Normalized cyclic convolution: 

The case of even length

Sergei V. Fedorenko

Abstract—A normalized cyclic convolution is a cyclic convolution when one of its factors is a fixed polynomial. Herein, a novel method for constructing a normalized cyclic convolution over a finite field is introduced. This novel method is the first constructive and best known method for even lengths. This method can be applied for computing discrete Fourier transforms over finite fields.

Index Terms—Convolution, discrete Fourier transforms, fast Fourier transforms, Galois fields, Reed–Solomon codes.

I. INTRODUCTION

Reed–Solomon codes are used to correct errors in digital storage and communication systems, as well as for many other applications. The discrete Fourier transform (DFT) over a finite field can be applied for encoding and decoding the Reed–Solomon codes. A normalized cyclic convolution is a cyclic convolution when one of its factors is a fixed polynomial. A novel method for constructing a normalized cyclic convolution can be applied to compute the DFT over a finite field [10], [11], [12], [13]. The history and an overview of fast convolutions of arbitrary length over finite fields [12]. Some methods can be applied to compute the DFT over a finite field [10], [4].

There are no general algorithms for efficient short cyclic convolutions of arbitrary length over finite fields [12]. Some results on short cyclic convolutions were reported in [3], [1], [11], [12], [13]. The history and an overview of fast convolution algorithms can be found in the textbook [4]. The primary problem considered in this paper is how to reduce the complexity of the normalized cyclic convolution computation over a finite field. The novel algorithm proposed for computing the normalized cyclic convolution is valid for even length $m$.

The remainder of this paper is organized as follows. In section II, we present basic notations and definitions. In section III, we consider the relation between the multipoint evaluation and normalized cyclic convolution. In section IV, we propose and prove the novel algorithm for the computation of a multipoint evaluation. In section V, we consider the complexity of the normalized cyclic convolution computation. In the Appendix, we present a collection of normalized cyclic convolutions.

II. BASIC NOTIONS AND DEFINITIONS

We assume that the field of the computation is the finite field $GF(2^m)$ and that $m$ is even. Let $\alpha$ be a primitive element of the field $GF(2^m)$. Every vector $f = (f_i)$, $i = 0, 1, \ldots, n-1$, is associated with a polynomial $f(x) = \sum_{i=0}^{n-1} f_i x^i$.

Definition 1: The binary conjugacy class of element $\alpha^k$ in the field $GF(2^m)$ is

$$\left(\alpha^k, \alpha^k x^2, \alpha^k x^2^2, \ldots, \alpha^k x^2^{m-1}\right),$$

where $\alpha$ is a primitive element of the field $GF(2^m)$, $\alpha^k$ is a generator of the $k$th binary conjugacy class, and $m_k$ is the cardinality of the $k$th binary conjugacy class, and $m_k | m$.

To simplify the presentation, we can assume that the binary conjugacy classes of $GF(2^m)$ have cardinality $m$. The binary conjugacy classes of cardinality $m_k < m$ can be addressed in the same manner.

Definition 2: The minimal polynomial over a subfield $GF(2^{m_k}) \subset GF(2^m)$ of $\beta \in GF(2^m)$ is the lowest-degree monic polynomial $M(x)$ with coefficients from $GF(2^{m_k})$ such that $M(\beta) = 0$.

Let $M_k(x)$ be the minimal polynomial over $GF(2)$ of the element $\alpha^{c_k}$.

Let $M_{k,i}(x)$ be the minimal polynomial over $GF(2^{m/2})$ of the element $\alpha^{c_k x^2}$.

Definition 3: The matrix

$$\begin{pmatrix}
\alpha_0^i & \alpha_1^i & \alpha_2^i & \cdots & \alpha_{m-1}^i \\
\alpha_0^j & \alpha_1^j & \alpha_2^j & \cdots & \alpha_{m-1}^j \\
\alpha_0^j & \alpha_1^j & \alpha_2^j & \cdots & \alpha_{m-1}^j \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha_0^j & \alpha_1^j & \alpha_2^j & \cdots & \alpha_{m-1}^j \\
\end{pmatrix} = \left(\alpha_i^{j-1}\right),$$

$i, j = 1, 2, \ldots, t$, is called a Vandermonde matrix.

Definition 4: A Moore matrix is a matrix of the form

$$\begin{pmatrix}
\alpha_1^i & \alpha_2^i & \alpha_3^i & \cdots & \alpha_{m-1}^i \\
\alpha_2^i & \alpha_3^i & \alpha_4^i & \cdots & \alpha_{m-2}^i \\
\alpha_3^i & \alpha_4^i & \alpha_5^i & \cdots & \alpha_{m-3}^i \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\alpha_{m-1}^i & \alpha_{m-2}^i & \alpha_{m-3}^i & \cdots & \alpha_1^i \\
\end{pmatrix} = \left(\alpha_i^{q-1}\right),$$

$i, j = 1, 2, \ldots, t$, where $q$ is a prime power [9].

The transpose of a Vandermonde (respectively, Moore) matrix is also called a Vandermonde (respectively, Moore) matrix. If a matrix is simultaneously both a Vandermonde matrix and a Moore matrix, then it is called a Moore–Vandermonde matrix.

A basis $(\beta^0, \beta^1, \beta^2, \ldots, \beta^{m-1})$ of $GF(2^m)$ over $GF(2)$ is a polynomial basis for the field $GF(2^m)$, and a basis $(\delta^0, \delta^1, \delta^2, \ldots, \delta^{m/2-1})$, $\delta \in GF(2^{m/2})$, is a polynomial basis for the subfield $GF(2^{m/2}) \subset GF(2^m)$.

Let

$$\left(\gamma^0, \gamma^2, \gamma^2, \ldots, \gamma^{2^{m-1}}\right)$$

Part of this work was completed while S. V. Fedorenko visited the Communications Engineering Lab at the Technische Universität Darmstadt, Darmstadt, Germany. The work of S. V. Fedorenko was supported by the Alexander von Humboldt Foundation, Germany. This paper was presented in part at the 2011 IEEE International Symposium on Information Theory.

S. V. Fedorenko is with the Information Systems Security Department, St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia (e-mail: sergei.fedorenko@gmail.com).
be a normal basis for the field $GF(2^m)$.

