembles as those states can be applied in a similar manner as the standard basis and can be used in the same quantum gates that are already available.

Looking at U_n as a matrix as we have described above, the problem can be seen as characterizing

$$A_n = \begin{bmatrix} a_{0,0} & a_{1,0} & \ldots & a_{n-1,0} \\ a_{0,1} & a_{1,1} & \ldots & a_{n-1,1} \\ \ldots & \ldots & \ldots & \ldots \\ a_{0,n-1} & a_{1,n-1} & \ldots & a_{n-1,n-1} \end{bmatrix},$$

such that $U_nA_n = A_nU_n$ [6]. To the best of our knowledge, any reference for complete characterization is not available. In this paper we give some characterization of A_n. In this paper we consider only the commutativity part. For $n = 2$, problem is very easy and can solved by easy calculations, see [5]. In [5] authors give complete characterization up to $n = 3$ and 4, but they use computer software [7] to solve the required system of linear equations. In this paper we complete characterization up to $n = 5$ theoretically. We also provide a major result for matrices A_n for all values of n. Throughout the paper the matrices U_n and A_n denote the above matrices.

2. Characterization of the matrices A_n

In this section we first state some well known results on the unitary DFT matrices U_n, then we discuss our contribution to characterize the matrices which commute with unitary DFT matrices U_n. Now and onward we say $i-1$-th row instead of i-th row, e.g., consider the first row of U_n, i.e., $(1 \quad 1 \quad \ldots \quad 1)$, we call this row as 0-th row. Also by means of n-th row we mean 0-th row. Similar notations are applicable for columns also.

Note that there are n^2 variables and n^2 equations in $U_nA_n = A_nU_n$. For $i, j = 0, 1, \ldots, n-1$ we call the variables in A_n as a_{ij} and the equation determine by the equality of (i, j)-th elements of U_nA_n and (i, j)-th elements of A_nU_n as $E_{i,j}$. Throughout the paper if any suffix is n then it will be considered as 0, e.g. a_{nn} should be considered as a_{00}. In this paper our aim is to reduce the number of variables as well as the number of equations, using relations between the variables. It would also be helpful if we could identify some free variables, which are not involved in any of the equations (which have to be solved).

We need some well known results on unitary DFT matrices U_n, which can be easily verified, to characterize A_n. The results are as follows:

Result 1. *If* $U_n = ((\omega_n^{(i-1)\cdot(j-1)})) = ((u_{ij}))$ *then* $U_n^* = U_n^3 = U_n^{-1} = ((u_{ij}^{-1})) = ((\omega_n^{-(i-1)\cdot(j-1)}))$ *and*

$$U_n^2 = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}$$

Next we state our contribution for characterization of A_n. We prove some theoretical results on A_n when it commutes with U_n. We observed that U_n^2 has a nice form, also when A_n commutes with U_n it should commute with U_n^2. In the following results A_n is fully characterized when it commutes with U_n^2, and this condition is a necessary condition for A_n when it commutes with U_n. This theorem reduced almost half of the variables and the same number of equations.

Theorem 1. *If* $A_n = ((a_{ij}))_{i,j=0(1)n-1}$ *then* $U_n^2A_n = A_nU_n^2$ *if and only if* $a_{ij} = a_{n-i,n-j}$, *for all* $i, j = 0, 1, \ldots, n-1$.
Hence if $U_nA_n = A_nU_n$ *then* $a_{ij} = a_{n-i,n-j}$, *for all* $i, j = 0, 1, \ldots, n-1$.