The inverse cyclotomic Discrete Fourier Transform algorithm

Sergei V. Fedorenko[1]

***Abstract*—The proof of the theorem concerning to the inverse cyclotomic Discrete Fourier Transform algorithm over finite field is provided.**

I. INTRODUCTION

The discrete Fourier transform (DFT) can be applied in error correcting codes and code-based cryptography. The cyclotomic DFT method [1], [2] is the best one for computing the DFT over finite field. Alexey Maevskiy pointed that formula [2, (6)] in the example of paper [2] had not been proved. We have corrected this mistake and introduced the proof.

II. BASIC NOTIONS AND DEFINITIONS

The DFT of length $n \mid 2^m - 1$ of a vector $f = (f_i), \quad i \in [0, n-1]$, $f_i \in GF(2^m)$, is the vector $F = (F_j)$

$$F_j = \sum_{i=0}^{n-1} f_i \alpha^{ij}, \quad j \in [0, n-1],$$

where α is an element of order n in $GF(2^m)$. Let us write the DFT in matrix form

$$F = Wf, \tag{1}$$

where $W = (\alpha^{ij}), \quad i, j \in [0, n-1]$, is a Vandermonde matrix. We assume that the length of the n-point Fourier transform over $GF(2^m)$ is $n = 2^m - 1$.

Let us consider cyclotomic cosets modulo $n = 2^m - 1$ over $GF(2)$

$$\begin{aligned} \{c_0\} &= \{0\} \\ \{c_1, c_1 2, c_1 2^2, \ldots, c_1 2^{m_1 - 1}\}&, \\ &\ldots, \\ \{c_l, c_l 2, c_l 2^2, \ldots, c_l 2^{m_l - 1}\}&, \end{aligned}$$

where $c_k \equiv c_k 2^{m_k} \bmod n$, $l+1$ is the number of cyclotomic cosets modulo n over $GF(2)$.

Let us introduce the set of indices modulo n

$$\begin{aligned} Z = (Z_i) = (c_0, c_1, c_1 2, c_1 2^2, \ldots, c_1 2^{m_1 - 1}, \ldots, \\ c_l, c_l 2, c_l 2^2, \ldots, c_l 2^{m_l - 1}), \quad i \in [0, n-1]. \end{aligned}$$

Then, we define a permutation matrix $\Pi = (\Pi_{i,j}), \quad i, j \in [0, n-1]$,

$$\Pi_{i,j} = \begin{cases} 1, & \text{if } j = Z_i, \quad i \in [0, n-1] \\ 0, & \text{otherwise.} \end{cases}$$

*The reported study was funded by RFBR according to the research project No. 16-01-00716 a.

[1]Sergei V. Fedorenko is with National Research University Higher School of Economics, Russian Federation `sfedorenko@hse.ru`

Let us denote a basis $\beta_k = (\beta_{k,0}, \ldots, \beta_{k,m_k-1})$ of the subfield $GF(2^{m_k}) \subset GF(2^m)$.

Then we can write the cyclotomic DFT [1], [2]

$$F_j = \sum_{k=0}^{l} \sum_{s=0}^{m_k-1} a_{k,j,s} \left(\sum_{p=0}^{m_k-1} \beta_{k,s}^{2^p} f_{c_k 2^p} \right),$$

where $a_{k,j,s} \in GF(2)$.

This equation can be represented in matrix form as

$$F = AL(\Pi f), \tag{2}$$

where A is a matrix with elements $a_{k,j,s} \in GF(2)$ and L is a block diagonal matrix with elements $\beta_{k,s}^{2^p}$. If one chooses the normal basis β_k, then all the blocks of the matrix L are circulant matrices.

The inverse DFT in the field $GF(2^m)$ is

$$f = W^{-1} F.$$

It is easily shown that

$$W^{-1} = EW, \tag{3}$$

where E is a matrix

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdot & 0 & \cdot & 0 & 0 \\ 0 & 0 & 0 & \cdot & 0 & \cdot & 0 & 1 \\ 0 & 0 & 0 & \cdot & 0 & \cdot & 1 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & 1 & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & \cdot & 0 & \cdot & 0 & 0 \\ 0 & 1 & 0 & \cdot & 0 & \cdot & 0 & 0 \end{pmatrix}.$$

III. THE INVERSE CYCLOTOMIC DFT

Since both matrices A and L are invertible, from (2) the following representation of the inverse DFT can be derived

$$\Pi f = L^{-1} A^{-1} F.$$

Lemma 1 ([3]): Suppose β_k are the normal bases, then it is possible to show that blocks of L^{-1} consist of elements of bases β_k' which are dual to β_k, that is, the blocks of L^{-1} are also circulant matrices.