**Definition 5:** A circulant matrix, or a circulant, is a matrix in which each row is obtained from the preceding row by a left (right) cyclic shift by one position. Let us denote by $L$ an $m \times m$ circulant, the first row of which is of a normal basis. We call it a basis circulant [5]:

$$L = \begin{pmatrix}
\gamma^{2^0} & \gamma^{2^1} & \cdots & \gamma^{2^{m-1}} \\
\gamma^{2^1} & \gamma^{2^2} & \cdots & \gamma^{2^{m-2}} \\
\vdots & \vdots & \ddots & \vdots \\
\gamma^{2^{m-1}} & \gamma^{2^{m-2}} & \cdots & \gamma^{2^0}
\end{pmatrix}
= \begin{pmatrix}
\gamma^{2^{i+j}}
\end{pmatrix},
$$

for $i, j = 0, 1, \ldots, m - 1$.

The basis circulant matrix is a Moore matrix for $q = 2$.

**Definition 6:** An $m$-point cyclic convolution is $a(x) = b(x)c(x)$ (mod $x^m - 1$), where $a(x) = \sum_{i=0}^{m-1} a_ix^i$, $b(x) = \sum_{i=0}^{m-1} b_ix^i$, $c(x) = \sum_{i=0}^{m-1} c_ix^i$, $a_i, b_i, c_i \in GF(2^m)$.

The cyclic convolution can be written as a matrix product

$$
\begin{pmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{m-1}
\end{pmatrix}
= \begin{pmatrix}
b_0 & b_{m-1} & b_{m-2} & \cdots & b_1 \\
b_1 & b_{m-2} & b_{m-3} & \cdots & b_0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
b_{m-1} & b_1 & b_0 & \cdots & b_{m-2}
\end{pmatrix}
\begin{pmatrix}
c_0 \\
c_1 \\
\vdots \\
c_{m-1}
\end{pmatrix}.
$$

**Definition 7:** A normalized cyclic convolution of length $m$ is a cyclic convolution when $b(x) = \gamma^{2^0} + \gamma^{2^{m-1}}x + \gamma^{2^{m-2}}x^2 + \cdots + \gamma^{2^1}x^{m-1}$ [10], [6].

The computation of a normalized cyclic convolution can be represented as a multiplication by a basis circulant matrix $L$.

**III. THE RELATION BETWEEN THE MULTIPRODUCT EVALUATION AND NORMALIZED CYCLIC CONVOLUTION**

**Definition 8:** The multipoint evaluation for the polynomial $t(x)$ and the point set $\{e_j \mid j \in J\}$ is a computation $t(e_j)$, $j \in J$ [7, Chapter 10.1].

The computation of a multipoint evaluation for any point set can be represented as a multiplication by a Vandermonde matrix. If the point set is the $kth$ binary conjunctive class, then the computation of a multipoint evaluation can be represented as a multiplication by a Moore–Vandermonde matrix $V_k = \begin{pmatrix} \alpha^{c_k2^0} \end{pmatrix}, i, j = 0, 1, \ldots, m - 1$.

Consider the simple construction of a polynomial basis. For this purpose, we require the following trivial Lemma.

**Lemma 1 ([6]):** Let $\beta$ be an arbitrary nonzero element in $GF(2^m)$ whose minimal polynomial over $GF(2)$ has degree $m$. Then, $(\beta^0, \beta^1, \beta^2, \ldots, \beta^{m-1})$ is a polynomial basis for the field $GF(2^m)$.

**Proof:** The proof is similar to the proof from [8, Chapter 4, Property (M4)]. The proof is achieved using reductio ad absurdum. If $(\beta^0, \beta^1, \beta^2, \ldots, \beta^{m-1})$ are linearly dependent, there exists a nonzero polynomial $\sum_{i=0}^{m-1} a_ix^i$, $a_i \in GF(2)$, having $\beta$ as a root, and the minimal polynomial over $GF(2)$ of $\beta$ has degree less than $m$, which is a contradiction. Therefore, $(\beta^0, \beta^1, \beta^2, \ldots, \beta^{m-1})$ are linearly independent.

For the $kth$ binary conjunctive class, whose minimal polynomial over $GF(2)$ has degree $m$, the basis $(\alpha^{c_k0}, (\alpha^{c_k})^1, (\alpha^{c_k})^2, \ldots, (\alpha^{c_k})^{m-1})$ is a polynomial basis, whereas $(\gamma^{2^0}, \gamma^{2^1}, \gamma^{2^2}, \ldots, \gamma^{2^{m-1}})$ is a normal basis for the field $GF(2^m)$.

Let us construct the basis transformation matrix $N_k$ as follows:

$$
\begin{pmatrix}
(\alpha^{c_k})^0 & (\alpha^{c_k})^1 & (\alpha^{c_k})^2 & \cdots & (\alpha^{c_k})^{m-1}
\end{pmatrix} = \frac{1}{N_k}.
$$

Note that the $m \times m$ matrix $N_k$ is binary and nonsingular.

**Lemma 2 ([6]):** The relation between the Moore–Vandermonde matrix $V_k$ and the basis circulant $L = L_k N_k$, where $N_k$ is the basis transformation matrix.

**Proof:** Let $V_k = \begin{pmatrix} \alpha^{c_k2^0} \end{pmatrix}, i, j = 0, 1, \ldots, m - 1$, be a Moore–Vandermonde matrix. $L = \begin{pmatrix} \gamma^{2^{i+j}} \end{pmatrix}, i, j = 0, 1, \ldots, m - 1$, is a basis circulant matrix.

Using (1), we have

$$
\begin{pmatrix}
\gamma^{2^0} & \gamma^{2^1} & \cdots & \gamma^{2^{m-1}} \\
\gamma^{2^1} & \gamma^{2^2} & \cdots & \gamma^{2^{m-2}} \\
\vdots & \vdots & \ddots & \vdots \\
\gamma^{2^{m-1}} & \gamma^{2^{m-2}} & \cdots & \gamma^{2^0}
\end{pmatrix}
= \begin{pmatrix}
(\alpha^{c_k})^02^0 & (\alpha^{c_k})^12^0 & \cdots & (\alpha^{c_k})^{m-1}2^0 \\
(\alpha^{c_k})^02^1 & (\alpha^{c_k})^12^1 & \cdots & (\alpha^{c_k})^{m-1}2^1 \\
\vdots & \vdots & \ddots & \vdots \\
(\alpha^{c_k})^02^{m-1} & (\alpha^{c_k})^12^{m-1} & \cdots & (\alpha^{c_k})^{m-1}2^{m-1}
\end{pmatrix} N_k
$$

and $L = V_k N_k$.

Thus, the complexities of a normalized cyclic convolution and a multipoint evaluation computation are almost identical. They differ only by the matrix of pre-additions $N_k$.

