FORMALIZED MATHEMATICS
2006, Vol. 14, No. 4, Pages 121–128
DOI: 10.2478/v10037-006-0015-y

Multiplication of Polynomials using Discrete Fourier Transformation

Krzysztof Treyderowski
Department of Computer Science
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk, Poland

Christoph Schwarzweller
Department of Computer Science
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk, Poland

Summary. In this article we define the Discrete Fourier Transformation for univariate polynomials and show that multiplication of polynomials can be carried out by two Fourier Transformations with a vector multiplication inbetween. Our proof follows the standard one found in the literature and uses Vandermonde matrices, see e.g. [27].

MML identifier: `POLYNOM8`, version: `7.8.03 4.75.958`

The articles [20], [26], [28], [5], [6], [19], [12], [3], [18], [13], [25], [2], [4], [23], [8], [24], [14], [10], [11], [16], [7], [29], [22], [1], [15], [9], [21], and [17] provide the notation and terminology for this paper.

1. Preliminaries

The following proposition is true

(1) Let n be an element of $\mathbb{N}$, L be a unital integral domain-like non degenerated non empty double loop structure, and x be an element of L. If $x \neq 0_L$, then $x^n \neq 0_L$.

ISSN 1426–2630

One can verify that every associative right unital add-associative right zeroed right complementable left distributive non empty double loop structure which is field-like is also integral domain-like.

The following four propositions are true:

(2) Let L be an add-associative right zeroed right complementable associative commutative left unital field-like distributive non empty double loop structure and x, y be elements of L. If $x \neq 0_L$ and $y \neq 0_L$, then $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$.

(3) Let L be an associative commutative left unital distributive field-like non empty double loop structure and z, z_1 be elements of L. If $z \neq 0_L$, then $z_1 = \frac{z_1 \cdot z}{z}$.

(4) Let L be a left zeroed right zeroed add-associative right complementable non empty double loop structure, m be an element of $\mathbb{N}$, and s be a finite sequence of elements of L. Suppose $\operatorname{len} s = m$ and for every element k of $\mathbb{N}$ such that $1 \leq k$ and $k \leq m$ holds $s_k = 1_L$. Then $\sum s = m \cdot 1_L$.

(5) Let L be an add-associative right zeroed right complementable associative commutative left unital distributive field-like non empty double loop structure, s be a finite sequence of elements of L, and q be an element of L. Suppose $q \neq 1_L$ and for every natural number i such that $1 \leq i$ and $i \leq \operatorname{len} s$ holds $s(i) = q^{i -' 1}$. Then $\sum s = \frac{1_L - q^{\operatorname{len} s}}{1_L - q}$.

Let L be a unital non empty double loop structure and let m be an element of $\mathbb{N}$. The functor m_L yielding an element of L is defined as follows:

(Def. 1) $m_L = m \cdot 1_L$.

Next we state several propositions:

(6) Let L be a field and m, n, k be elements of $\mathbb{N}$. Suppose $m > 0$ and $n > 0$. Let M_1 be a matrix over L of dimension $m \times n$ and M_2 be a matrix over L of dimension $n \times k$. Then $(m_L \cdot M_1) \cdot M_2 = m_L \cdot (M_1 \cdot M_2)$.

(7) Let L be a non empty zero structure, p be an algebraic sequence of L, and i be an element of $\mathbb{N}$. If $p(i) \neq 0_L$, then $\operatorname{len} p \geq i + 1$.

(8) For every non empty zero structure L and for every algebraic sequence s of L such that $\operatorname{len} s > 0$ holds $s(\operatorname{len} s - 1) \neq 0_L$.

(9) Let L be an add-associative right zeroed right complementable distributive commutative associative left unital integral domain-like non empty double loop structure and p, q be polynomials of L. If $\operatorname{len} p > 0$ and $\operatorname{len} q > 0$, then $\operatorname{len}(p * q) \leq \operatorname{len} p + \operatorname{len} q$.

(10) Let L be an associative non empty double loop structure, k, l be elements of L, and s_1 be a sequence of L. Then $k \cdot (l \cdot s_1) = (k \cdot l) \cdot s_1$.

2. Multiplication of Algebraic Sequences

Let L be a non empty double loop structure and let m_1, m_2 be sequences of L. The functor $m_1 \cdot m_2$ yields a sequence of L and is defined as follows:

(Def. 2) For every element i of $\mathbb{N}$ holds $(m_1 \cdot m_2)(i) = m_1(i) \cdot m_2(i)$.

