Linear transforms supporting circular convolution over a commutative ring with identity

M.M. Nessibi

Abstract. We consider a commutative ring R with identity and a positive integer N. We characterize all the 3-tuples $(\mathrm{L}_1, \mathrm{L}_2, \mathrm{L}_3)$ of linear transforms over R^{N}, having the "circular convolution" property, i.e. such that $x * y = \mathrm{L}_3(\mathrm{L}_1(x) \otimes \mathrm{L}_2(y))$ for all $x, y \in \mathrm{R}^{\mathrm{N}}$.

Keywords: circular convolution property

Classification: 15A04

1. Introduction

Let R be a commutative ring with identity, N a positive integer and $A = (a_{ij})$ $(0 \leq i, j \leq N-1)$ a square matrix of order N over R. The linear transform $L_A : R^{\mathrm{N}} \to R^{\mathrm{N}}$ defined by

$$L_A(x_0, x_1, \cdots, x_{\mathrm{N}-1}) = (y_0, y_1, \cdots, y_{\mathrm{N}-1}),$$

where $y_k = a_{k0}x_0 + a_{k1}x_1 + \cdots + a_{kN-1}x_{N-1}$ $(0 \leq k \leq N-1)$ is the linear transform over R^N with matrix A.

For the case R being the field $\mathbb{C}$ of complex numbers and $A = (a_{kl})$ the square matrix defined by

$$a_{kl} = (e^{-2i\pi \frac{kl}{N}}) \quad (0 \leq k, l \leq N-1),$$

the linear transform L_A is the discrete Fourier transform D. This transform is often used to compute the circular convolution product of two elements $x = (x_0, x_1, \cdots, x_{N-1})$ and $y = (y_0, y_1, \cdots, y_{N-1})$ of $\mathbb{C}^N$ as follows:

$$x * y = D^{-1}(D(x) \otimes D(y)), \tag{1}$$

where $D^{-1} = (\frac{1}{N} e^{+2i\pi \frac{kl}{N}})$ is the inverse discrete Fourier transform and

$$x \otimes y = (x_0y_0, x_1y_1, \cdots, x_{\mathrm{N}-1}y_{\mathrm{N}-1}), \tag{2}$$

$$x * y = (z_0, z_1, \cdots, z_{\mathrm{N}-1}), \tag{3}$$

where $z_k = \sum_{j=0}^{\mathrm{N}-1} x_j y_{k-j}$ $(0 \leq k \leq N-1)$ and $y_{k-j} = y_m$ for the integer m such that $m \equiv k-j \pmod N$ and $0 \leq m \leq N-1$. The discrete Fourier transform plays a key role in physics because it can be used as a mathematical tool to describe the relationship between the time domain and frequency domain representation of a discrete signal (see [5, p. 211]). In this paper, we characterize all 3-tuples (L_1, L_2, L_3) of linear transforms over R^{N}, having the "circular convolution" property, i.e. such that $x * y = \mathrm{L}_3(\mathrm{L}_1(x) \otimes \mathrm{L}_2(y))$ for all $x, y \in \mathrm{R}^{\mathrm{N}}$, where $*$ and $\otimes$ are defined as in (2) and (3).

This question for an integral domain and for the case $N = 2$ was completely solved by L. Skula in [3]. For the case $N \geq 3$, L. Skula gave in [3] a sufficient condition for linear transforms over a commutative ring with identity to have the "circular convolution" property. The converse direction (necessary condition) was established by P. Cikánek ([1, p. 74]). This gives another characterization of the linear transforms supporting circular convolution over a commutative ring R with identity.

In this work, by applying Theorem 2.2 we characterize all linear transforms supporting circular convolution over a residue class ring $\mathbb{Z}/m\,\mathbb{Z}$ for any integer $m \geq 2$.

In [4], L. Skula, by means of p-adic integers, described all linear transforms supporting circular convolution over a residue class ring $\mathbb{Z}/m\,\mathbb{Z}$, for any integer $m \geq 2$.