**Example I:** The finite field $GF(2^4)$ is defined by an element $\alpha$, which is a root of the primitive polynomial $x^4 + x + 1$. Let $c_k = 1, (\alpha^{c_k0}, \alpha^{c_k1}, \alpha^{c_k2}, \alpha^{c_k3})$ be a polynomial basis, while $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ is a normal basis for $GF(2^4)$, where $\gamma = \alpha^6$.

Let us construct the basis transformation matrix $N_1$ as follows:

$$
\begin{pmatrix}
\gamma^1 & \gamma^2 & \gamma^4 & \gamma^8
\end{pmatrix} = \begin{pmatrix}
\alpha^0 & \alpha^1 & \alpha^2 & \alpha^3
\end{pmatrix}
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
1 & 1 & 1 & 1
\end{pmatrix}.
$$

Using the relation $L = V_1 N_1$ between the Moore–Vandermonde matrix $V_1$ and the basis circulant $L$, we obtain

$$
\begin{pmatrix}
\gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 \\
\gamma^2 & \gamma^4 & \gamma^8 & \gamma^1 \\
\gamma^4 & \gamma^8 & \gamma^1 & \gamma^2 \\
\gamma^8 & \gamma^1 & \gamma^2 & \gamma^4
\end{pmatrix}
= \begin{pmatrix}
1 & \alpha^1 & \alpha^2 & \alpha^3 \\
1 & \alpha^2 & \alpha^4 & \alpha^6 \\
1 & \alpha^4 & \alpha^8 & \alpha^{12} \\
1 & \alpha^8 & \alpha^1 & \alpha^9
\end{pmatrix}
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 \\
1 & 1 & 1 & 1
\end{pmatrix}.
$$
IV. THE MULTIPoint EVALUATION FOR THE BINARY CONJUGACY CLASS

Consider the multipoint evaluation for the polynomial $t(x) = \sum_{i=0}^{m-1} t_i x^i$ and the binary conjugacy class $(\alpha^c, \alpha^{c2}, \alpha^{c22}, \ldots, \alpha^{c2^{m-1}})$ of $GF(2^m)$. We compute

$$T_i = t\left(\alpha^{c2^i}\right), \quad i = 0, 1, \ldots, m - 1.$$ 

Let us write the multipoint evaluation in matrix form:

$$\begin{pmatrix} T_0 \\ T_1 \\ \vdots \\ T_{m-1} \end{pmatrix} = \begin{pmatrix} t(\alpha^{c2^0}) \\ t(\alpha^{c2^1}) \\ \vdots \\ t(\alpha^{c2^{m-1}}) \end{pmatrix} = \begin{pmatrix} \alpha^{c0} & \alpha^{c12^0} & \alpha^{c22^0} & \ldots & \alpha^{c(m-1)2^0} \\ \alpha^{c02} & \alpha^{c12^1} & \alpha^{c22^1} & \ldots & \alpha^{c(m-1)2^1} \\ \vdots \\ \alpha^{c02^{m-1}} & \alpha^{c12^{m-1}} & \alpha^{c22^{m-1}} & \ldots & \alpha^{c(m-1)2^{m-1}} \end{pmatrix} \begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ \vdots \\ t_{m-1} \end{pmatrix},$$

where

$$T = V_k t,$$

$T = (T_i), t = (t_i), \quad i = 0, 1, \ldots, m - 1, \quad V_k = \left(\alpha^{c2^j}\right), \quad i, j = 0, 1, \ldots, m - 1,$

is a Moore–Vandermonde matrix.

Let us formulate the main result for the computation of a multipoint evaluation.

**Theorem 1:** For any finite field $GF(2^m)$ with even $m$, there exists a binary conjugacy class of cardinality $m$; the multipoint evaluation for this class reduces to two multipoint evaluations for the binary conjugacy class of cardinality $m/2$ in the subfield $GF(2^{m/2})$ and approximately $m$ extra field operations.

The multipoint evaluation matrix for even $m, \ m \geq 2,$ is defined in formula (4), $\Delta = \left(\delta^{j2^i}\right), \quad i, j = 0, 1, \ldots, m/2 - 1,$ is a Moore–Vandermonde matrix, $\delta = \left(\alpha^{2^{j2^i}+1}\right)^{c^k} \in GF(2^{m/2})$, and the binary matrix $B$ is defined in Lemma 9.

Note that the matrix $B$ may be calculated directly from formula (2). In the remainder of this section, we consider the proof of Theorem 1.

A. The properties of the binary conjugacy class

**Lemma 3:** Let $\alpha^{c^k}$ be a generator of the $k$th binary conjugacy class $(\alpha^{c^k}, \alpha^{c^k2}, \alpha^{c^k2^2}, \ldots, \alpha^{c^k2^{m-1}})$ of cardinality $m$, where $m$ is even, $\alpha$ is a primitive element of the field $GF(2^m)$, and $GF(2^{m/2})[x]$ is a polynomial ring (the ring of polynomials over field $GF(2^{m/2})$). The polynomials

$$(x - \alpha^{c^2i})(x - \alpha^{c2^{m/2+i}}) \in GF(2^{m/2})[x],$$

$i = 0, 1, \ldots, m/2 - 1$, are the different, irreducible, and minimal polynomials over $GF(2^{m/2})$.

**Proof:** Let $M_{k,i}(x) = (x - \alpha^{c^2i})(x - \alpha^{c2^{m/2+i}})$

$$= x^2 + \left(\alpha^{c2^i} + \alpha^{c2^{m/2+i}}\right)x + \alpha^{c2(2^{m/2}+1)} = x^2 + \beta_i + \beta_i^{2^{m/2}} + x^2 \delta^{2^i},$$

where $\beta_i = \alpha^{c2^i}, \ i = 0, 1, \ldots, m/2 - 1, \delta = \alpha^{2^{m/2}+1} \in GF(2^{m/2})$.

The element $(\beta_i + \beta_i^{2^{m/2}})^{2^{m/2}}$ is a root of the polynomial $x^{2^{m/2}} + x$; hence, $(\beta_i + \beta_i^{2^{m/2}}) \in GF(2^{m/2})$.

Thus, the polynomials $M_{k,i}(x) \in GF(2^{m/2})[x], \ i = 0, 1, \ldots, m/2 - 1, \alpha$ are the minimal and irreducible polynomials over $GF(2^{m/2})$.

Using $M_k(x) = \prod_{i=0}^{m/2-1} (x - \alpha^{c2^i}) = \prod_{i=0}^{m/2-1} M_{k,i}(x)$, we see that all of the polynomials $M_{k,i}(x)$ are different. 

Let us formulate the condition that the minimal polynomial $M_k(x)$ over $GF(2^{m/2})$ has two coefficients equal to 1.