Theorem 1: The inverse cyclotomic DFT for $GF(2^m)$ is

$$(\Pi E)F = L^{-1} A^{-1} f.$$

Proof: From (1) and (2) we have

$$W = AL\Pi$$

and

$$W^{-1} = \Pi^{-1} L^{-1} A^{-1}.$$

From the last formula and (3) we obtain

$$W^{-1} = EW = \Pi^{-1} L^{-1} A^{-1}$$

and

$$W = E^{-1} \Pi^{-1} L^{-1} A^{-1}.$$

Hence,

$$F = Wf = (E^{-1}\Pi^{-1}) L^{-1} A^{-1} f.$$

and

$$(\Pi E) F = L^{-1} A^{-1} f.$$

IV. EXAMPLES

A. DFT of length $n = 7$

Let $(\gamma, \gamma^2, \gamma^4)$ be a normal basis of $GF(2^3)$, where $\gamma = \alpha^3$ and α is a root of the primitive polynomial $x^3 + x + 1$. Then the cyclotomic DFT can be represented as

$$F = \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \\ F_6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

$$\times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \gamma^1 & \gamma^2 & \gamma^4 & 0 & 0 & 0 \\ 0 & \gamma^2 & \gamma^4 & \gamma^1 & 0 & 0 & 0 \\ 0 & \gamma^4 & \gamma^1 & \gamma^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma^1 & \gamma^2 & \gamma^4 \\ 0 & 0 & 0 & 0 & \gamma^2 & \gamma^4 & \gamma^1 \\ 0 & 0 & 0 & 0 & \gamma^4 & \gamma^1 & \gamma^2 \end{pmatrix}$$

$$\times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \end{pmatrix} = AL\Pi f.$$

Using Theorem 1, we obtain the inverse cyclotomic DFT

$$(\Pi E)F$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\times \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \\ F_6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \gamma^1 & \gamma^2 & \gamma^4 & 0 & 0 & 0 \\ 0 & \gamma^2 & \gamma^4 & \gamma^1 & 0 & 0 & 0 \\ 0 & \gamma^4 & \gamma^1 & \gamma^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma^1 & \gamma^2 & \gamma^4 \\ 0 & 0 & 0 & 0 & \gamma^2 & \gamma^4 & \gamma^1 \\ 0 & 0 & 0 & 0 & \gamma^4 & \gamma^1 & \gamma^2 \end{pmatrix}$$

$$\times \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \end{pmatrix} = L^{-1} A^{-1} f.$$

■

Finally note that the last formula coincides with formula [2, (6)].

$$\begin{pmatrix} F_0 \\ F_6 \\ F_5 \\ F_3 \\ F_4 \\ F_1 \\ F_2 \end{pmatrix} = L^{-1} A^{-1} \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \end{pmatrix}.$$

This algorithm requires 6 multiplications and 24 additions and appears to be the best known 7-point DFT for $GF(2^3)$.

B. DFT of length $n = 15$

Let $(\alpha^3, \alpha^6, \alpha^{12}, \alpha^9)$ and $(\alpha^{11}, \alpha^7, \alpha^{14}, \alpha^{13})$ be the normal bases of $GF(2^3)$, where α is a root of the primitive polynomial $x^4 + x + 1$. Then the cyclotomic DFT can be represented as formula (4) or $F = AL(\Pi f)$. The inverse cyclotomic DFT can be written as formula (5) or $(\Pi E)F = L^{-1} A^{-1} f$.

ACKNOWLEDGMENT

The author would like to thank Alexey Maevskiy for pointing out a methodological mistake in the paper [2], and Peter Trifonov for helpful discussions.

REFERENCES

[1] P. V. Trifonov and S. V. Fedorenko. A method for fast computation of the Fourier transform over a finite field. *Problems of Information Transmission*, vol. 39, no. 3, pp. 231–238, 2003. Translation of *Problemy Peredachi Informatsii*.

[2] E. Costa, S. V. Fedorenko, and P. V. Trifonov. On computing the syndrome polynomial in Reed–Solomon decoder. *European Transactions on Telecommunications*, vol. 15, no. 3, pp. 337–342, 2004.