2. Characterization of linear transforms supporting circular convolution over R.

Definition 2.1. *Let $A = (a_{kl})$, $B = (b_{kl})$ and $C = (c_{kl})$ $(0 \leq k, l \leq N-1)$ be square matrices over the ring R. We say that the matrices A, B, C support circular convolution or briefly are SCC-matrices if for each u, v and w in $\{0, 1, \cdots, N-1\}$ the following relation holds:*

$$\sum_{k=0}^{\mathrm{N}-1} a_{ku} b_{kv} c_{kw} = \begin{cases} 1 & \text{for } \; u + v \equiv w \,(\operatorname{mod} N) \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.1. *The matrices A, B, C support circular convolution if and only if the 3-tuple (L_A, L_B, L_{C^*}) supports circular convolution, where $C^* = (c^*_{kl})$ is the square matrix of order N over R defined by*

$$c^*_{kl} = c_{lj} \quad (0 \leq k, l \leq N - 1)$$

with $0 \leq j \leq N - 1$ and $j \equiv -k \,(\operatorname{mod} N)$.
(See [3, p. 12–14]).

Proposition 2.1. *Let A, B, C be SCC-matrices over R. Then the determinants of A, B, C are not zero-divisors in R.*

Corollary 2.1. *Let A, B, C be SCC-matrices over R. We suppose that each non zero-divisor element of R is invertible. Then for each k $(0 \le k \le N-1)$ there exists $g_k \in R$ such that*

(1) $g_k^{\mathrm{N}} = 1$.
(2) $a_{ku} = g_k^u a_{k0}$, $b_{ku} = g_k^u b_{k0}$, $c_{ku} = g_k^u c_{k0}$ *for each* $u \in \{0, \cdots, \mathrm{N}-1\}$.
(3) *For each* $i, j \in \{0, \cdots, N-1\}$ *such that* $i \neq j$, $g_i - g_j$ *is not a zero-divisor in* R.

Corollary 2.2. *If $N.1$ is invertible in R and if there exist $g_0, \cdots, g_{\mathrm{N}-1} \in R$ such that*

(1) $g_k^{\mathrm{N}} = 1$ *for each* $k \in \{0, \cdots, N-1\}$.
(2)

$$\sum_{k=0}^{\mathrm{N}-1} g_k^m = \begin{cases} \mathrm{N} & \text{for } m \equiv 0 \pmod{\mathrm{N}}, \\ 0 & \text{otherwise.} \end{cases}$$

Then for each $i, j \in \{0, \cdots, N-1\}$ such that $i \neq j$, $(g_i - g_j)$ is not a zero-divisor in R.

Proposition 2.2. *Let $g_0, \cdots, g_{\mathrm{N}-1} \in R$ satisfying*

(1) $g_k^{\mathrm{N}} = 1$ *for each* $k \in \{0, \cdots, N-1\}$.
(2) $g_i - g_j$ *is not a zero-divisor in* R *for each* $i, j \in \{0, \cdots, N-1\}$ *such that* $i \neq j$.

Then we have

$$g_0 g_1 \cdot \cdots \cdot g_{\mathrm{N}-1} = (-1)^{\mathrm{N}-1}.$$

Proof: We denote by $D(g_0, \cdots, g_{\mathrm{N}-1})$ the Vandermonde determinant defined as follows:

$$D(g_0, \cdots, g_{\mathrm{N}-1}) = \begin{vmatrix} 1 & g_0 & \cdots & g_0^{\mathrm{N}-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g_{\mathrm{N}-1} & \cdots & g_{\mathrm{N}-1}^{\mathrm{N}-1} \end{vmatrix}.$$

Using the assertion (1) we obtain

$$D(g_0, \cdots, g_{\mathrm{N}-1}) = \begin{vmatrix} g_0 & \cdots & g_0^{\mathrm{N}-1} & g_0^{\mathrm{N}} \\ \vdots & \ddots & \vdots & \vdots \\ g_{\mathrm{N}-1} & \cdots & g_{\mathrm{N}-1}^{\mathrm{N}-1} & g_{\mathrm{N}-1}^{\mathrm{N}} \end{vmatrix}.$$

We deduce that

$$D(g_0, \cdots, g_{\mathrm{N}-1}) = (-1)^{\mathrm{N}-1} g_0 g_1 \cdots g_{\mathrm{N}-1} D(g_0, \cdots, g_{\mathrm{N}-1}).$$

The result follows from the last relation, the assertion (2) and the following equality:

$$D(g_0, \cdots, g_{\mathrm{N}-1}) = \prod_{0 \le i < j \le \mathrm{N}-1} (g_i - g_j).$$

□

Corollary 2.3. *Under the same hypothesis as in Proposition* 2.2 *we have*

(1) $D(g_0, \cdots, g_{\mathrm{N}-1}) = N g_r^s D_{rs}^* \ (0 \leq r, s \leq N-1)$, *where* D_{rs}^* *means the cofactor of the* r^{th} *row and the* s^{th} *column of the determinant* D.