**Lemma 4:** If $\alpha^{c^k} = \alpha^{c2^i} + 1, \ m$ is even, for the binary conjugacy class $(\alpha^{c^k}, \alpha^{c^k2}, \alpha^{c^k2^2}, \ldots, \alpha^{c^k2^{m-1}})$, then

1) $\alpha^{c^k}$ is a root of the polynomial $x^{2^{m/2}} + x + 1$;

2) $\alpha^{c^k2^i} = \alpha^{c2^i} + 1$ for all $i = 0, 1, \ldots, m/2 - 1$;

3) the minimal polynomials over $GF(2^{m/2})$ are

$$M_{k,i}(x) = \left(x - \alpha^{c2^i}\right)\left(x - \alpha^{c2^{m/2+i}}\right) = x^2 + x + \delta^{2^i},$$

where $\delta = \left(\alpha^{2^{m/2}+1}\right)^{c^k} \in GF(2^{m/2}), \ i = 0, 1, \ldots, m/2 - 1$.

4) the minimal polynomials $M_{k,i}(x), \ i = 0, 1, \ldots, m/2 - 1$, over $GF(2^{m/2})$ are different. The elements $\delta^{2^i}, \ i = 0, 1, \ldots, m/2 - 1$ are also different;

5) the minimal polynomial over $GF(2)$ is

$$M_k(x) = \prod_{i=0}^{m/2-1} (x - \alpha^{c2^i})$$

$$= \prod_{i=0}^{m/2-1} M_{k,i}(x) = \prod_{i=0}^{m/2-1} \left(x^2 + x + \delta^{2^i}\right).$$

**Proof:** The proof is trivial. 


B. The binary conjugacy class choice

Theorem 2: For any finite field $GF(2^m)$ with even $m$, there exists the binary conjugacy class $(\alpha^c, \alpha^{ck}, \alpha^{2ck}, \ldots, \alpha^{(2^m-1)ck})$ such that $\alpha^{ck} = \alpha^{2m/2} + 1$.

To prove this theorem, we require two Lemmas.

Lemma 5: For any finite field $GF(2^m)$ with even $m$:

$$x^{2^{m/2}} + x + 1 | x^{2^m} + x.$$

Proof: We clearly have

$$x^{2^m} + x = (x^{2^{m/2}} + x + 1) (x^{2^{m/2} - 2} + 1).$$

Lemma 6: For any finite field $GF(2^m)$ with even $m$, there exists the minimal polynomial $M_k(x)$ of degree $m$ over $GF(2)$ such that

$$M_k(x) | x^{2^{m/2}} + x + 1.$$

Proof: The number of elements of order $2^m - 1$ is larger than $2^m - 2^{m/2} + 1$ [2, Theorem 3.35]. Therefore, this polynomial has at least one root of order $2^m - 1$. The minimal degree of $m$ over $GF(2)$ for this root divides the polynomial $x^{2^{m/2}} + x + 1$.

This completes the proof of Theorem 2.

The binary conjugacy class choice consists of two steps:

1. construct the minimal polynomial $M_k(x)$ of degree $m$ over $GF(2)$ such that

$$M_k(x) | x^{2^{m/2}} + x + 1;$$

2. choose a root $\alpha^{ck}$ of the minimal polynomial $M_k(x)$ as a generator of the $k$th binary conjugacy class $(\alpha^{ck}, \alpha^{ck^2}, \alpha^{ck^2^2}, \ldots, \alpha^{ck^{2^m-1}})$.

We further assume that the binary conjugacy class $(\alpha^{ck}, \alpha^{ck^2}, \alpha^{ck^2^2}, \ldots, \alpha^{ck^{2^m-1}})$ (hence, the minimal polynomial $M_k(x)$ and the multipoint evaluation matrix $V_k$) is chosen according to Theorem 2.

C. The Goertzel–Blahut algorithm

Definition 9: The DFT of length $n$ of a vector $f = (f_i), i = 0, 1, \ldots, n - 1, n | (2^m - 1)$, in the field $GF(2^m)$ is the vector $F = (F_j)$,

$$F_j = f(\alpha^j) = \sum_{i=0}^{n-1} f_i \alpha^{ij}, j = 0, 1, \ldots, n - 1,$$

where $\alpha$ is an element of order $n$ in $GF(2^m)$.

We consider the Blahut modification for the DFT computation over finite fields of Goertzel’s algorithm [3].

The first step of the Goertzel–Blahut algorithm is a long division of $f(x)$ by each minimal polynomial $M_k(x)$:

$$f(x) = M_k(x)q_k(x) + r_k(x), \quad \deg r_k(x) < \deg M_k(x) = m_k,$$

where $r_k(x) = \sum_{j=0}^{m_k-1} r_{kj} x^j$ and $l$ is the number of binary conjugacy classes.

The second step of the Goertzel–Blahut algorithm is to evaluate the remainder at each element of the finite field:

$$F_i = f(\alpha^i) = r_k(\alpha^i) = \sum_{j=0}^{m_k-1} r_{kj} \alpha^{ij},$$

$$i = 0, 1, \ldots, n - 1,$$

where an element $\alpha^i$ is a root of the minimal polynomial $M_k(x)$.

Note that the Goertzel–Blahut algorithm can be written in matrix form [4] as follows:

$$F = \text{diag}(L_0, L_1, \ldots, L_{l-1}) R f,$$

where $L_0, L_1, \ldots, L_{l-1}$ are the basis circulant matrices and $R$ is a binary matrix.

D. Two division levels in the multipoint evaluation

The novel method that we introduce for the multipoint evaluation is similar to the Goertzel–Blahut algorithm. From Lemma 4, it follows that the quadratic polynomial $M_k(x)$ has two coefficients equal to 1, and a division by this polynomial is very simple.

The upper level of divisions is a long division of polynomial $t(x) = \sum_{i=0}^{m-1} t_i x^i$ by each quadratic polynomial $M_k(x) = x^2 + x + \delta^2 = (x - \alpha^{ck^2}) (x - \alpha^{ck^{2^m-1}})$, $i = 0, 1, \ldots, m/2 - 1$:

$$t(x) = x^2 + \delta^2 q_i(x) + u_i(x),$$

$$u_i(x) = u_{i,1} x + u_{i,0},$$

$$i = 0, 1, \ldots, m/2 - 1,$$

where $\delta = (\alpha^{2^{m/2} + 1})^{ck} \in GF(2^{m/2})$.