[3] J. Hong and M. Vetterli. Computing m DFT's over $GF(q)$ with one DFT over $GF(q^m)$. *IEEE Transactions on Information Theory*, vol. 39, no. 1, pp. 271–274, January 1993.

$$
\begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \\ F_6 \\ F_7 \\ F_9 \\ F_{10} \\ F_{11} \\ F_{12} \\ F_{13} \\ F_{14} \\ F_{15} \end{pmatrix}
=
\begin{pmatrix}
111111111111111 \\
110011000111010 \\
111000100011101 \\
110000001010011 \\
101100010101110 \\
101011111010101 \\
101001000001011 \\
111100100011010 \\
100110001110101 \\
100010010100011 \\
110101111101010 \\
111011000110001 \\
100100100000111 \\
110110001100110 \\
101110010001101
\end{pmatrix}
$$

$$
\times
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^5 & \alpha^{10} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{10} & \alpha^5
\end{pmatrix}
$$

$$
\times
\begin{pmatrix}
100000000000000 \\
010000000000000 \\
001000000000000 \\
000010000000000 \\
000000001000000 \\
000100000000000 \\
000000100000000 \\
000000000000100 \\
000000000100000 \\
000000010000000 \\
000000000000001 \\
000000000000010 \\
000000000001000 \\
000001000000000 \\
000000000010000
\end{pmatrix}
\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \\ f_9 \\ f_{10} \\ f_{11} \\ f_{12} \\ f_{13} \\ f_{14} \\ f_{15} \end{pmatrix}
\tag{4}
$$

$$
\begin{aligned}
&\begin{pmatrix}
100000000000000\\
010000000000000\\
001000000000000\\
000010000000000\\
000000001000000\\
000100000000000\\
000000100000000\\
000000000000100\\
000000000100000\\
000000010000000\\
000000000000001\\
000000000000010\\
000000000001000\\
000001000000000\\
000000000010000
\end{pmatrix}
\begin{pmatrix}
100000000000000\\
000000000000001\\
000000000000010\\
000000000000100\\
000000000001000\\
000000000010000\\
000000000100000\\
000000001000000\\
000000010000000\\
000000100000000\\
000001000000000\\
000010000000000\\
000100000000000\\
001000000000000\\
010000000000000
\end{pmatrix}
\begin{pmatrix}
F_0\\ F_1\\ F_2\\ F_3\\ F_4\\ F_5\\ F_6\\ F_7\\ F_9\\ F_{10}\\ F_{11}\\ F_{12}\\ F_{13}\\ F_{14}\\ F_{15}
\end{pmatrix}\\
&=\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & \alpha^{11} & \alpha^{7} & \alpha^{14} & \alpha^{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & \alpha^{7} & \alpha^{14} & \alpha^{13} & \alpha^{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & \alpha^{14} & \alpha^{13} & \alpha^{11} & \alpha^{7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & \alpha^{13} & \alpha^{11} & \alpha^{7} & \alpha^{14} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & \alpha^{11} & \alpha^{7} & \alpha^{14} & \alpha^{13} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & \alpha^{7} & \alpha^{14} & \alpha^{13} & \alpha^{11} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & \alpha^{14} & \alpha^{13} & \alpha^{11} & \alpha^{7} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & \alpha^{13} & \alpha^{11} & \alpha^{7} & \alpha^{14} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{11} & \alpha^{7} & \alpha^{14} & \alpha^{13} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{7} & \alpha^{14} & \alpha^{13} & \alpha^{11} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} & \alpha^{13} & \alpha^{11} & \alpha^{7} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{13} & \alpha^{11} & \alpha^{7} & \alpha^{14} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{5} & \alpha^{10}\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{10} & \alpha^{5}
\end{pmatrix}\\
&\times\begin{pmatrix}
111111111111111\\
100011110101100\\
100100011110101\\
110101100100011\\
101100100011110\\
101111011110111\\
110111101111011\\
111101111011110\\
111011110111101\\
110101111000100\\
111000100110101\\
101111000100110\\
100110101111000\\
101101101101101\\
110110110110110
\end{pmatrix}
\begin{pmatrix}
f_0\\ f_1\\ f_2\\ f_3\\ f_4\\ f_5\\ f_6\\ f_7\\ f_9\\ f_{10}\\ f_{11}\\ f_{12}\\ f_{13}\\ f_{14}\\ f_{15}
\end{pmatrix}
\end{aligned}
\tag{5}
$$