Let L be an add-associative right zeroed right complementable left distributive non empty double loop structure and let m_1, m_2 be algebraic sequences of L. Observe that $m_1 \cdot m_2$ is finite-Support.

We now state two propositions:

(11) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and m_1, m_2 be algebraic sequences of L. Then $\operatorname{len}(m_1 \cdot m_2) \leq \min(\operatorname{len} m_1, \operatorname{len} m_2)$.

(12) Let L be an add-associative right zeroed right complementable distributive integral domain-like non empty double loop structure and m_1, m_2 be algebraic sequences of L. If $\operatorname{len} m_1 = \operatorname{len} m_2$, then $\operatorname{len}(m_1 \cdot m_2) = \operatorname{len} m_1$.

3. Powers in Double Loop Structures

Let L be an associative commutative left unital distributive field-like non empty double loop structure, let a be an element of L, and let i be an integer. The functor a^i yielding an element of L is defined as follows:

(Def. 3) $a^i = \begin{cases} \operatorname{power}_L(a, i), & \text{if } 0 \leq i, \\ \operatorname{power}_L(a, |i|)^{-1}, & \text{otherwise.} \end{cases}$

Next we state a number of propositions:

(13) Let L be an associative commutative left unital distributive field-like non empty double loop structure and x be an element of L. Then $x^0 = 1_L$.

(14) Let L be an associative commutative left unital distributive field-like non empty double loop structure and x be an element of L. Then $x^1 = x$.

(15) Let L be an associative commutative left unital distributive field-like non empty double loop structure and x be an element of L. Then $x^{-1} = x^{-1}$.

(16) Let L be an associative commutative left unital distributive field-like non degenerated non empty double loop structure and i be an integer. Then $(1_L)^i = 1_L$.

(17) Let L be an associative commutative left unital distributive field-like non empty double loop structure, x be an element of L, and n be an element of $\mathbb{N}$. Then $x^{n+1} = x^n \cdot x$ and $x^{n+1} = x \cdot x^n$.

(18) Let L be an add-associative right zeroed right complementable associative commutative left unital distributive field-like non degenerated non empty double loop structure, i be an integer, and x be an element of L. If $x \neq 0_L$, then $(x^i)^{-1} = x^{-i}$.

(19) For every field L and for every integer j and for every element x of L such that $x \neq 0_L$ holds $x^{j+1} = x^j \cdot x^1$.

(20) For every field L and for every integer j and for every element x of L such that $x \neq 0_L$ holds $x^{j-1} = x^j \cdot x^{-1}$.

(21) For every field L and for all integers i, j and for every element x of L such that $x \neq 0_L$ holds $x^i \cdot x^j = x^{i+j}$.

(22) Let L be a field-like associative unital add-associative right zeroed right complementable left distributive commutative non degenerated non empty double loop structure, k be an element of $\mathbb{N}$, and x be an element of L. If $x \neq 0_L$, then $(x^{-1})^k = x^{-k}$.

(23) Let L be a field and x be an element of L. Suppose $x \neq 0_L$. Let i, j, k be natural numbers. Then $x^{(i-1)\cdot(k-1)} \cdot x^{-(j-1)\cdot(k-1)} = x^{(i-j)\cdot(k-1)}$.

(24) Let L be an associative commutative left unital distributive field-like non empty double loop structure, x be an element of L, and n, m be elements of $\mathbb{N}$. Then $x^{n\cdot m} = (x^n)^m$.

(25) For every field L and for every element x of L such that $x \neq 0_L$ and for every integer i holds $(x^{-1})^i = (x^i)^{-1}$.

(26) For every field L and for every element x of L such that $x \neq 0_L$ and for all integers i, j holds $x^{i\cdot j} = (x^i)^j$.

(27) Let L be an associative commutative left unital distributive field-like non empty double loop structure, x be an element of L, and i, k be elements of $\mathbb{N}$. If $1 \leq k$, then $x^{i\cdot(k-1)} = (x^i)^{k-1}$.

4. Conversion between Algebraic Sequences and Matrices

Let m be a natural number, let L be a non empty zero structure, and let p be an algebraic sequence of L. The functor $\mathrm{mConv}(p, m)$ yielding a matrix over L of dimension $m \times 1$ is defined as follows:

(Def. 4) For every natural number i such that $1 \leq i$ and $i \leq m$ holds $(\mathrm{mConv}(p, m))_{i,1} = p(i - 1)$.