The lower level of divisions consists of evaluating the remainder $u_i(x)$ at pair conjugates $\alpha^{ck^2}$ and $\alpha^{ck^{2^m-1}}$ (with respect to $GF(2^{m/2})$) for all $i = 0, 1, \ldots, m/2 - 1$:

$$T_{i} = t(\alpha^{ck^2}) = u_i (\alpha^{ck^2}),$$

$$T_{m/2+i} = t(\alpha^{ck^{2^m-1}}) = u_i (\alpha^{ck^{2^m-1}}),$$

$$i = 0, 1, \ldots, m/2 - 1.$$

E. The matrix form of two division levels in the multipoint evaluation

We decompose the multipoint evaluation matrix into two factors

$$V_k = V_{lower} U_{upper},$$

where $U_{lower}, U_{upper}$ are nonsingular.
a) The lower level of divisions: Consider the matrix form of the lower level of divisions

\[
\begin{pmatrix}
T_0 \\
T_1 \\
T_2 \\
\vdots \\
T_{m/2} \\
T_{m/2+1} \\
\vdots \\
T_{m-1}
\end{pmatrix}
= U_{\text{lower}}
\begin{pmatrix}
u_{0,0} \\
u_{0,1} \\
u_{1,0} \\
u_{1,1} \\
u_{2,0} \\
u_{2,1} \\
\vdots \\
u_{m/2-1,0} \\
u_{m/2-1,1}
\end{pmatrix},
\]

where

\[
U_{\text{lower}} =
\begin{pmatrix}
1 & \alpha^{ck} & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & \alpha^{ck/2} & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \cdots & 1 & \alpha^{ck2^m-2} \\
1 & \alpha^{ck2^m/2} & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & \alpha^{ck2^m/2+1} & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \alpha^{ck2^m-1}
\end{pmatrix}
\times
\begin{pmatrix}
I_{m/2} \\
I_{m/2} \\
O \\
O
\end{pmatrix}
\]

\[
= \left( \begin{array}{c|c}
I_{m/2} & O \\
\hline
I_{m/2} & I_{m/2} \\
O & O
\end{array} \right)
\]

b) The upper level of divisions: Consider the matrix form of the upper level of divisions for \( m > 2 \)

\[
U_{\text{upper}} = U_{\text{upper}}^{-1}
\begin{pmatrix}
t_0 \\
t_1 \\
t_2 \\
\vdots \\
t_{m-1}
\end{pmatrix},
\]

where

\[
\Delta = \begin{pmatrix}
\delta^{02^0} & \delta^{12^1} & \delta^{22^0} & \cdots & \delta^{(m/2-1)2^0} \\
\delta^{02^1} & \delta^{12^2} & \delta^{22^1} & \cdots & \delta^{(m/2-1)2^1} \\
\delta^{02^2} & \delta^{12^3} & \delta^{22^2} & \cdots & \delta^{(m/2-1)2^2} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\delta^{02^{m/2-2}} & \delta^{12^{m/2-1}} & \delta^{22^{m/2-2}} & \cdots & \delta^{(m/2-1)2^{m/2-2}}
\end{pmatrix} = \left( \delta^{2^i} \right), \quad i, j = 0, 1, \ldots, m/2 - 1,
\]

is a Moore–Vandermonde matrix, \( \delta = \left( \alpha^{2^i+1} \right)^c_k \in GF(2^{m/2}), \) \( O \) is the \((m/2) \times (m/2)\) all-zero matrix, and the binary matrix \( B \) is defined in Lemma 9.

To prove this Theorem, we require several Lemmas.

Lemma 7: The polynomial \( r_1x + r_0 \) is the remainder polynomial of the polynomial \( t(x) = \sum_{i=0}^{m-1} t_i x^i \), \( m > 2 \), when divided by the quadratic polynomial \( x^2 + x + \epsilon \), \( \epsilon \in GF(2^m) \), in a characteristic two finite field. Then,

\[
\left( \begin{array}{c}
r_0 \\
r_1
\end{array} \right) = U \left( \begin{array}{c}
t_0 \\
t_1 \\
t_2 \\
\vdots \\
t_{m-1}
\end{array} \right),
\]

where the remainder matrix is

\[
U = \left( \begin{array}{c c c c c}
r_{0,0} & r_{0,1} & r_{0,2} & \cdots & r_{0,m-1} \\
\r_{1,0} & r_{1,1} & r_{1,2} & \cdots & r_{1,m-1}
\end{array} \right),
\]

with initial conditions

\[
\begin{align*}
& \begin{cases}
\begin{array}{l}
r_{1,0} = 0 \\
r_{0,0} = 1 \\
r_{1,i+1} = r_{1,i} + r_{0,i} \\
r_{0,i+1} = \epsilon r_{1,i}
\end{array}
\end{cases} \\
& \quad \text{Proof: Let } x^i \equiv r_{1,i}x + r_{0,i} \pmod{x^2 + x + \epsilon}.
\end{align*}
\]

From \( r_1x + r_0 \equiv \sum_{i=0}^{m-1} t_i x^i \equiv \sum_{i=0}^{m-1} t_i (r_{1,i}x + r_{0,i}) \equiv \)
Lemma 9: If $m$ is even and $\epsilon = \delta = \delta^0 = \left(\alpha^{2m/2+1}\right)^{t_k} \in GF(2^{m/2})$, then all elements of the remainder matrix

$$U = U(0) = \begin{pmatrix} r_{0,0} & r_{0,1} & r_{0,2} & \cdots & r_{0,m-1} \\ r_{1,0} & r_{1,1} & r_{1,2} & \cdots & r_{1,m-1} \end{pmatrix}$$

belong to the subfield $GF(2^{m/2}) \subset GF(2^m)$.

Corollary 2: If $m$ is even, then the remainder matrix of $U(i) = \left[U(0)\right]^{2^i} = \left[U\right]^{2^i}$, where the matrix $\left[U\right]^j$ consists of the $j$th power of all elements of the matrix $U$.

Lemma 8: Let $\delta = \left(\alpha^{2m/2+1}\right)^{t_k} \in GF(2^{m/2})$, $m$ is even, and $m > 2$; then, \(\delta^0, \delta^1, \delta^2, \ldots, \delta^{m/2-1}\) is a polynomial basis for the subfield $GF(2^{m/2}) \subset GF(2^m)$.

Proof: Because all elements $\delta^i$, $i = 0, 1, \ldots, m/2-1$, are different (see Lemma 4, Property 4), it follows that $\left(\delta^0, \delta^1, \delta^2, \ldots, \delta^{m/2-1}\right)$ is the binary conjugacy class of $GF(2^{m/2})$. Using Lemma 1 for the case of the field $GF(2^{m/2})$, we have that $\left(\delta^0, \delta^1, \delta^2, \ldots, \delta^{m/2-1}\right)$ is a polynomial basis for the subfield $GF(2^{m/2}) \subset GF(2^m)$.

