Ladislav Skula

Linear transforms and convolution

Mathematica Slovaca, Vol. 37 (1987), No. 1, 9--30

Persistent URL: http://dml.cz/dmlcz/136435

Math. Slovaca 37, 1987, No. 1, 9—30

LINEAR TRANSFORMS AND CONVOLUTION

LADISLAV SKULA

1. Introduction

In contemporary applications of mathematics *Convolutions* and *Discrete Fourier Transform* (*DFT*) are very often used. For the sequences $u = \{u_n\}_{n=0}^{N-1}$, $v = \{v_n\}_{n=0}^{N-1}$ of complex numbers with N members the sequence $u * v = w = \{w_l\}_{l=0}^{N-1}$ is called the *circular convolution of the sequences u and v* if

$$w_l = \sum_{n=0}^{N-1} u_n v_{l-n} \qquad (0 \leqslant l \leqslant N-1),$$

$v_{l-n} = v_m$ where $m \equiv l - n (\mathrm{mod}\, N)$ and $0 \leqslant m \leqslant N-1$.

The *discrete Fourier transform* $X = \{X_l\}_{l=0}^{N-1} = \mathrm{D}(x)$ *of a sequence* $x = \{x_n\}_{n=0}^{N-1}$ of complex numbers is defined by

$$X_l = \sum_{n=0}^{N-1} x_n W^{nl} \qquad (0 \leqslant l \leqslant N-1),$$

where $W = \cos\frac{2\pi}{N} - \mathrm{j}\sin\frac{2\pi}{N} (\mathrm{j} = \sqrt{-1})$.

The *inverse discrete Fourier transform* $X = \{X_n\}_{n=0}^{N-1} = \mathrm{D}^{-1}(x)$ *of a sequence* $x = \{x_l\}_{l=0}^{N-1}$ of complex numbers is defined by

$$X_n = \frac{1}{N} \sum_{l=0}^{N-1} x_l W^{-ln} \qquad (0 \leqslant n \leqslant N-1).$$

In modern computation techn que the circular convolution of the sequences u and v is often computed by means of the *DFT* as follows:

$$u * v = \mathrm{D}^{-1}(\mathrm{D}(u) \otimes \mathrm{D}(v))$$

($\otimes$ denotes component-wise multiplication).

The circular convolution is also computed by other transforms having this "*convolution property*", e.g. "*Number Theoretic Transforms*" (*NTT*). The book [6] by H. I. Nussbaumer deals with these topics and the collection of

papers [3] arranged by J. H. McClelan and Ch. M. Rader deals with the applications of number theory in this direction. There is a book [4] by V. Čížek on *Discrete Fourier Transform* in Czech.

The aim of our paper is to study all linear transforms having this "*convolution property*" in general over a commutative ring with identity. In paper [1] by R. C. Agarwal and Ch. S. Burrus this question is solved for special linear transforms over a commutative field (4.2).

We give an equivalent characteristic to the "*convolution property*" by means of "certain" condition on the matrices of these linear transforms in Paragraph 2 (2.5).

This question for a commutative field is completely solved in Paragraph 3 (3.6). In Paragraph 4 we give a complete solution for the integral domain (4.1) and for the case $N = 2$, where N is the length of the considered sequences (4.4). The case $N \geqslant 3$ is open in general.

In Paragraph 5 the linear transforms having the "*convolution property*" are investigated over a residue class ring modulo a prime power. It is shown that for this purpose the ring of p-adic integers is of great importance. By means of linear transforms with "*convolution property*" over the ring of p-adic integers we can construct linear transforms with this property over the residue class ring modulo p^n (p a prime, n a positive integer) (5.2). If this construction describes all these linear transforms over a residue class ring modulo prime power, it is open for $N \geqslant 3$.

2. Linear Transforms Supporting Circular Convolution

In the whole paper we shall denote by

R a commutative ring with identity element 1_R ($\neq 0_R$, the zero element of R) and

N a positive integer.

If c is an integer, we shall also consider c as the element $c \,.\, 1_R$ from the ring R, hence $c = c \,.\, 1_R$, $1 = 1_R$, $0 = 0 \,.\, 1_R = 0_R$, $N = N \,.\, 1_R$, e.t.c.

2.1. Definition. *A mapping L of the set of all sequences of length N of elements from the ring R into itself is called a linear transform (of the sequences of length N of elements from the ring R) if there exist $a_{ij} \in R$ $(0 \leqslant i, j \leqslant N-1)$ such that for each sequence $x = \{x_j\}_{j=0}^{N-1}$ $(x_j \in R)$ we have*

$$L(x) = y = \{y_i\}_{i=0}^{N-1} \qquad (y_i \in R)$$

with

$$y_i = \sum_{j=0}^{N-1} a_{ij} x_j \qquad (0 \leqslant i \leqslant N-1).$$

The matrix $\mathbf{A} = (a_{ij})_{0 \leqslant i,j \leqslant N-1}$ *is said to be the matrix of the linear transform L.*

The sequences of length N will often be considered as N-dimensional vectors, i.e. matrices of size $N \times 1$ over R. Hence, the sequence $x = \{x_j\}_{j=0}^{N-1}$ will be considered as the vector

$$x = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix}.$$

The value x_j will be extended onto all integer-indices in the following way: $x_m = x_k$ for an integer m, where $0 \leqslant k \leqslant N-1$, $m \equiv k (\mathrm{mod}\ N)$.

Then the equality $L(x) = y$ can be written in the form:

$$y = \mathbf{A} \,.\, x.$$

2.2. Definition. *Let*

$$u = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{N-1} \end{bmatrix}, \qquad v = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix}$$

be N-dimensional vectors over R. By the product of the vectors u and v we understand the vector

$$u \otimes v = \begin{bmatrix} u_0 v_0 \\ u_1 v_1 \\ \vdots \\ u_{N-1} v_{N-1} \end{bmatrix}.$$

The vector or the sequence

$$u * v = \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{N-1} \end{bmatrix}$$

is called the circular convolution of the vectors or the sequences u and v if for each $0 \leqslant l \leqslant N-1$ *we have*

$$w_l = \sum_{n=0}^{N-1} u_n v_{l-n}.$$

2.3. Definition. *Let* L_1, L_2, L_3 *be linear transforms of the sequences of length N of elements from the ring R. We say that the* 3*-tuple* (L_1, L_2, L_3) *supports*

circular convolution or briefly it is (SCC) if for each sequence x_1 and each sequence x_2 of length N of elements from the ring R the equality

$$x_1 * x_2 = L_3(L_1(x_1) \otimes L_2(x_2))$$

is satisfied.

2.4. Notation. For $0 \leqslant t \leqslant N-1$ put

$$x(t) = \begin{bmatrix} x_{t0} \\ x_{t1} \\ \vdots \\ x_{tN-1} \end{bmatrix},$$

where for $0 \leqslant u \leqslant N-1$ we have

$$x_{tu} = \begin{cases} 1_R & \text{for } t = u \\ 0_R & \text{otherwise.} \end{cases}$$

2.5. Theorem. *Let L_1, L_2, L_3 be linear transforms of the sequences of length N of elements from the ring R and let $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (C_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ be their matrices. Then the following statements are equivalent:*

(a) The 3-tuple (L_1, L_2, L_3) supports circular convolution.

(b) For each $0 \leqslant u, v \leqslant N-1$ the following is satisfied:

$$x(u) * x(v) = L_3(L_1(x(u)) \otimes L_2(x(v))).$$

(c) For each $0 \leqslant u, v, w \leqslant N-1$ there holds:

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

Proof. Clearly (a) implies (b).

