Annales Univ. Sci. Budapest., Sect. Comp. 23 (2004) 25-40

THE STRUCTURE OF THE BOOLEAN–ZHEGALKIN TRANSFORM

J. Gonda (Budapest, Hungary)

Dedicated to Professor I. Kátai on his 65th birthday

Abstract. In [6] a linear algebraic aspect is given for the transformation of a Boolean function to its Zhegalkin-representation. In this article, we investigate the linear-algebraic structure of that transform.

In this article the elements of the field with two elements are denoted by 0 and 1; $\mathbf{N}_0$ denotes the non-negative integers, and $\mathbf{N}$ the positive ones.

In [6] we pointed out that if we consider the coefficients of a Boolean function of n variables and the coefficients of the Zhegalkin polynomial of n variables, respectively, as the components of an element of a 2^n-dimensional linear space over $\mathbf{F}_2$, then the relation between the vectors belonging to the two representations of the same Boolean function of n variables could be given by $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$. Here $\underline{k}$ is the vector containing the components of the Zhegalkin polynomial, $\underline{\alpha}$ is the vector, composed by the coefficients of the Boolean representation of the given function, and $\mathbf{A}^{(n)}$ is the matrix of the transform in the natural basis. In the article mentioned above is proved that

$$\mathbf{A}^{(n)} = \begin{cases} (1), & \text{if } n = 0, \\ \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix}, & \text{if } n \in \mathbf{N}, \end{cases}$$

and as a consequence that

$$\mathbf{A}^{(n)^2} = \mathbf{I}^{(n)},$$

where $\mathbf{I}^{(n)}$ and $\mathbf{0}^{(n)}$ denote the 2^n-dimensional identity and zero matrix, respectively. From this follows that if $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$, then $\underline{\alpha} = \mathbf{A}^{(n)}\underline{k}$.

In the following part of our article, we consider the transform given above by $\mathbf{A}^{(n)}$.

Theorem 1.

$$\mathbf{A}^{(n)}+\lambda\mathbf{I}^{(n)} \equiv \begin{cases} (1+\lambda)\mathbf{I}^{(n)}, & \text{if } n=0, \\ \begin{pmatrix} \mathbf{I}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{0}^{(n-1)} & (1+\lambda^2)\mathbf{I}^{(n-1)} \end{pmatrix}, & \text{if } n \in \mathbf{N}, \end{cases}$$

where $\mathbf{U}(\lambda) \equiv \mathbf{V}(\lambda)$ *means that the two* λ*-matrices are equivalent, that is there are invertible* λ*-matrices* $\mathbf{R}(\lambda)$ *and* $\mathbf{L}(\lambda)$ *so, that* $\mathbf{V}(\lambda)=\mathbf{L}(\lambda)\mathbf{U}(\lambda)\mathbf{R}(\lambda)$.

Proof. If $n=0$, then

$$\mathbf{A}^{(n)}+\lambda\mathbf{I}^{(n)}=\mathbf{A}^{(0)}+\lambda\mathbf{I}^{(0)}=(1)+\lambda(1)=(1+\lambda)(1)=(1+\lambda)\mathbf{I}^{(0)}=(1+\lambda)\mathbf{I}^{(n)}.$$

Now let $n \in \mathbf{N}_0$,

$$\begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{A}^{(n)} \\ \mathbf{I}^{(n)} & \mathbf{I}^{(n)}+\lambda\mathbf{A}^{(n)} \end{pmatrix} = \mathbf{L}^{(n+1)}(\lambda), \ \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)}+\lambda\mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} = \mathbf{R}^{(n+1)}(\lambda)$$

and let $\mathbf{C}^{(n+1)}(\lambda)$ denote $\begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & (1+\lambda^2)\mathbf{I}^{(n)} \end{pmatrix}$, then

$$\mathbf{L}^{(n+1)}(\lambda)\mathbf{A}^{(n+1)}\mathbf{R}^{(n+1)}(\lambda) = \begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{A}^{(n)} \\ \mathbf{I}^{(n)} & \mathbf{I}^{(n)}+\lambda\mathbf{A}^{(n)} \end{pmatrix} \times$$

$$\times \begin{pmatrix} \mathbf{A}^{(n)}+\lambda\mathbf{I}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)}+\lambda\mathbf{I}^{(n)} \end{pmatrix} \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)}+\lambda\mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} =$$

$$= \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & (1+\lambda^2)\mathbf{I}^{(n)} \end{pmatrix} = \mathbf{C}^{(n+1)}(\lambda),$$

$\left(\mathbf{A}^{(n)}\right)^2 = \mathbf{I}^{(n)}$, so $1 = \det\left(\mathbf{I}^{(n)}\right) = \det\left(\left(\mathbf{A}^{(n)}\right)^2\right) = \left(\det\left(\mathbf{A}^{(n)}\right)\right)^2$, and then $\det\left(\mathbf{A}^{(n)}\right) = 1$. As $\det\left(\mathbf{L}^{(n+1)}(\lambda)\right) = \det\left(\mathbf{A}^{(n)}\right)$, we get that $\det\left(\mathbf{L}^{(n+1)}(\alpha)\right) = 1$. With a similar calculation we can get that

$$\det\left(\mathbf{R}^{(n+1)}(\alpha)\right) = 1,$$

so $\mathbf{L}(\lambda)$ and $\mathbf{R}(\lambda)$ are invertible matrices, and

$$\mathbf{C}^{(n+1)} = \mathbf{L}^{(n+1)}(\lambda)\left(\mathbf{A}^{(n+1)}+\lambda\mathbf{I}^{(n+1)}\right)\mathbf{R}^{(n+1)}(\lambda),$$

i.e. the two matrices are equivalent.