(2)
$$\sum_{k=0}^{\mathrm{N}-1} g_k^m = \begin{cases} \mathrm{N} & \text{if } m \equiv 0 \ (\mathrm{mod}\, \mathrm{N}), \\ 0 & \text{otherwise.} \end{cases}$$

Using Corollaries 2.1–2.3 and considering the total quotient ring of R (see [6, p. 221]) we deduce the following theorem:

Theorem 2.2. *Let* A, B, C *be square matrices of order* N *over* R. *Then the following statements are equivalent:*

(1) *The matrices* A, B, C *support circular convolution.*

(2) $N\, a_{k0}\, b_{k0}\, c_{k0} = 1 \ (0 \leq k \leq N-1)$ *and there exist* $g_0, \cdots, g_{\mathrm{N}-1}$ *in* R *satisfying*

  (i) $g_k^{\mathrm{N}} = 1$ *for* $k \in \{0, \cdots, N-1\}$.

  (ii) $a_{ku} = g_k^u a_{k0}$, $b_{ku} = g_k^u b_{k0}$, $c_{ku} = g_k^u c_{k0} \ \ (0 \leq k, u \leq \mathrm{N}-1)$.

  (iii) *For each* i, j *in* $\{0, \cdots, N-1\}$ *such that* $i \neq j$, $(g_i - g_j)$ *is not a zero-divisor in* R.

Remark. For the case R being an integer domain, the condition (2) (iii) of Theorem 2.2 becomes $g_i \neq g_j$ for $i \neq j$ and we find the result of L. Skula [3, p. 20].

Theorem 2.3. *Let* $T = (t_{ij}) \ (0 \leq i, j \leq N-1)$ *be an invertible square matrix of order* N *over* R. *Then the following statements are equivalent:*

(1) *The matrices* T, T^{-1} *support circular convolution.*

(2) $N.1$ *is invertible in* R *and there exist* $g_0, \cdots, g_{\mathrm{N}-1}$ *in* R *such that*

  (i) $g_k^{\mathrm{N}} = 1$ *for* $k \in \{0, \cdots, N-1\}$.

  (ii) $t_{ku} = g_k^u \ \ (0 \leq k, u \leq \mathrm{N}-1)$.

  (iii) $(g_i - g_j)$ *is not a zero-divisor in* R *for each* i, j *in* $\{0, \cdots, N-1\}$ *such that* $i \neq j$.

Furthermore, $T^{-1} = (T_{ij}) \ (0 \leq i, j \leq \mathrm{N}-1)$ *with*
$$T_{ij} = (N.1)^{-1} g_j^{-i} \quad (0 \leq i, j \leq \mathrm{N}-1).$$

3. Matrices supporting circular convolution over a residue class ring $\mathbb{Z}/m\mathbb{Z}$, m integer ≥ 2

First we suppose that $m = p^n$, where n is a positive integer and p is a prime. In [3], [4] L. Skula showed that there exist SCC-matrices A, B, C of order N over the ring $\mathbb{Z}/p^n\mathbb{Z}$ if and only if N divides $p-1$. In [4] he described all the linear transforms supporting circular convolution over $\mathbb{Z}/p^n\mathbb{Z}$ by means of p-adic integers.

Using another method we give in this section another characterization of all the linear transforms supporting circular convolution over $\mathbb{Z}/p^n\mathbb{Z}$.