I. Let (b) hold and let $0 \leqslant u, v, w \leqslant N-1$.

Put

$y_1 = L_1(x(u))$, $y_2 = L_2(x(v))$, $y_3 = y_1 \otimes y_2$, $y = L_3(y_3)$,

$$y_1 = \begin{bmatrix} y_{10} \\ \vdots \\ y_{1N-1} \end{bmatrix}, \qquad y_2 = \begin{bmatrix} y_{20} \\ \vdots \\ y_{2N-1} \end{bmatrix},$$

$$y_3 = \begin{bmatrix} y_{30} \\ \vdots \\ y_{3N-1} \end{bmatrix}, \qquad y = \begin{bmatrix} y_0 \\ \vdots \\ y_{N-1} \end{bmatrix},$$

Then for $0 \leqslant k \leqslant N-1$ we have

$$y_{1k} = a_{ku}, \qquad y_{2k} = b_{kv}, \qquad y_{3k} = a_{ku} . b_{kv},$$

hence

$$y_w = \sum_{k=0}^{N-1} a_{ku} b_{kv} c_{wk} .$$

Since $y = x(u) * x(v)$, there holds

$$y_w = \sum_{n=0}^{N-1} x_{un} x_{vw-n} = x_{vw-u} = \begin{cases} 1_R & \text{for } w - u \equiv v (\text{mod } N) \\ 0_R & \text{otherwise.} \end{cases}$$

Therefore (c) is valid.

II. Let (c) hold and let

$$x_1 = \begin{bmatrix} x_{10} \\ \vdots \\ x_{1N-1} \end{bmatrix}, \qquad x_2 = \begin{bmatrix} x_{20} \\ \vdots \\ x_{2N-1} \end{bmatrix}$$

be N-dimensional vectors over R.

Put

$$y_1 = L_1(x_1) = \begin{bmatrix} y_{10} \\ \vdots \\ y_{1N-1} \end{bmatrix}, \qquad y_2 = L_2(x_2) = \begin{bmatrix} y_{20} \\ \vdots \\ y_{2N-1} \end{bmatrix},$$

$$y_3 = y_1 \otimes y_2 = \begin{bmatrix} y_{30} \\ \vdots \\ y_{3N-1} \end{bmatrix}, \qquad y = L_3(y_3) = \begin{bmatrix} y_0 \\ \vdots \\ y_{N-1} \end{bmatrix}.$$

Then we have for each $0 \leqslant k \leqslant N-1$

$$y_{3k} = y_{1k} \cdot y_{2k} = \sum_{u=0}^{n-1} \sum_{v=0}^{N-1} a_{ku} b_{kv} x_{1u} x_{2v} .$$

For $0 \leqslant w \leqslant N-1$ there holds:

$$y_w = \sum_{k=0}^{N-1} c_{wk} y_{3k} = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} x_{1u} x_{2v} \sum_{k=0}^{N-1} a_{ku} b_{kv} c_{wk} =$$

$$= \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} x_{1u} x_{2v} (w \equiv u + v (\text{mod } N))$$

$$= \sum_{u=0}^{N-1} x_{1u} x_{2w-u} .$$

Hence $y = x_1 * x_2$ and the statement (c) is valid.

The Theorem is proved.

Suppose that the ring R is the direct sum of rings $R_\iota (\iota \in I)$, p_ι is the projection from R onto R_ι and L is a linear transform of the sequences of elements from

R of length N with matrix $\mathbf{A} = (a_{ij})$. Denote by L_t the linear transform of the sequences of elements from R_t of length N whose matrix is $\mathbf{A}_t = (p_t(a_{ij}))$. (Under the *direct sum of the rings* R_t $(t \in I)$ we understand the set R that equals the cartesian product of the sets R_t $(t \in I)$ and the operations are defined componentwise). From Theorem 2.5 we obtain immediately:

2.6. Proposition. *Let* L_1, L_2, L_3 *be linear transforms of the sequences of elements from* R *of length* N *and let* R *be the direct sum of the rings* R_t $(t \in I)$.

Then the 3*-tuple* (L_1, L_2, L_3) *is* (*SCC*) *if and only if the* 3*-tuple* (L_{1t}, L_{2t}, L_{3t}) *is* (*SCC*) *for each* $t \in I$.

Further let I be and ideal of the ring R and L be a linear transform of the sequences of elements from R of length N with matrix $\mathbf{A} = (a_{ij})$. We denote by $\bar{a}$ the coset of I containing $a \in R$ and by L the linear transform of the sequences of elements from the quotient ring R/I with the matrix $\bar{\mathbf{A}} = (\bar{a}_{ij})$.

We get from Theorem 2.5. Immediately:

2.7. Proposition. *Let* L_1, L_2, L_3 *be linear transforms of the sequences of elements from* R *of length* N *and let* I *be an ideal of the ring* R. *If the* 3*-tuple* (L_1, L_2, L_3) *is* (*SCC*), *then the* 3*-tuple* $(\bar{L}_1, \bar{L}_2, \bar{L}_3)$ *of linear transforms of the sequences of elements from the quotient ring* R/I *is* (*SCC*).

2.8. Definition. *Let* $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (c_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ *be quadratic matrices of order* N *over the ring* R. *We say that the matrices* **A**, **B**, **C** *support circular convolution or briefly are SCC-matrices if for each* $0 \leqslant u, v, w \leqslant N-1$ *the following relation holds*:

$$\sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} = \begin{cases} 1_R & \text{for } u + v + w \equiv 0 \pmod{N} \\ O_R & \text{otherwise.} \end{cases}$$

We denote by $\mathbf{C}^*$ the quadratic matrix (d_{ij}) $(0 \leqslant i, j \leqslant N-1)$ of order N over R, where $d_{ij} = c_{jk}$, $0 \leqslant k \leqslant N-1$, $k \equiv -i \pmod{N}$. Let $L_{\mathbf{A}}$, $L_{\mathbf{B}}$, $L_{\mathbf{C}^*}$ be linear transforms with the matrices **A**, **B**, $\mathbf{C}^*$. Then we obtain from Theorem 2.5:

2.9. Proposition. *The matrices* **A**, **B**, **C** *support circular convolution if and only if the* 3*-tuple* $(L_{\mathbf{A}}, L_{\mathbf{B}}, L_{\mathbf{C}^*})$ *supports circular convolution.*

2.10. Remark. The given change of the transform $L_{\mathbf{C}^*}$ into the matrix **C** has the meaning that the matrices **A**, **B**, **C** have symmetrical functions in the definition of *SCC*-matrices. If we then prove an assertion for some of these

matrices, this assertion also holds for the others. Further we remark that $(\mathbf{C}^*)^* = \mathbf{C}$.

3. SCC-Matrices over a Field

In this paragraph we give a description of all matrices **A**, **B**, **C** over a (commutative) field supporting circular convolution.

We denote by

F a (commutative) field

and

$$\mathbf{A} = (a_{ij}),\ \mathbf{B} = (b_{ij}),\ \mathbf{C} = (c_{ij}) \qquad (0 \leqslant i, j \leqslant N-1)$$

quadratic matrices of order N over F.

For $0 \leqslant i, j \leqslant N-1$ we denote by $A^*(i, j)$ the cofactor of the element a_{ij} in the determinant of **A**. (For $N = 1$ we define $A^*(0, 0) = 1$.)

If n is an integer, we put $A^*(i, n) = A^*(i, j)$, where $0 \leqslant j \leqslant N-1$ and $n \equiv j \pmod N$.