We now state two propositions:

(28) Let m be a natural number. Suppose $m > 0$. Let L be a non empty zero structure and p be an algebraic sequence of L. Then $\mathrm{len}\,\mathrm{mConv}(p, m) = m$ and $\mathrm{width}\,\mathrm{mConv}(p, m) = 1$ and for every natural number i such that $i < m$ holds $(\mathrm{mConv}(p, m))_{i+1,1} = p(i)$.

(29) Let m be a natural number. Suppose $m > 0$. Let L be a non empty zero structure, a be an algebraic sequence of L, and M be a matrix over L of dimension $m \times 1$. Suppose that for every natural number i such that $i < m$ holds $M_{i+1,1} = a(i)$. Then $\mathrm{mConv}(a, m) = M$.

Let L be a non empty zero structure and let M be a matrix over L. The functor aConv M yielding an algebraic sequence of L is defined by the conditions (Def. 5).

(Def. 5)(i) For every natural number i such that $i < \operatorname{len} M$ holds $(\mathrm{aConv}\, M)(i) = M_{i+1,1}$, and

(ii) for every natural number i such that $i \geq \operatorname{len} M$ holds $(\mathrm{aConv}\, M)(i) = 0_L$.

5. Primitive Roots, DFT and Vandermonde Matrix

Let L be a unital non empty double loop structure, let x be an element of L, and let n be an element of $\mathbb{N}$. We say that x is primitive root of degree n if and only if:

(Def. 6) $n \neq 0$ and $x^n = 1_L$ and for every element i of $\mathbb{N}$ such that $0 < i$ and $i < n$ holds $x^i \neq 1_L$.

We now state three propositions:

(30) Let L be a unital add-associative right zeroed right complementable right distributive non degenerated non empty double loop structure and n be an element of $\mathbb{N}$. Then 0_L is !not primitive root of degree n.

(31) Let L be an add-associative right zeroed right complementable associative commutative unital distributive field-like non degenerated non empty double loop structure, m be an element of $\mathbb{N}$, and x be an element of L. If x is primitive root of degree m, then x^{-1} is primitive root of degree m.

(32) Let L be an add-associative right zeroed right complementable associative commutative left unital distributive field-like non degenerated non empty double loop structure, m be an element of $\mathbb{N}$, and x be an element of L. Suppose x is primitive root of degree m. Let i, j be natural numbers. If $1 \leq i$ and $i \leq m$ and $1 \leq j$ and $j \leq m$ and $i \neq j$, then $x^{i-j} \neq 1_L$.

Let m be a natural number, let L be a unital non empty double loop structure, let p be a polynomial of L, and let x be an element of L. The functor $\mathrm{DFT}(p, x, m)$ yielding an algebraic sequence of L is defined by the conditions (Def. 7).

(Def. 7)(i) For every element i of $\mathbb{N}$ such that $i < m$ holds $(\mathrm{DFT}(p, x, m))(i) = \mathrm{eval}(p, x^i)$, and

(ii) for every element i of $\mathbb{N}$ such that $i \geq m$ holds $(\mathrm{DFT}(p, x, m))(i) = 0_L$.

The following propositions are true:

(33) Let m be a natural number, L be a unital non empty double loop structure, and x be an element of L. Then $\mathrm{DFT}(\mathbf{0}.\, L, x, m) = \mathbf{0}.\, L$.

(34) Let m be a natural number, L be a field, p, q be polynomials of L, and x be an element of L. Then $\mathrm{DFT}(p, x, m) \cdot \mathrm{DFT}(q, x, m) = \mathrm{DFT}(p * q, x, m)$.

Let L be an associative commutative left unital distributive field-like non empty double loop structure, let m be a natural number, and let x be an element of L. The functor Vandermonde(x, m) yielding a matrix over L of dimension m is defined as follows:

(Def. 8) For all natural numbers i, j such that $1 \leq i$ and $i \leq m$ and $1 \leq j$ and $j \leq m$ holds $(\mathrm{Vandermonde}(x, m))_{i,j} = x^{(i-1)\cdot(j-1)}$.

Let L be an associative commutative left unital distributive field-like non empty double loop structure, let m be a natural number, and let x be an element of L. We introduce $\mathrm{VM}(x, m)$ as a synonym of Vandermonde(x, m).