Theorem 3.1. *We suppose that N divides $(p-1)$. Let A, B, C be square matrices of order N over $\mathbb{Z}/p^n\,\mathbb{Z}$. The following statements are equivalent:*

(1) *The matrices A, B, C support circular convolution.*
(2) $N a_{k0} b_{k0} c_{k0} = 1$ *for* $k \in \{0, \cdots, N-1\}$ *and* $a_{ku} = g_k^u a_{k0}$, $b_{ku} = g_k^u b_{k0}$, $c_{ku} = g_k^u c_{k0}$ $(0 \le k, u \le \mathrm{N}-1)$, *where*

$$\{g_0, \cdots, g_{\mathrm{N}-1}\} = \{\alpha \in (\mathbb{Z}/p^n\,\mathbb{Z}) \mid \alpha^{\mathrm{N}} = 1\}.$$

Proof: By using the fact that the multiplicative group $(\mathbb{Z}/p^n\,\mathbb{Z})^*$ is cyclic (see [2, p. 55–58]) and by applying the Hensel's lemma (see [2, p. 169]) we deduce that if N divides $p-1$ we have the two following results:

- The set $H_n = \{x \in \mathbb{Z}/p^n\,\mathbb{Z} \mid x^{\mathrm{N}} = 1\}$ contains exactly N elements.
- For each $x, y \in H_n$ such that $x \neq y$, $x - y$ is not a zero-divisor in $\mathbb{Z}/p^n\,\mathbb{Z}$.

The result follows from these properties together with Theorem 2.2.

For general integer m; $m \ge 2$ we write $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $\alpha_1, \cdots, \alpha_r$ are positive integers and p_i $(1 \le i \le r)$ are primes such that $p_i \neq p_j$ for $i \neq j$. Hence we have

$$\mathbb{Z}/m\,\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\,\mathbb{Z}) \otimes \cdots \otimes (\mathbb{Z}/p_r^{\alpha_r}\,\mathbb{Z}).$$

We denote by Π_i $(1 \le i \le r)$ the canonical homomorphism from the ring $\mathbb{Z}/m\,\mathbb{Z}$ onto the ring $(\mathbb{Z}/p_i^{\alpha_i}\,\mathbb{Z})$. □

By using Theorem 3.1 and Proposition 2.6 in [3, p. 14] we deduce the following theorem:

Theorem 3.2. *Let A, B, C be square matrices of order N over $\mathbb{Z}/m\,\mathbb{Z}$. The following statements are equivalent:*

(1) *The matrices A, B, C support circular convolution.*
(2) $N\, a_{k0}\, b_{k0}\, c_{k0} = 1$ $(0 \le k \le N-1)$ *and there exist* $g_0, \cdots, g_{\mathrm{N}-1} \in (\mathbb{Z}/m\,\mathbb{Z})$ *such that*
   (i) $g_k^{\mathrm{N}} = 1$ *for* $k \in \{0, \cdots, N-1\}$.
   (ii) $a_{ku} = g_k^u a_{k0}$, $b_{ku} = g_k^u b_{k0}$, $c_{ku} = g_k^u c_{k0}$ $(0 \le k, u \le \mathrm{N}-1)$.
   (iii) $\Pi_i(g_k) \neq \Pi_i(g_l)$ *for each* k, l *in* $\{0, \cdots, N-1\}$ *such that* $k \neq l$.

Acknowledgments. I am grateful to Professor K. Trimèche for helpful comments. I thank the referee for his corrections and remarks.

References

[1] Cikánek P., *SCC matice nad komutativnim okruhem*, PhD-Thesis, Section 5, pp. 63–81, Brno, 1992.
[2] Hasse H., *Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1980.
[3] Skula L., *Linear transforms and convolution*, Math. Slovaca **37:1** (1987), 9–30.
[4] ———, *Linear transforms supporting circular convolution on residue class rings*, Math. Slovaca **39:4** (1989), 377–390.

[5] Nussbaumer H.T., *Fast Fourier transform and convolution algorithms*, Springer-Verlag, Berlin-Heidelberg-New York, 1981.
[6] Zarisky O., Samuel P., *Commutative Algebra*, Vol. 1, 1958, D. van Nostrand, Inc., Princeton, New Jersey, London.

Départment de Mathématiques, Facult e des Sciences de Tunis, 1060 Tunis, Tunisie

(*Received* May 27, 1994, *revised* November 21, 1994)