3.1. Proposition. *For SCC-matrices* **A**, **B**, **C** *the following assertions are valid*:

(*a*) $\det \mathbf{A} \,.\, \det \mathbf{B} \,.\, \det \mathbf{C} \neq 0$,

(*b*) $(\det \mathbf{A}) \,.\, b_{kv} \,.\, c_{kw} = A^*(k, -v-w)$ *for each* $0 \leqslant k, v, w \leqslant N-1$,

(*c*) $a_{ij} \,.\, b_{ij} \,.\, c_{ij} \,.\, A^*(i, j) \neq 0$ *for each* $0 \leqslant i, j \leqslant N-1$.

Proof. I. Suppose $\det \mathbf{A} = 0$. Then there exist elements $f_i \in F$ $(0 \leqslant i \leqslant N-1)$ and an integer u $(0 \leqslant u \leqslant N-1)$ such that $f_u \neq 0$ and

$$\sum_{i=0}^{N-1} f_i a_{ki} = 0$$

is valid for each $0 \leqslant k \leqslant N-1$.

From this relation we get

$$\sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} = -\sum_{\substack{i=0 \\ i \neq u}}^{N-1} f_u^{-1} f_i \sum_{k=0}^{N-1} a_{ki} b_{kv} c_{kw}$$

for each $0 \leqslant v, w \leqslant N-1$.

Let $v \equiv -u \pmod N$ and $w = 0$. Then $i + v + w \equiv i - u \not\equiv 0 \pmod N$ for $i \neq u$ and $0 \leqslant i \leqslant N-1$, therefore for this i we have

$$\sum_{k=0}^{N-1} a_{ki} b_{kt} c_{kw} = 0.$$

Since $u + v + w \equiv 0 (\mathrm{mod}\ N)$, we obtain

$$1 = \sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} = 0,$$

which is a contradiction.

Thus $\det \mathbf{A} \neq 0$ and by reason of symmetry also $\det \mathbf{B}$, $\det \mathbf{C} \neq 0$.

II. Let $0 \leqslant v, w \leqslant N-1$. Put $x_k = b_{kv} c_{kw}$ for each $0 \leqslant k \leqslant N-1$. Then for each $0 \leqslant u \leqslant N-1$ we have

$$\sum_{k=0}^{N-1} a_{ku} x_k = \begin{cases} 1 & \textit{for } \mathrm{u} + \mathrm{v} + \mathrm{w} \equiv 0 (\mathrm{mod}\ N) \\ 0 & \text{otherwise.} \end{cases}$$

Since $\det A \neq 0$, we obtain from the *Cramer Theorem* $(\det \mathbf{A}) . x_k = A^*(k, -v - w)$.

III. Let $0 \leqslant k, w \leqslant N-1$ and $c_{kw} = 0$. It follows from (b) that $A^*(k, h) = 0$ for each integer h, hence $\det \mathbf{A} = 0$, which is a contradiction to (a). Thus $c_{ij} \neq 0$ $(0 \leqslant i, j \leqslant N-1)$ and by reason of symmetry also $a_{ij}, b_{ij} \neq 0$. From (a) and (b) we then get $A^*(i, j) \neq 0$.

3.2. Proposition. *Let* $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *be SCC-matrices. Then for each* $0 \leqslant k \leqslant N-1$ *there exist elements* $a_k, b_k, c_k, g_k \in F$ *such that*

$$g_k^N = 1$$

and

$$a_{kh} = g_k^h a_k,\ b_{kh} = g_k^h b_k,\ c_{kh} = g_k^h c_k$$

for each $0 \leqslant h \leqslant N-1$.

Proof. Let $0 \leqslant k \leqslant N-1$. For an integer n and for an integer h $(0 \leqslant h \leqslant N-1)$ put

$$\alpha_n = A^*(k, -n) . (\det \mathbf{A})^{-1},\ \beta_h = b_{kh},\ \gamma_h = c_{kh}.$$

According to 3.1 (c) the elements $\alpha_n, \beta_h, \gamma_h$ differ from 0 and according to 3.1 (b) we have for integers v, w $(0 \leqslant v, w \leqslant N-1)$:

$$\alpha_{v+w} = \beta_v \gamma_w .$$

It follows that $\alpha_0 = \beta_0 \gamma_0$, $\beta_v = \alpha_v \gamma_0^{-1}$, $\gamma_w = \alpha_w \beta_0^{-1}$, therefore

$$\beta_v = \alpha_v \beta_0 \alpha_0^{-1}, \qquad \gamma_w = \alpha_w \gamma_0 \alpha_0^{-1},$$
$$\alpha_{v+w} = \alpha_v \alpha_w \alpha_0^{-1}.$$

From this we easily derive by mathematical induction that for each integer n $(0 \leqslant n \leqslant N)$

$$\alpha_n = \left(\frac{\alpha_1}{\alpha_0}\right)^n . \alpha_0$$

and it follows that for each integer h $(0 \leqslant h \leqslant N-1)$ we have

$$\beta_h = \left(\frac{\alpha_1}{\alpha_0}\right)^h \cdot \beta_0, \quad \gamma_h = \left(\frac{\alpha_1}{\alpha_0}\right)^h \cdot \gamma_0.$$

Put $g_k = \dfrac{\alpha_1}{\alpha_0}$, $b_k = \beta_0$, $c_k = \gamma_0$. Then $\alpha_0 = \alpha_N = g_k^N \alpha_0$, thus $g_k^N = 1$. Further we have $b_{kh} = \beta_h = g_k^h b_k$ and $c_{kh} = \gamma_h = g_k^h c_k$. By reason of symmetry we also obtain $a_{kh} = g_k^h a_k$, where a_k is an element from F.

Four our next investigation we shall need the following assertion, which is essentially known in algebra, but in spite of it we give its proof.

3.3. Proposition. *Let the polynomial $x^N - 1$ have N different roots in the field F. Then*

(a) there exists $\zeta \in F$ such that $\{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\}$ is the set of all roots of the polynomial $x^N - 1$ in the field F,

(b) char *F does not divide the integer N,*

(c) for an integer m the equality

$$\sum_{k=0}^{N-1} \zeta^{km} = \begin{cases} N & \text{for } m \equiv 0 (\mathrm{mod}\ N) \\ 0 & \text{otherwise} \end{cases}$$

is valid.

(The symbol char F means the characteristic of the field F.)

Proof. I. Let R' be the set of all roots of the polynomial $x^N - 1$ in the field F and let $\bar{R}$ be the set of all orders of elements from R'. If $\varrho \in R'$ and r is the order of ϱ, then the elements $1, \varrho, \varrho^2, \ldots, \varrho^{r-1}$ are different and form the set of all roots of the polynomial $x^r - 1$ *in* F. It follows that the set

$$M(r) = \{\varrho^x : 1 \leqslant x \leqslant r;\ x, r \text{ are relatively prime}\}$$

is the set of all elements from R' of order r and the number $|M(r)|$ of elements of the set $M(r)$ equals $\varphi(r)$, where φ means the *Euler function.*

Let P mean the subset of elements of the set R' of order $< N$ and let M be the number of elements of P. Since each $r \in \bar{R}$ divides N, we have

$$M = \sum |M(r)| \ (r \in P) = \sum \varphi(r) \ (r \in \bar{R} - \{N\}) \leqslant$$

$$\leqslant \sum \varphi(d) \ (1 \leqslant d < N,\ d \text{ divides } N) =$$

$$= N - \varphi(N)$$

(we have used the equality $\Sigma(d)$ $(1 \leqslant d \leqslant N, d$ divides $N) = N$). Since $\varphi(N) \geqslant 1$, we have $M < N$, therefore there exists an element $\zeta \in R'$ with order N. The set $\{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\}$ is then the set of all roots of the polynomial $x^N - 1$ in the field$F$.