One can prove the following propositions:

(35) Let L be a field and m, n be natural numbers. Suppose $m > 0$. Let M be a matrix over L of dimension $m \times n$. Then $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_L^{m \times m} \cdot M = M$.

(36) Let L be a field and m be an element of $\mathbb{N}$. Suppose $0 < m$. Let u, v, u_1 be matrices over L of dimension m. Suppose that for all natural numbers i, j such that $1 \leq i$ and $i \leq m$ and $1 \leq j$ and $j \leq m$ holds $(u \cdot v)_{i,j} = m_L \cdot (u_1)_{i,j}$. Then $u \cdot v = m_L \cdot u_1$.

(37) Let L be a field, x be an element of L, s be a finite sequence of elements of L, and i, j, m be elements of $\mathbb{N}$. Suppose that x is primitive root of degree m and $1 \leq i$ and $i \leq m$ and $1 \leq j$ and $j \leq m$ and $\mathrm{len}\, s = m$ and for every natural number k such that $1 \leq k$ and $k \leq m$ holds $s_k = x^{(i-j)\cdot(k-1)}$. Then $(\mathrm{VM}(x, m) \cdot \mathrm{VM}(x^{-1}, m))_{i,j} = \sum s$.

(38) Let L be a field, m, i, j be elements of $\mathbb{N}$, and x be an element of L. Suppose $i \neq j$ and $1 \leq i$ and $i \leq m$ and $1 \leq j$ and $j \leq m$ and x is primitive root of degree m. Then $(\mathrm{VM}(x, m) \cdot \mathrm{VM}(x^{-1}, m))_{i,j} = 0_L$.

(39) Let L be a field and m be an element of $\mathbb{N}$. Suppose $m > 0$. Let x be an element of L. If x is primitive root of degree m, then $\mathrm{VM}(x, m) \cdot \mathrm{VM}(x^{-1}, m) = m_L \cdot \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_L^{m \times m}$.

(40) Let L be a field, m be an element of $\mathbb{N}$, and x be an element of L. If $m > 0$ and x is primitive root of degree m, then $\mathrm{VM}(x, m) \cdot \mathrm{VM}(x^{-1}, m) = \mathrm{VM}(x^{-1}, m) \cdot \mathrm{VM}(x, m)$.

6. DFT-Multiplication of Polynomials

We now state four propositions:

(41) Let L be a field, p be a polynomial of L, and m be an element of $\mathbb{N}$. Suppose $m > 0$ and $\operatorname{len} p \leq m$. Let x be an element of L and i be an element of $\mathbb{N}$. If $i < m$, then $(\mathrm{DFT}(p, x, m))(i) = (\mathrm{VM}(x, m) \cdot \mathrm{mConv}(p, m))_{i+1,1}$.

(42) Let L be a field, p be a polynomial of L, and m be a natural number. If $0 < m$ and $\operatorname{len} p \leq m$, then for every element x of L holds $\mathrm{DFT}(p, x, m) = \mathrm{aConv}(\mathrm{VM}(x, m) \cdot \mathrm{mConv}(p, m))$.

(43) Let L be a field, p, q be polynomials of L, and m be an element of $\mathbb{N}$. Suppose $m > 0$ and $\operatorname{len} p \leq m$ and $\operatorname{len} q \leq m$. Let x be an element of L. If x is primitive root of degree $2 \cdot m$, then $\mathrm{DFT}(\mathrm{DFT}(p*q, x, 2 \cdot m), x^{-1}, 2 \cdot m) = (2 \cdot m)_L \cdot (p * q)$.

(44) Let L be a field, p, q be polynomials of L, and m be an element of $\mathbb{N}$. Suppose $m > 0$ and $\operatorname{len} p \leq m$ and $\operatorname{len} q \leq m$. Let x be an element of L. Suppose x is primitive root of degree $2 \cdot m$. If $(2 \cdot m)_L \neq 0_L$, then $((2 \cdot m)_L)^{-1} \cdot \mathrm{DFT}(\mathrm{DFT}(p, x, 2 \cdot m) \cdot \mathrm{DFT}(q, x, 2 \cdot m), x^{-1}, 2 \cdot m) = p * q$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[4] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[7] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[9] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[10] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[11] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[12] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[13] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[14] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

[15] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[16] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[17] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

[18] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[19] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[20] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[21] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[22] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[24] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[25] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[27] J. von zur Gathen and J. Gerhard *Modern Computer Algebra*. Cambridge University Press, 1999.

[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[29] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received October 12, 2006