Lemma 9: If the remainder matrix $U$ is defined in Lemma 7, for $\epsilon = \delta$

$$U = U(0) = \begin{pmatrix} r_{0,0} & r_{0,1} & r_{0,2} & \cdots & r_{0,m-1} \\ r_{1,0} & r_{1,1} & r_{1,2} & \cdots & r_{1,m-1} \end{pmatrix}$$

$m$ is even, $m > 2$, $\left(\delta^0, \delta^1, \delta^2, \ldots, \delta^{m/2-1}\right)$ is a polynomial basis for the subfield $GF(2^{m/2}) \subset GF(2^m)$, and $\delta = \left(\alpha^{2m/2+1}\right)^{t_k} \in GF(2^{m/2})$, then there is a nonsingular binary matrix $B$ such that

$$UB = \begin{pmatrix} \delta^0 & 0 & \delta^1 & 0 & \delta^2 & 0 & \cdots & \delta^{m/2-1} & 0 \\ 0 & \delta^0 & 0 & \delta^1 & 0 & \delta^2 & \cdots & 0 & \delta^{m/2-1} \end{pmatrix}$$

Proof: Let the matrix $U_j$ consist of the first $2(j + 1)$ columns of the matrix $U$.

$$U_j = \begin{pmatrix} r_{0,0} & r_{0,1} & r_{0,2} & \cdots & r_{0,2j} \\ r_{1,0} & r_{1,1} & r_{1,2} & \cdots & r_{1,2j} \end{pmatrix}$$

We use mathematical induction on $j$.
The complexity of operations in the subfields is considerably less than the complexity of operations in the field of the computation. We choose not to distinguish between operations in the subfields and operations in the field of the computation. This completes the proof of Theorem 1. The examples are given in the Appendix.

V. THE COMPLEXITY OF THE NORMALIZED CYCLIC CONVOLUTION COMPUTATION

The complexity of the novel method is calculated from the number of nontrivial multiplications and additions in the field of the computation \( GF(2^n) \). Considering that the complexity of operations in the subfields is considerably less than the complexity of operations in the field of the computation, we choose not to distinguish between operations in the subfields and field of the computation in the bookkeeping [4].

The recursive formulae for the number of multiplications and additions of the multipoint evaluation (or the normalized cyclic convolution computation) over \( GF(2^n) \) are

\[
\begin{align*}
\text{Mult}(m) &= 2 \text{Mult}(m/2) + m/2, \\
\text{Add}(m) &= 2 \text{Add}(m/2) + m,
\end{align*}
\]

with initial condition \( \text{Mult}(1) = \text{Add}(1) = 0 \).

These recursions are satisfied by

\[
\begin{align*}
\text{Mult}(m) &= \frac{1}{2} m \log_2 m \\
\text{Add}(m) &= m \log_2 m
\end{align*}
\]

for \( m = 2^i, \ i \geq 0 \).

Let us recall (see Lemma 2) that the complexities of a normalized cyclic convolution and a multipoint evaluation computation are almost identical. They differ only by the matrix of pre-additions. Taking into account (3), we see that the matrix of pre-additions \( B^{-1} \) (or \( B^{-1} N_k \)) can be absorbed into the binary matrix \( R \) of the DFT computation.

It follows that the algorithm complexity does not depend on pre-additions. In the formula for the number of additions and in Table I, the number of pre-additions is not included. The complexity of the normalized cyclic convolution computation over \( GF(2^n) \) for old methods [3], [12, Table 1], and for even \( m \) of the novel method is shown in Table I.

A novel method for computing the normalized cyclic convolution over a finite field with reduced complexity is described. The proposed method is applicable for any composite length, but reduced complexity is achieved only for even lengths. For the normalized cyclic convolution computation of length \( m \) in the field \( GF(2^n) \) for even \( m \), the novel method is the best known method, and the exact formulae for the number of multiplications and additions are analytically obtained.

VI. CONCLUSION

The author would like to thank the Alexander von Humboldt Foundation, Germany, for the many years of support of his research; Prof. Anja Klein for her hospitality at the Technische Universität Darmstadt, Darmstadt, Germany; Valentin Afanassiev and Peter Trifonov for helpful discussions; and Grigory Kabatiansky for pointing out a mistake in an earlier version of this paper.

<table>
<thead>
<tr>
<th>( m )</th>
<th>Mult</th>
<th>Add</th>
<th>Mult</th>
<th>Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>5</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>16</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>21</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>24</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>19</td>
<td>35</td>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>18</td>
<td>40</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>10</td>
<td>28</td>
<td>52</td>
<td>23</td>
<td>42</td>
</tr>
<tr>
<td>11</td>
<td>42</td>
<td>76</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>12</td>
<td>32</td>
<td>53</td>
<td>24</td>
<td>44</td>
</tr>
</tbody>
</table>

ACKNOWLEDGMENT
APPENDIX

A COLLECTION OF NORMALIZED CYCLIC CONVOLUTIONS

LENGTH m = 2

Let $c_k=1$ while the binary conjugacy class is $(\alpha^1, \alpha^2)$ of $GF(2^2)$ and $(\gamma, \gamma^2)$ is a normal basis for the $GF(2^2)$, where $\gamma = \alpha$.

There is only a lower level of divisions.

$$\begin{pmatrix} \gamma^1 & \gamma^2 \\ \gamma^2 & \gamma^1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha^1 \\ 1 & \alpha^2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha^0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot$$

LENGTH m = 4

The finite field $GF(2^4)$ is defined by an element $\alpha$, which is the root of the primitive polynomial $x^4 + x + 1$. Let $c_k=1$ while the binary conjugacy class is $(\alpha^1, \alpha^2, \alpha^4, \alpha^8), (\alpha^0, \alpha^2, \alpha^2, \alpha^8)$ is a polynomial basis, and $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ is a normal basis for the $GF(2^4)$, where $\gamma = \alpha^6$.

$$\begin{pmatrix} \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 \\ \gamma^2 & \gamma^4 & \gamma^8 & \gamma^1 \\ \gamma^4 & \gamma^8 & \gamma^1 & \gamma^2 \\ \gamma^8 & \gamma^1 & \gamma^2 & \gamma^4 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 10 & 0 & 0 \\ 1 & 11 & 0 & 0 \\ 1 & 01 & 0 & 0 \\ 1 & 00 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & \alpha^{36} & \alpha^9 & \alpha^{18} \\ \alpha^9 & \alpha^{36} & \alpha^9 & \alpha^{18} \\ \alpha^{18} & \alpha^9 & \alpha^{36} & \alpha^9 \\ \alpha^{18} & \alpha^{18} & \alpha^{18} & \alpha^{18} \end{pmatrix} \cdot$$

Using $\delta = \alpha^5$, we have

$$\Delta = \begin{pmatrix} 1 & \alpha^5 \\ 1 & \alpha^{10} \end{pmatrix} = \begin{pmatrix} 1 & \delta \\ 1 & \delta^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot$$

The last three matrices in the 4-point convolution form the matrix of pre-additions. The multiplication by the matrix $\Delta$ requires one multiplication and two additions according to the computation complexity of the 2-point convolution. The last procedure is computed twice. The multiplication by the second matrix requires two multiplications and two additions. Finally, the multiplication by the first matrix requires two additions. The resulting complexity is 4 multiplications and 8 additions.