II. Let the prime p be the characteristic of F, $N = pM$, where M is a positive integer. The elements ζ^{Mi} $(0 \leqslant i \leqslant p-1)$ are different and therefore

$$x^p - 1 = \prod (x - \zeta^{Mi}) \quad (0 \leqslant i \leqslant p-1).$$

On the other hand we have $x^P - 1 = (x-1)^P$, which is a contradiction. Hence char F does not divide N.

III. Let $m \equiv 0 \pmod{N}$. Then $\zeta^{km} = 1$ for every integer k, thus

$$\sum_{k=0}^{N-1} \zeta^{km} = N.$$

Let $m \not\equiv 0 \pmod{N}$. Then $\zeta^m \neq 1$ and we have $(\zeta^m - 1) \sum_{k=0}^{N-1} \zeta^m = \zeta^{Nm} - 1 = 0$, therefore

$$\sum_{k=0}^{N-1} \zeta^{km} = 0.$$

Recall that for $x_0, x_1, \ldots, x_{N-1} \in F$ the determinant

$$D = D(x_0, x_1, \ldots, x_{N-1}) = \begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^{N-1} \\ 1 & x_1 & x_1^2 & \ldots & x_1^{N-1} \\ \vdots & & & & \\ 1 & x_{N-1} & x_{N-1}^2 & \ldots & x_{N-1}^{N-1} \end{vmatrix}$$

is called the *Vandermonde determinant* and there holds

$$D = \prod (x_i - x_j) \quad (0 \leqslant j < i \leqslant N-1) \quad \text{for } N > 1$$
$$D = 1 \quad \text{for } N = 1.$$

For $0 \leqslant r, s \leqslant N-1$ let D_{rs}^* mean the cofactor of the element in the rth row and the sth column of the determinant D (for $N = 1$ we define $D_{00}^* = 1$). Then we have

3.4. Proposition. *Let $x_0, x_1, \ldots, x_{N-1}$ be different elements of the field F with the property $x_i^N = 1$ $(0 \leqslant i \leqslant N-1)$. Then there holds for $0 \leqslant r, s \leqslant N-1$*

$$D = N x_r^s D_{rs}^*.$$

Proof. We can suppose $N \leqslant 2$. Put $X = x_0 x_1 \ldots x_{r-1} x_{r+1} \ldots x_{N-1}$. We have

$$D^*_{rs} = (-1)^{r+s} \begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^{s-1} & x_0^{s+1} & \ldots & x_0^{N-1} \\ 1 & x_1 & & & & & & \\ \vdots & & & & & & & \\ 1 & x_{r-1} & & & & \ldots & & \\ 1 & x_{r+1} & & & & & & \\ \vdots & & & & & & & \\ 1 & x_{N-1} & & & & & & x_{N-1}^{N-1} \end{vmatrix} =$$

$$= (-1)^{r+s+(N-1-s)s} \begin{vmatrix} x_0^{s+1} & x_0^{s+2} & \ldots & x_0^{N+s-1} \\ \vdots & & & \\ x_{r-1}^{s+1} & & & \\ x_{r+1}^{s+1} & & \ldots & \\ \vdots & & & \\ x_{N-1}^{s+1} & & & x_{N-1}^{N+s-1} \end{vmatrix}$$

$$= (-1)^{r+s+Ns} X^{s+1} D(x_0, x_1, \ldots, x_{r-1}, x_{r+1}, \ldots, x_{N-1})$$

$$= (-1)^{r+s+Ns} X^{s+1} \prod (x_i - x_j) \; (0 \leqslant j < i \leqslant N-1, \; i \neq r \neq j).$$

Thus

$$D^*_{rs} \prod (x_r - x_j) \; (0 \leqslant j \leqslant N-1, j \neq r) = (-1)^{r+s+Ns+N-1-r} X^{s+1} D.$$

Since $x^N - 1 = (x - x_0)\ (x - x_1)\ldots(x - x_{N-1})$, we have $x_0 . x_1 \ldots x_{N-1} = (-1)^{N-1}$, therefore $X = (-1)^{N-1} . x_r^{-1}$. If we put $X_r = x_r \prod (x_r - x_j) \times$ $\times \; (0 \leqslant j \leqslant N-1, j \neq r)$, we obtain

$$D^*_{rs} X_r x_r^s = D,$$

thus

$$ND = \sum_{s=0}^{N-1} D^*_{rs} X_r x_r^s = X_r D.$$

It follows that $N = X_r$ and hence $D = N x_r^s D^*_{rs}$.

3.5. Proposition. *Let* **A**, **B**, **C** *be SCC-matrices. Then* using notation of 3.2 *we have*:

(*a*) *the elements* g_k $(0 \leqslant k \leqslant N-1)$ *are different*,

(*b*) char F *does not divide the integer* N,

(*c*) $Na_k b_k c_k = 1$ *for each* $0 \leqslant k \leqslant N-1$.

Proof. I. According to 3.2 $\det \mathbf{A} = a_0 a_1 \ldots a_{N-1} D(g_0, g_1, \ldots, g_{N-1}) = a_0 a_1 \ldots \ldots a_{N-1} \prod (g_i - g_j)$ $(0 \leqslant j < i \leqslant N-1)$. Since $\det \mathbf{A} \neq 0$ (3.1 (a)), the elements g_k $(0 \leqslant k \leqslant N-1)$ are different.

II. According to I and 3.3 (b) char F does not divide N as by 3.2 $g_k^N = 1$.

III. Let $0 \leqslant k \leqslant N-1$. According to (3.1) (b)

$$(\det \mathbf{A})\, b_{k0} c_{k0} = A^*(k, 0).$$

From 3.2 and 3.4 we obtain

$$\det \mathbf{A} = a_0 a_1 \ldots a_{N-1} D(g_0, g_1, \ldots, g_{N-1}) = a_k N A^*(k, 0),$$

therefore

$$N a_k b_k c_k A^*(k, 0) = A^*(k, 0)$$

and since $A^*(k, 0) \neq 0$ (3.1 (c)), we have $N a_k b_k c_k = 1$.

3.6. Main theorem. *The following statement are equivalent*:

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

(*b*) *For each* $0 \leqslant k \leqslant N-1$ *there exist* $a_k, b_k, c_k, g_k \in F$ *such that*

(α) $g_k^N = 1$,

(β) $N a_k b_k c_k = 1$,

(γ) *the elements* g_k $(0 \leqslant k \leqslant N-1)$ *are different,*

(δ) $a_{kh} = g_k^h a_k$, $b_{kh} = g_k^h b_k$, $c_{kh} = g_k^h c_k$ *for each* $0 \leqslant h \leqslant N-1$.

Proof. If the statement (a) holds, then according to 3.2 and 3.5 the statement (b) also holds.

Let (b) hold and let $0 \leqslant u, v, w \leqslant N-1$, $m = u + v + w$. Then according to 3.3 (a) there exists $\zeta \in F$ such that $\{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\} = \{g_0, g_1, \ldots, g_{N-1}\}$. We get according to 3.3 (c)

$$N \sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} = N \sum_{k=0}^{N-1} a_k b_k c_k g_k^m =$$

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

Since char$F$ does not divide N (3.3 (b)), we have

$$\sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} = 1$$

for $u + v + w \equiv 0 \,(\mathrm{mod}\, N)$.

The Theorem is proved.

3.7. Example. The *Discrete Fourier Transform* (*DFT*) is a linear transform D of the sequences of elements from the field of complex numbers of length N,

whose matrix $\mathbf{A}$ has the form

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & & \dots & 1 \\ 1 & W & W^2 & \dots & W^{N-1} \\ \vdots & \vdots & W^{kj} & & \\ 1 & W^{N-1} & & & W^{(N-1)^2} \end{bmatrix} \qquad (0\ k, j \leqslant N-1),$$

where $W = \cos\frac{2\pi}{N} - \mathrm{j}\sin\frac{2\pi}{N}$ ($\mathrm{j} = \sqrt{-1}$). The *Inverse Discrete Fourier Transform* D^{-1} is a linear transform with the matrix

$$\mathbf{A}^{-1} = (N^{-1}W^{-kj})\ (0 \leqslant k, j \leqslant N-1).$$

It is well known that *the 3-tuple* (D, D, D^{-1}) *supports circular convolution.*

If $\mathbf{C} = (c_{ij}) = (\mathbf{A}^{-1})^*$, then $c_{ij} = N^{-1}W^{ij}$. *The matrices* $\mathbf{A}$, $\mathbf{A}$, $\mathbf{C}$ *support circular convolution.*

4. Some Other Cases

From the Main Theorem 3.6 we derive the analogous Theorem for *SCC*-matrices over an integral domain:

4.1. Theorem. *Let* $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (c_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ *be quadratic matrices of order N over an integral domain D. Then the following statements are equivalent*:

(*a*) *The matrices* $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ *support circular convolution.*

(*b*) *For each* $0 \leqslant k \leqslant N-1$ *there exist* $a_k, b_k, c_k, g_k \in D$ *such that*

(α) $g_k^N = 1$,

(β) $Na_kb_kc_k = 1$,

(γ) *the elements* g_k $(0 \leqslant k \leqslant N-1)$ *are different,*

(δ) $a_{kh} = g_k^h a_k$, $b_{kh} = g_k^h b_k$, $c_{kh} = g_k^h c_k$

for each $0 \leqslant h \leqslant N-1$.

Proof. Let F be the quotient field of D. According to 3.6 the statement (a) follows immediately from (b).

Let $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ support circular convolution. According to 3.6 there exist $a_k, b_k, c_k, g_k \in F$ $(0 \leqslant k \leqslant N-1)$ fulfilling the conditions (α) – (δ) in the statement (b). We must show that these elements a_k, b_k, c_k, g_k belong to D.

Put $h = 0$ in (δ). Then $a_k = a_{k0} \in D$ and analogously $b_k \in D$ and $c_k \in D$. For $h = 1$ we have $a_{k1} = g_k a_k$ and by multiplication of this equality by the element Nb_kc_k we get $g_k = Na_kb_kc_kg_k = Nb_kc_ka_{k1} \in D$.

The Theorem is proved.

The paper [1] deals with the case when $\mathbf{A} = \mathbf{B} = \mathbf{T}$ is a regular matrix and $\mathbf{C}^* = \mathbf{T}^{-1}$. The following theorem (slightly adapted) is given in this paper:

4.2. Theorem. (*Agarwal, Burrus*). *Let* $\mathbf{T} = (t_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ *be a regular matrix of order N over a (commutative) field F. Let L and* L^{-1} *be linear transforms with matrices* $\mathbf{T}$ *and* $\mathbf{T}^{-1}$, *respectively. Then the following statements are equivalent*:

(*a*) *The 3-tuple* (L, L, L^{-1}) *supports circular convolution.*

(*b*) *For* $0 \leqslant k \leqslant N-1$ *there exist different* $g_k \in F$ *such that* $g_k^N = 1$ *and for* $0 \leqslant h \leqslant N-1$

$$t_{kh} = g_k^h,$$

and char *F does not divide N.*

Then for $\mathbf{T}^{-1} = (\bar{t}_{kh})$ $(0 \leqslant k, h \leqslant N-1)$ *we have*

$$\bar{t}_{kh} = N^{-1} g_h^{-k}.$$

Proof. Recall that the condition "char *F does not divide N*" is equivalent to the condition "*N has an inverse in F*". Then this inverse will be denoted by N^{-1}.

Put $\mathbf{A} = \mathbf{B} = \mathbf{T} = (t_{ij})$, $\mathbf{C} = (c_{ij}) = (\mathbf{T}^{-1})^* = (\bar{t}_{ij})^*$ $(0 \leqslant i, j \leqslant N-1)$, hence $\bar{t}_{ij} = c_{jl(i)}$ where $l(i) \equiv -i (\mathrm{mod}\ N)$, $0 \leqslant l(i) \leqslant N-1$. The statement (a) is equivalent to the statement: "**A**, **B**, **C** *are SCC-matrices*". If this holds, then according 3.6 there exist $a_k = b_k$, c_k, $g_k \in F$ $(0 \leqslant k \leqslant N-1)$ with the properties $(\alpha) - (\delta)$ from 3.6 (b). We must show that $a_k = b_k = 1$.

According to 3.3 (a) there exists $\zeta \in F$ with $\zeta^N = 1$ and a permutation p of the set $\{0, 1, 2, \ldots, N-1\}$ such that $g_k = \zeta^{p(k)}$ $(0 \leqslant k \leqslant N-1)$.

We get for $\mathbf{A} \cdot \mathbf{C}^* = (x_{ij})$ according to 3.3 (c)

$$\begin{aligned} x_{ij} &= \sum_{k=0}^{N-1} t_{ih} \bar{t}_{hj} = \sum_{k=0}^{N-1} t_{ih} c_{jl(h)} = \sum_{h=0}^{N-1} g_i^h a_i g_j^{l(h)} c_j = \\ &= a_i c_j \sum_{h=0}^{N-1} \zeta^{h(p(i)-p(j))} = \\ &= \begin{cases} N a_i c_i & \text{for } i = j \\ 0 & \text{otherwise} \end{cases} = \\ &= \begin{cases} 1 & \text{for } i = j \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Therefore $N a_i c_i = 1 = N a_i^2 c_i$ and then $a_i = b_i = 1$.

The implication "(b) → (a)" follows directly from 3.6 because the matrix $(N^{-1} g_h^{-k})$ $(0 \leqslant k, h \leqslant N-1)$ is the inverse matrix of $\mathbf{T}$ (3.3 (c)).

4.3. Remark. This Theorem and Theorem 3.6 do not hold in a general case of the ring *R*.

Example. Let R be the residue classs ring $\mathbf{Z}/15\mathbf{Z}$ modulo 15. Put

$$\mathbf{T} = \mathbf{A} = \mathbf{B} = \begin{bmatrix} 1 & 4 \\ 1 & 11 \end{bmatrix}, \qquad \mathbf{C} = (\mathbf{T}^{-1})^* = \begin{bmatrix} 8 & 2 \\ 8 & 13 \end{bmatrix}.$$

(The integers in matrices **A**, **C** mean the corresponding residue classes modulo 15.)

The elements in the matrix **T** have not the form from 4.2 (b), but the matrices **A**, **B**, **C** support circular convolution.

In the following Theorem we give complete solution of the case $N = 2$.

4.4 Theorem. *Let* $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, $\mathbf{C} = (c_{ij})$ $(0 \leqslant i, j \leqslant 1)$ *be quadratic matrices of order* 2 *over the ring* R. *Then the following statements are equivalent*:

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

(*b*) *There exist* $a_k, b_k, c_k, \zeta \in R$ $(0 \leqslant k \leqslant 1)$ *such that*

(α) $\zeta^2 = 1$,

(β) $2a_k b_k c_k = 1$ *for* $0 \leqslant k \leqslant 1$,

(γ) $a_{kh} = g_k^h a_k$, $b_{kh} = g_k^h b_k$, $c_{kh} = g_k^h c_k$ *for* $0 \leqslant k, h \leqslant 1$, *where* $\{g_0, g_1\} = \{\zeta, -\zeta\}$.