Note that the matrix $B$ is

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

LENGTH m = 6

$GF(2^6)$, $\alpha^6 + \alpha + 1 = 0$, $\gamma = \alpha^3$.

$$\begin{pmatrix} \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 & \gamma^{16} & \gamma^{32} \\ \gamma^2 & \gamma^4 & \gamma^8 & \gamma^{16} & \gamma^{32} & \gamma^1 \\ \gamma^4 & \gamma^8 & \gamma^{16} & \gamma^{32} & \gamma^1 & \gamma^4 \\ \gamma^8 & \gamma^{16} & \gamma^{32} & \gamma^1 & \gamma^4 & \gamma^8 \\ \gamma^{16} & \gamma^{32} & \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 \\ \gamma^{32} & \gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 & \gamma^{16} \end{pmatrix} = \begin{pmatrix} 100000 \\ 010000 \\ 001000 \\ 000100 \\ 000010 \end{pmatrix} = \begin{pmatrix} 1 & \beta^3 & \beta^2 \\ 1 & \beta^2 & \beta^4 \\ 1 & \beta^4 & \beta^1 \\ \alpha^{11} & 0 & 0 \\ 0 & \alpha^{22} & 0 \\ 0 & 0 & \alpha^{44} \end{pmatrix} \cdot$$

From [3] it follows that

$$\begin{pmatrix} 1 & \beta^3 & \beta^2 \\ 1 & \beta^2 & \beta^4 \\ 1 & \beta^4 & \beta^1 \end{pmatrix} = \begin{pmatrix} 111 & 110 & 1110 & 1011 & 010110 \\ 0111 & 1101 & 1101 & 1010 & 011000 \\ 0011 & 1010 & 1100 & 1001 & 000011 \\ 0001 & 00010 & 000010 & 010000 & 000001 \end{pmatrix} \times \begin{pmatrix} 111 & 110 & 1110 & 1010 & 100 \end{pmatrix} \cdot$$

over $GF(2^3)$, $\beta^3 + \beta^2 + 1 = 0$.

Substituting $\beta = \alpha^{36}$, we get

$$\Delta = \begin{pmatrix} 1 & \alpha^{36} & \alpha^9 \\ 1 & \alpha^{9} & \alpha^{18} \\ 1 & \alpha^{18} & \alpha^{36} \end{pmatrix} = \begin{pmatrix} 1 & \beta^1 & \beta^2 \\ 1 & \beta^2 & \beta^4 \\ 1 & \beta^4 & \beta^1 \end{pmatrix} \cdot$$

Note that the matrices of pre-additions for the 3-point convolution can be absorbed into the matrices of pre-additions for the 6-point convolution.

LENGTH m = 8

$GF(2^8)$, $\zeta^8 + \zeta^4 + \zeta^3 + \zeta^2 + 1 = 0$, $\eta = \zeta^5$.

$$\begin{pmatrix} \eta^1 & \eta^2 & \eta^4 & \eta^8 & \eta^{16} & \eta^{32} & \eta^{64} & \eta^{128} \\ \eta^2 & \eta^4 & \eta^8 & \eta^{16} & \eta^{32} & \eta^{64} & \eta^{128} & \eta^1 \\ \eta^4 & \eta^8 & \eta^{16} & \eta^{32} & \eta^{64} & \eta^{128} & \eta^1 & \eta^4 \\ \eta^8 & \eta^{16} & \eta^{32} & \eta^{64} & \eta^{128} & \eta^1 & \eta^4 & \eta^8 \\ \eta^{16} & \eta^{32} & \eta^{64} & \eta^{128} & \eta^1 & \eta^2 & \eta^4 & \eta^8 \\ \eta^{32} & \eta^{64} & \eta^{128} & \eta^1 & \eta^4 & \eta^8 & \eta^{16} & \eta^{32} \\ \eta^{128} & \eta^1 & \eta^4 & \eta^8 & \eta^{16} & \eta^{32} & \eta^{64} & \eta^{128} \end{pmatrix} = \begin{pmatrix} 10000000 \\ 01000000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000010 \\ 00000001 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & \zeta^7 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \zeta^{14} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \zeta^{28} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & \zeta^{56} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot$$
Using $\alpha = \zeta^{17} \in GF(2^4)$, we get the 4-point convolution over $GF(2^4) \subset GF(2^8)$ for submatrix

$$
\Delta = \begin{pmatrix}
1 & \zeta^{119} & \zeta^{238} & \zeta^{187} & \zeta^{119} \\
\zeta^{238} & \zeta^{221} & \zeta^{187} & \zeta^{119} & \zeta^{101} \\
\zeta^{187} & \zeta^{221} & \zeta^{101} & \zeta^{204} & \zeta^{107} \\
\zeta^{119} & \zeta^{238} & \zeta^{107} & \zeta^{204} & \zeta^{101} \\
\end{pmatrix}
= \begin{pmatrix}
\gamma^1 & \gamma^2 & \gamma^4 & \gamma^8 \\
\gamma^2 & \gamma^4 & \gamma^8 & \gamma^1 \\
\gamma^4 & \gamma^8 & \gamma^1 & \gamma^2 \\
\gamma^8 & \gamma^1 & \gamma^2 & \gamma^4 \\
\end{pmatrix}
= \begin{pmatrix} 1 & 1111 \\
1111 & 1010 \\
1010 & 1100 \\
1100 & 1000 \\
\end{pmatrix}.
$$

The details and definitions for $\alpha$, $\gamma$, and $\delta$ are given in the Example for the 4-point convolution.