Proof. Clearly the statement (a) follows from (b). Let the matrices **A**, **B**, **C** support circular convolution. For simplicity put

$$\mathbf{A} = (a_{ij}) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \mathbf{B} = (b_{ij}) = \begin{bmatrix} p & q \\ r & s \end{bmatrix},$$

$$\mathbf{C} = (c_{ij}) = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

where $a, \ldots, w \in R$.

Then there holds

$$\begin{aligned} apx + crz &= 1 \\ apy + crw &= 0 \\ aqx + csz &= 0 \\ aqy + csw &= 1 \\ bpx + drz &= 0 \\ bpy + drw &= 1 \\ bqx + dsz &= 1 \\ bqy + dsw &= 0. \end{aligned} \tag{1}$$

The elements $a, \ldots, w$ are not zero-divisors. We show this for the element a.

(For the other elements it is shown analogously.) If a is a zero-divisor, then there exists $\alpha \in R$, $\alpha \neq 0$ such that $a\alpha = 0$. Since $apx + crz = 1$, we have $\alpha = \alpha crz$, and since $apy + crw = 0$, there holds $\alpha crw = 0$, which implies $\alpha w = 0$. From the equality $aqy + csw = 1$ we get $\alpha = 0$.

Let T be the total quotient ring of R (analog of the quotient field (see, e.g., [5] p. 12), each non zero-divisor of R has an inverse element in T).

From (1) we get

$$a = -\frac{crw}{py}, \qquad b = -\frac{drz}{px}$$

and

$$\begin{aligned} cr(zy - wx) &= y \\ szpy &= rwqx \\ cswp - crwq &= p \\ dr(wx - zy) &= x \\ dszp - drzq &= p \\ swpx &= rzqy. \end{aligned} \tag{2}$$

Since y is not a zero-divisor, we get from the first equality of (2) that the element $zy - wx$ is not zero-divisor either. Then we obtain from (2)

$$c = \frac{y}{r(zy - wx)}, \qquad d = \frac{x}{r(wx - zy)}, \qquad p = \frac{rwqx}{szy}$$

and

$$\begin{aligned} ys(wx - zy) &= xr(zy - wx) \\ zs(wx - zy) &= wr(wx - zy) \\ w^2x^2 &= z^2y^2. \end{aligned} \tag{3}$$

It follows that

$$x = -\frac{ys}{r}, \qquad r = \frac{zs}{w}$$

and

$$z^4 = w^4.$$

Then $zy - wx = \frac{ys}{rw}(z^2 + w^2)$, thus the element $z^2 + w^2$ is not a zero-divisor. Then the equality $z^4 = w^4$ follows $z^2 = w^2$. The element 2 is not a zero-divisor

because $2w^2 = z^2 + w^2$. Put $\zeta = -\frac{w}{z}$. Then $\zeta^2 = 1$ and we obtain by successive substitution of r, x, p, c, d into derived formulas

$$a = \frac{1}{2qy}, \quad b = \frac{1}{2qy}\zeta, \quad c = \frac{1}{2sw}, \quad d = -\frac{1}{2sw}\zeta,$$
$$p = q\zeta, \quad r = -s\zeta, \quad x = y\zeta, \quad z = -w\zeta.$$

Put

$$a_0 = \frac{1}{2qy}, \quad b_0 = q\zeta, \quad c_0 = y\zeta, \quad a_1 = \frac{1}{2sw}, \quad b_1 = -s\zeta, \quad c_1 = -w\zeta,$$
$$g_0 = \zeta, \quad g_1 = -\zeta.$$

Then $a_0, b_0, c_0, a_1, b_1, c_1 \in R$, $\zeta = -2sza_1 \in R$ and we can see easily that (b) holds.

The proof is complete.

4.5 Remark. The case $N = 1$ is quite easy, but the case $N \geqslant 3$ is open. However, we can give the following sufficient condition.

Let $g_0, g_1, \ldots, g_{N-1} \in R$ and let $g_k^N = 1$ for each $0 \leqslant k \leqslant N-1$. We call the set $\{g_0, g_1, \ldots, g_{N-1}\}$ a *regular system of the Nth roots of unity (in R)* if

$\sum_{k=0}^{N-1} g_k^s = 0$ for every integer s, $s \not\equiv 0 (\mathrm{mod}\ N)$.

Clearly this holds.

Proposition. *Let $a_k, b_k, c_k \in R$ and $Na_kb_kc_k = 1$ $(0 \leqslant k \leqslant N-1)$. Let $\{g_0, g_1, \ldots, g_{N-1}\}$ be a regular system of the Nth roots of units in R. Put* $\mathbf{A} = (a_{kh})$, $\mathbf{B} = (b_{kh})$, $\mathbf{C} = (c_{kh})$ $(0 \leqslant k, h \leqslant N-1)$, *where*

$$a_{kh} = g_k^h a_k, \qquad b_{kh} = g_k^h b_k, \qquad c_{kh} = g_k^h c_k.$$

Then the matrices **A**, **B**, **C** *support circular convolution.*

5. SCC-Matrices over Residue Class Rings

According to 2.6 the study of *SCC*-matrices over the residue class rings modulo m (m is an integer $\geqslant 2$) is reduced to the case when m is a prime power.

In this paragraph we denote by

p a prime
n a positive integer
φ_n the canonical homomorphism from the ring **Z** of rational integers onto the

residue class ring $\mathbf{Z}/p^n\mathbf{Z}$ modulo p^n, i.e. for $z \in \mathbf{Z}$ we have $z \in \varphi_n(z) \in \mathbf{Z}/p^n\mathbf{Z}$,

$\mathbf{Z}_p$ the ring of p-adic integers, hence each element $\alpha \in \mathbf{Z}_p$ has the form $\alpha = a_0 + a_1 p + a_2 p^2 + \ldots$, where $0 \leqslant a_i \leqslant p-1$ $(0 \leqslant i < \infty)$ are rational integers,

$\mathbf{Q}_p$ the p-adic number field, hence the quotient field of the ring $\mathbf{Z}_p$.

The basic properties of the p-adic numbers are mentioned in the book of *Z. J. Borevich* and *I. R. Shafarevich* [2] or in the book of *H. Koch* and *H. Pieper* [7]. In the latter (Satz 3.5) the following *Hensel Theorem* is mentioned:

Theorem (*Hensel*). *The multiplicative group of the field* Q_p *is isomorph to the direct sum of additive groups*

$$(\mathbf{Z}, +) \oplus (\mathbf{Z}_p, +) \oplus (\mathbf{Z}/(p-1)\mathbf{Z}, +) \text{ for } p \neq 2,$$
$$(\mathbf{Z}, +) \oplus (\mathbf{Z}_2, +) \oplus (\mathbf{Z}/2\mathbf{Z}, +) \text{ for } p = 2.$$

This Theorem states that there exist N different Nth roots of unity in the field $\mathbf{Q}_p$ if and only if N divides p-1 for p odd and $N = 1$ or $N = 2$ for $p = 2$. Then these Nth roots of unity belong to the ring $\mathbf{Z}_p$ because this ring is integrally closed (in$\mathbf{Q}_p$).

From 3.6 and 4.1 we get the Existence Theorem for *SCC*-matrices over $\mathbf{Q}_p$ and $\mathbf{Z}_p$.

5.1 Theorem. *There exist SCC-matrices* $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *of order N over the field* $\mathbf{Q}_p$ *if and only if N divides* $p-1$ *or* $N = 2$.

There exist SCC-matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *of order N over the ring* $\mathbf{Z}_p$ *if and only if N divides* $p-1$.

(The case of $N = 2$ is excluded for the ring $\mathbf{Z}_2$ because the equation $NX = 1$ has no solution in this ring.)

The description of these matrices is given by Theorems 3.6 and 4.1.

From *SCC*-matrices over the ring $\mathbf{Z}_p$ we can construct *SCC*-matrices over the residue class ring $\mathbf{Z}/p^n\mathbf{Z}$ modulo p^n by means of the following Proposition, which follows immediately from 2.7.

5.2. Proposition. *Let* $\mathbf{A} = (\alpha_{ij})$, $\mathbf{B} = (\beta_{ij})$, $\mathbf{C} = (\gamma_{ij})$ $(0 \leqslant i, j \leqslant N-1)$ *be SCC-matrices over the ring* $\mathbf{Z}_p$. *Let* a_{ij}, b_{ij}, c_{ij} *be rational integers with the properties*:

$$a_{ij} \equiv \alpha_{ij}, \qquad b_{ij} \equiv \beta_{ij}, \qquad c_{ij} \equiv \gamma_{ij} (\mathrm{mod}\, p^n)$$

$(0 \leqslant i, j \leqslant N-1)$. *Then the matrices* $\bar{\mathbf{A}} = (\varphi_n(a_{ij}))$, $\bar{\mathbf{B}} = (\varphi_n(b_{ij}))$, $\bar{\mathbf{C}} = (\varphi_n(c_{ij}))$ $(0 \leqslant i, j \leqslant N-1)$ *over the ring* $\mathbf{Z}/p^n\mathbf{Z}$ *support circular convolution.*

The following Theorem states an equivalent condition when, by construction of 5.2, all *SCC*-matrices over the ring $\mathbf{Z}/p^n\mathbf{Z}$ are described.

5.3. Theorem. *The following statements are equivalent*:

(*a*) *For every positive integer n and rational integers* a_{ij}, b_{ij}, c_{ij} *such that the*

matrices

$$(\varphi_n(a_{ij})), \qquad (\varphi_n(b_{ij})), \qquad (\varphi_n(c_{ij}))\ (0 \leqslant i, j \leqslant N-1)$$

over the ring $\mathbf{Z}/p^n\mathbf{Z}$ *support circular convolution, there exist p-adic integers* α_{ij}, β_{ij}, γ_{ij} *such that the matrices*

$$(\alpha_{ij}), \qquad (\beta_{ij}), \qquad (\gamma_{ij})\ (0 \leqslant i, j \leqslant N-1)$$

over the ring $\mathbf{Z}_p$ *support circular convolution and*

$$a_{ij} \equiv \alpha_{ij}, \qquad b_{ij} \equiv \beta_{ij}, \qquad c_{ij} \equiv \gamma_{ij} (\mathrm{mod}\ p^n)$$

for $0 \leqslant i, j \leqslant N-1$.

(*b*) *For every positive integer n and rational integers* a_{ij}, b_{ij}, c_{ij} *such that the matrices*

$$(\varphi_n(a_{ij})), \qquad (\varphi_n(b_{ij})), \qquad (\varphi_n(c_{ij}))\ (0 \leqslant i, j \leqslant N-1)$$

over the ring $\mathbf{Z}/p^n\mathbf{Z}$ *support circular convolution, there exist rational integers* a'_{ij}, b'_{ij}, c'_{ij} *such that the matrices*

$$(\varphi_{n+1}(a'_{ij})), \qquad (\varphi_{n+1}(b'_{ij})), \qquad (\varphi_{n+1}(c'_{ij}))\ (0 \leqslant i, j \leqslant N-1)$$

over the ring $\mathbf{Z}/p^{n+1}\mathbf{Z}$ *support circular convolution and*

$$a_{ij} \equiv a'_{ij}, \qquad b_{ij} \equiv b'_{ij}, \qquad c_{ij} \equiv c'_{ij} (\mathrm{mod}\ p^n)$$

for $0 \leqslant i, j \leqslant N-1$.

Proof. The implication (a) → (b) follows from 5.2. Let (b) hold and let $a_{ij}, b_{ij}, c_{ij} \in \mathbf{Z}$ and the matrices $(\varphi_n(a_{ij})), (\varphi_n(b_{ij})), (\varphi_n(c_{ij}))\ (0 \leqslant i,j \leqslant N-1)$ over the ring $\mathbf{Z}/p^n\mathbf{Z}$ support circular convolution.

Then there exist rational integers $a_{ij}^{(\mu)}$, $b_{ij}^{(\mu)}$, $c_{ij}^{(\mu)}$ $(0 \leqslant i, j \leqslant N-1, \mu = 0, 1, 2, \ldots)$ with these properties:

$$a_{ij}^{(0)} = a_{ij}, \quad b_{ij}^{(0)} = b_{ij}, \quad c_{ij}^{(0)} = c_{ij},$$

$$(\varphi_{n+\mu}(a_{ij}^{(\mu)})), \quad (\varphi_{n+\mu}(b_{ij}^{(\mu)})), \quad (\varphi_{n+\mu}(c_{ij}^{(\mu)}))\ (0 \leqslant i, j \leqslant N-1)$$

are *SCC*-matrices over the ring $\mathbf{Z}/p^{n+\mu}\mathbf{Z}$,

$$a_{ij}^{(\mu)} \equiv a_{ij}^{(\mu+1)}, \quad b_{ij}^{(\mu)} \equiv b_{ij}^{(\mu+1)}, \quad c_{ij}^{(\mu)} \equiv c_{ij}^{(\mu+1)} (\mathrm{mod}\ p^{n+\mu})$$

for every $\mu = 0, 1, 2, \ldots$.

Put

$$\alpha_{ij} = \lim_{\mu \to \infty} a_{ij}^{(\mu)}, \quad \beta_{ij} = \lim_{\mu \to \infty} b_{ij}^{(\mu)}, \quad \gamma_{ij} = \lim_{\mu \to \infty} c_{ij}^{(\mu)},$$

where $\lim_{\mu\to\infty}$ denotes the p-adic limit. Then the p-adic integers α_{ij}, β_{ij}, γ_{ij} have properties required in (a).

The Theorem is proved.

Further suppose that a_{ij}, b_{ij}, c_{ij} are rational integers and

$$(\varphi_n(a_{ij})), \quad (\varphi_n(b_{ij})), \quad (\varphi_n(c_{ij})) \; (0 \leqslant i, j \leqslant N-1)$$

are SCC-matrices over the ring $\mathbf{Z}/p^n\mathbf{Z}$.

Then we have for $0 \leqslant u, v, w \leqslant N-1$:

$$\sum_{k=0}^{N-1} a_{ku} b_{kv} c_{kw} = \varepsilon(u, v, w) + p^n s(u, v, w),$$

where

$$\varepsilon(u, v, w) = \begin{cases} 1 & \text{for } u+v+w \equiv 0 \,(\mathrm{mod}\, N) \\ 0 & \text{otherwise} \end{cases}$$

and $s(u, v, w)$ is a rational integer.