**LENGTH $m = 10$**

$GF(2^{10})$, $\alpha^{10} + \alpha^3 + 1 = 0$, $\gamma = \alpha^7$.

$$
\begin{pmatrix}
\gamma^1 & \gamma^2 & \ldots & \gamma^512 \\
\gamma^2 & \gamma^4 & \ldots & \gamma^1 \\
\ldots & \ldots & \ldots & \ldots \\
\gamma^{512} & \gamma^1 & \ldots & \gamma^{256} \\
\end{pmatrix}
= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \alpha^{37} & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & \alpha^{74} & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & \alpha^{148} & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & \alpha^{256} & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \alpha^{592} & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{pmatrix}
\times
\begin{pmatrix}
\Delta \\
\end{pmatrix}
\times
\begin{pmatrix}
\Delta \\
\end{pmatrix}
$$

over $GF(2^{10})$, $\beta^5 + \beta^4 + \beta^3 + \beta^2 + 1 = 0$.

**LENGTH $m = 12$**

$GF(2^{12})$, $\alpha^{12} + \alpha^6 + \alpha^4 + \alpha + 1 = 0$, $\gamma = \alpha^{17}$.

Using $\beta = \alpha^{66} \in GF(2^{5})$ and $\eta = \beta^3$, we get the 5-point convolution over $GF(2^{5}) \subset GF(2^{10})$ for submatrix

$$
\Delta = \begin{pmatrix}
1 & \alpha^{198} & \alpha^{396} & \alpha^{594} & \alpha^{792} \\
\alpha^{396} & \alpha^{792} & \alpha^{165} & \alpha^{561} & \alpha^{99} \\
\alpha^{792} & \alpha^{561} & \alpha^{330} & \alpha^{99} & \alpha^{198} \\
\alpha^{99} & \alpha^{198} & \alpha^{127} & \alpha^{596} & \alpha^{396} \\
\end{pmatrix}
= \begin{pmatrix} 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} \\
\beta^3 & \beta^6 & \beta^{12} & \beta^{24} & \beta^{17} \\
\beta^6 & \beta^{12} & \beta^3 & \beta^5 & \beta^3 \\
\beta^{12} & \beta^{24} & \beta^3 & \beta^5 & \beta^3 \\
\beta^9 & \beta^{17} & \beta^3 & \beta^5 & \beta^3 \\
\end{pmatrix}
$$

From [3] it follows that

$$
\Delta = \begin{pmatrix} 1 & 11011010001 \\
11011010001 & 1111111110 \\
1111111110 & 11001000101 \\
11001000101 & 10100100000 \\
10100100000 & 10001000000 \\
10001000000 & 10000000000 \\
\end{pmatrix}
\times
\begin{pmatrix} 1 & 11111 \\
11111 & 10001 \\
10001 & 00101 \\
00101 & 11000 \\
11000 & 00011 \\
00011 & 10100 \\
10100 & 01010 \\
01010 & 11110 \\
\end{pmatrix}
\times
\begin{pmatrix} 1 & 11010 \\
11010 & 10100 \\
10100 & 10010 \\
10010 & 10000 \\
\end{pmatrix}
$$

over $GF(2^{5})$, $\beta^5 + \beta^4 + \beta^3 + \beta^2 + 1 = 0$. 

**LENGTH $m = 12$**

$GF(2^{12})$, $\alpha^{12} + \alpha^6 + \alpha^4 + \alpha + 1 = 0$, $\gamma = \alpha^{17}$.
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & \alpha^{197} & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{394} & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{788} & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{1576} \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \alpha^{3152} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{2209}
\end{pmatrix}
\times
\begin{pmatrix}
\Delta_1 & O \\
O & \Delta_1
\end{pmatrix}
\times
\begin{pmatrix}
100000000000 \\
00100000000 \\
00010000000 \\
00001000000 \\
00000100000 \\
00000010000 \\
00000001000 \\
00000000100 \\
00000000010 \\
00000000001
\end{pmatrix}
\times
\begin{pmatrix}
0100100101011 \\
1001001101111 \\
01111111111 \\
01111111111 \\
01110111111 \\
01011110100 \\
00011101100 \\
00001110100 \\
00000110100 \\
00000010100
\end{pmatrix}
\]

where

\[
\Delta_1 = \begin{pmatrix}
1 & \alpha^{520} & \alpha^{1040} & \alpha^{1560} & \alpha^{2080} & \alpha^{2600} \\
\alpha^{1040} & \alpha^{2080} & \alpha^{3120} & \alpha^{65} & \alpha^{1105} & \alpha^{1330} \\
\alpha^{1560} & \alpha^{3120} & \alpha^{2145} & \alpha^{65} & \alpha^{2210} & \alpha^{2210} \\
\alpha^{2080} & \alpha^{65} & \alpha^{195} & \alpha^{260} & \alpha^{325} & \alpha^{325} \\
\alpha^{1560} & \alpha^{3120} & \alpha^{2145} & \alpha^{260} & \alpha^{520} & \alpha^{520} \\
\alpha^{2080} & \alpha^{65} & \alpha^{195} & \alpha^{260} & \alpha^{520} & \alpha^{520} \\
\alpha^{2600} & \alpha^{1105} & \alpha^{1330} & \alpha^{325} & \alpha^{520} & \alpha^{780} \\
\end{pmatrix}
\]

\[
\Delta_2 = \begin{pmatrix}
1 & \alpha^{4510} & \alpha^{2925} \\
\alpha^{2925} & \alpha^{3510} & \alpha^{1755} \\
\alpha^{1755} & \alpha^{4510} & \alpha^{2925}
\end{pmatrix}^{-1}
\]

References


Sergei Valentinovich Fedorenko was born in St. Petersburg, U.S.S.R., in 1967. He received his Ph.D. degree in computer science and his Doctor of Technical Science degree from the St. Petersburg State University of Airspace Instrumentation, St. Petersburg, Russia, in 1994 and 2009, respectively.

Currently, he is a full Professor in the Information Systems Security Department, St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia, in 1994 and 2009, respectively. Prof. Fedorenko is the Alexander von Humboldt Foundation Research Fellow at the Technische Universität Darmstadt, Darmstadt, Germany.

His research interests include error-correcting codes, decoding algorithms, discrete Fourier transform over finite fields, fast algorithms, and communication systems.

Prof. Fedorenko was the Organizer (2008), the Vice-Chair (2008–2009), and the Chair (2010–2012) of the IEEE Russia, Russia (Siberia), and Russia (Northwest) Joint Sections Information Theory Society Chapter. Prof. Fedorenko was the Organizing Committee General Vice Chair (2007, 2009) and the Program Chair (2012) of the International Symposiums on Problems of Redundancy in Information and Control Systems at St. Petersburg, Russia.