Then for the integers a'_{ij}, b'_{ij}, c'_{ij} from 5.3 (b) we have

$$a'_{ij} = a_{ij} + p^n x_{ij}, \quad b'_{ij} = b_{ij} + p^n y_{ij}, \quad c'_{ij} = c_{ij} + p^n z_{ij},$$

where x_{ij}, y_{ij}, $z_{ij} \in \mathbf{Z}$ and

$$(*) \sum_{k=0}^{N-1} b_{kv} c_{kw} x_{ku} + \sum_{k=0}^{N-1} a_{ku} c_{kw} y_{kv} + \sum_{k=0}^{N-} a_{ku} b_{kv} z_{kw} \equiv -s(u, v, w) \;(\mathrm{mod}\, p)$$

for $0 \leqslant u, v, w \leqslant N-1$.

The system $(*)$ is a system of N^3 linear equations with $3N^2$ unknowns x_{ku}, y_{kv}, z_{kw} over the field $\mathbf{Z}/p\mathbf{Z}$. Since the matrices $(\varphi_1(a_{ij}))$, $(\varphi_1(b_{ij}))$, $(\varphi_1(c_{ij}))$ over the field $\mathbf{Z}/p\mathbf{Z}$ support circular convolution, we have for $0 \leqslant i, j \leqslant N-1$ according to 3.6:

$$a_{ij} \equiv g_i^j a_i, \quad b_{ij} \equiv g_i^j b_i, \quad c_{ij} \equiv g_i^j c_i (\mathrm{mod}\, p),$$

where a_i, b_i, c_i, g_i are rational integers, $Na_ib_ic_i \equiv 1 \,(\mathrm{mod}\, p)$ and

$$\{\varphi_1(g_0), \varphi_1(g_1), \ldots, \varphi_1(g_{N-1})\} = \{\varphi_1(1), \varphi_1(g), \varphi_1(g^2), \ldots, \varphi_1(g^{N-1})\},$$

g is a rational integer, p does not divide g and g has order N mod p.

This implies that the rank of the system $(*)$ is equal to the rank of the matrix (mod p) of size $N^3 \times 3N^2$:

$$
\begin{array}{c}
 & x_{ku} & & y_{kv} & & z_{kw} \\
(u, v, w) & \left[\ldots\ g^{k(v+w)}\ \ldots\right. & & \ldots\ g^{k(u+w)}\ \ldots & & \ldots\ g^{k(u+v)}\ \ldots\right] \\
(u, v, w') & \ldots\ g^{k(v+w')}\ \ldots & & \ldots\ g^{k(u+w')}\ \ldots & & \ldots\ 0\ \ldots \\
(u, v', w) & \ldots\ g^{k(v'+w)}\ \ldots & & \ldots\ 0\ \ldots & & \ldots\ g^{k(u+v')}\ \ldots \\
(u', v, w) & \left.\ldots\ 0\ \ldots\right. & & \ldots\ g^{k(u'+w)}\ \ldots & & \left.\ldots\ g^{k(u'+v)}\ \ldots\right]
\end{array}
$$

$0 \leqslant u, v, w, k \leqslant N-1.$

$u' \neq u$
$v' \neq v$
$w' \neq w$

For $N = 1$ we can put $g = 1$ and then this matrix has the form:

$$[1, 1, 1].$$

Hence the system (*) is solvable.
For $N = 2$ we can put $g = -1$ and the given matrix has the form:

u v w	x_{00}	x_{10}	x_{01}	x_{11}	y_{00}	y_{10}	y_{01}	y_{11}	z_{00}	z_{10}	z_{01}	z_{11}
0 0 0	1	1	0	0	1	1	0	0	1	1	0	0
0 0 1	1	−1	0	0	1	−1	0	0	0	0	1	1
0 1 0	1	−1	0	0	0	0	1	1	1	−1	0	0
0 1 1	1	1	0	0	0	0	1	−1	0	0	1	−1
1 0 0	0	0	1	1	1	−1	0	0	1	−1	0	0
1 0 1	0	0	1	−1	1	1	0	0	0	0	1	−1
1 1 0	0	0	1	−1	0	0	1	−1	1	1	0	0
1 1 1	0	0	1	1	0	0	1	1	0	0	1	1

The determinant chosen from this matrix for columns $x_{00}, x_{10}, x_{01}, x_{11}, y_{00}, y_{10}, z_{00}, z_{10}$ has the value 64, from which it follows that the system (*) is solvable for any odd prime p and $N = 2$. Thus we have shown

5.4 Proposition. *Let $N = 1$ or $N = 2$. Let $a_{ij}, b_{ij}, c_{ij} \in \mathbf{Z}$ and the matrices*

$$(\varphi_n(a_{ij})), \quad (\varphi_n(b_{ij})), \quad (\varphi_n(c_{ij})) \ (0 \leqslant i, j \leqslant N-1)$$

over the ring $\mathbf{Z}/p^n\mathbf{Z}$ support circular convolution. Then there exist p-adic integers $\alpha_{ij}, \beta_{ij}, \gamma_{ij}$ such that the matrices

$$(\alpha_{ij}), \quad (\beta_{ij}), \quad (\gamma_{ij}) \ (0 \leqslant i, j \leqslant N-1)$$

over the ring $\mathbf{Z}_p$ support circular convolution and

$$a_{ij} \equiv \alpha_{ij}, \quad b_{ij} \equiv \beta_{ij}, \quad c_{ij} \equiv \gamma_{ij} (\mathrm{mod}\, p^n)$$

for each $0 \leqslant i, j \leqslant N-1$.

5.5. Remark. We can also obtain the proof of 5.4 by means of Theorem 4.4. For $N \geqslant 3$ the description of *SCC*-matrices over the ring $\mathbf{Z}/p^r\mathbf{Z}$ of order N in the way from Proposition 5.4 is an open question.

REFERENCES

[1] AGARWAL, R. C.—BURRUS, Ch. S.: Fast Convolution Using Fermat Number Transforms with Applications to Digital Filtering, IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. ASSP-22, No. 2, April 1974, 87—97.

[2] BOREVICH, Z. I.—SHAFAREVICH, I. R.: Number Theory, Transl. by N. Greenleaf, New York: Academic Press, 1966.

[3] MCCLELLAN, J. H.—RADER, Ch. M.: Number Theory in Digital Signal Processing, Prentice-Hall, Inc. Englewood Cliffs, New Jersey 07632, 1979.

[4] ČÍŽEK, V.: Diskrétní Fourierova transformace a její použití, matematický seminář SNTL, Praha 1981 (Czech).

[5] GILMER, R. W.: Multiplicative Ideal Theory, Queen's Papers in Pure and Applied Mathematics, No. 12, Queen's University, Kingston, Ontario, 1968.

[6] NUSSBAUMER, H. J.: Fast Fourier Transform and Convolution Algorithmus, Springer-Verlag, Berlin—Heidelberg—New York 1981.

[7] KOCH, H.—PIEPER, H.: Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, Berlin 1976 (German).

Received October 5, 1984

Katedra matematiky
přírodovědecké fakulty Univerzity J. E. Purkyně
Janáčkovo nám. 2a
662 95 *Brno*

ЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ И КОНВОЛЮЦИЯ

Ladislav Skula

Резюме

Изучаются линейные преобразования, которые удовлетворяют «свойствам конволюции». Скажем, что три линейные преобразования удовлетворяют свойствам конволюции, если мы можем вычислить круговою конволюцию двух последовательностей при помощи этих преобразований по формуле, известной в теории дискретного преобразования фурье. Это изучение развито для коммутативных колец с единицей. Эта проблема решена полностью для полей, областей целостности и в случае, когда длина изучаемых последовательностей равна 2. Для колец вычетов используется понятие p-адических чисел.