From the previous theorem, we can get many results. First, we can read out the minimal polynomial and characteristic polynomial of $\mathbf{A}^{(n)}$.

Corollary 2. *If $\mu^{(n)}$ denotes the minimal polynomial of $\mathbf{A}^{(n)}$, and $c^{(n)}$ denotes its characteristic polynomial, then*

$$\mu^{(n)} = \begin{cases} \lambda + 1, & \text{if } n = 0, \\ \lambda^2 + 1, & \text{if } n \in \mathbf{N}, \end{cases}$$
$$c^{(n)} = \lambda^{2^n} + 1.$$

Proof. The minimal polynomial of a quadratic matrix is its last invariant factor, in our case the abovementioned polynomials. The characteristic polynomial is the product of the invariant factors. If $n = 0$, then the only invariant factor is $\lambda + 1$, and $\lambda^{2^0} + 1 = \lambda + 1$. In the case, when $n \in \mathbf{N}$, that is when $n \geq 1$, then there are 2^{n-1} invariant factors equal to 1, and each of the further 2^{n-1} invariant factors is equal to $\lambda^2 + 1$, so $c^{(n)} = (\lambda^2 + 1)^{2^{n-1}} = (\lambda^2)^{2^{n-1}} + 1 = \lambda^{2^n} + 1$.

The results mentioned above are not surprising. $\mathbf{A}^{(0)} + \lambda\mathbf{I}^{(0)} = (1 + \lambda)$ and $\det((1 + \lambda)) = \lambda + 1$, so $\lambda + 1 \in \mathbf{F}_2[\lambda]$ is the characteristic polynomial of $\mathbf{A}^{(0)}$. The degree of that polynomial is equal to 1, which is the order of the matrix $\mathbf{A}^{(0)}$. As there is no nonzero polynomial of degree less than 1, of which $\mathbf{A}^{(0)}$ is the root, $\lambda + 1$ is the minimal polynomial of $\mathbf{A}^{(0)}$, as well.

Now let $n > 0$, then $\mathbf{A}^{(n)} \neq \mathbf{I}^{(n)}$ and $\mathbf{A}^{(n)} \neq \mathbf{0}^{(n)}$, so neither λ nor $\lambda + 1$ can be the minimal polynomial of the matrix. On the other hand, $\mathbf{A}^{(n)^2} = \mathbf{I}^{(n)}$ shows, that $\mathbf{A}^{(n)}$ is the root of the monic polynomial $\lambda^2 + 1$, and the minimal polynomial of a matrix is uniquely determined. Now let us consider the characteristic polynomial of $\mathbf{A}^{(n)}$. The degree of that polynomial is equal to 2^n, and the set of the roots of the characteristic polynomial is equal to the set of the roots of the minimal polynomial. As $\lambda^2 + 1 = (\lambda + 1)^2$ over $\mathbf{F}_2$, the only root of the minimal polynomial is 1. From this follows the characteristic polynomial of $\mathbf{A}^{(n)}$ is a polynomial of degree 2^n with exactly one root, namely 1. The only (monic) polynomial with these properties is $(\lambda + 1)^{2^n} = \lambda^{2^n} + 1$, and then the characteristic polynomial of $\mathbf{A}^{(n)}$ is $\lambda^{2^n} + 1$.

Another simple way to prove $\lambda^{2^n} + 1$ is the minimal polynomial of $\mathbf{A}^{(n)}$ is as follows. We saw above, that $c^{(0)} = \lambda + 1 = \lambda^{2^0} + 1$. If $c^{(n-1)} = \lambda^{2^{n-1}} + 1$, then

$$c^{(n)} =$$

$$= \det\left(\mathbf{A}^{(n)} + \lambda\mathbf{I}^{(n)}\right) = \det\left(\begin{pmatrix} \mathbf{A}^{(n-1)} + \lambda\mathbf{I}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} + \lambda\mathbf{I}^{(n-1)} \end{pmatrix}\right) =$$

$$= \left(\det\left(\mathbf{A}^{(n-1)} + \lambda\mathbf{I}^{(n-1)}\right)\right)^2 = {c^{(n-1)}}^2 = \left(\lambda^{2^{n-1}} + 1\right)^2 = \left(\lambda^{2^{n-1}}\right)^2 + 1 =$$

$$= \lambda^{2^n} + 1,$$

so for any nonnegative integer n $c^{(n)} = \lambda^{2^n} + 1$.

Corollary 3. *For any $n \in \mathbf{N}_0$ the 2^{n+1} dimensional linear space over $\mathbf{F}_2$ is a direct sum of 2^n two-dimensional cyclic subspaces invariant with respect to $\mathbf{A}^{(n+1)}$.*

Proof. The only invariant factor of $\mathbf{A}^{(n+1)}$ is equal to $\lambda^2 + 1$ and the multiplicity of that invariant factor is equal to 2^n. From this two facts immediately follows the statement above.

Let $\mathbf{A} \sim \mathbf{B}$ denote that the matrices $\mathbf{A}$ and $\mathbf{B}$ are similar, that is there is an invertible matrix $\mathbf{T}$ so, that $\mathbf{B} = \mathbf{T}^{-1}\mathbf{A}\mathbf{T}$.

Corollary 4.

$$\mathbf{A}^{(n)} \sim \begin{cases} \mathbf{B}^{(0)} = (1) = \mathbf{A}^{(0)}, \\ \mathbf{B}^{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ \mathbf{B}^{(n)} = \begin{pmatrix} \mathbf{B}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{0}^{(n-1)} & \mathbf{B}^{(n-1)} \end{pmatrix}, \quad 1 < n \in \mathbf{N}, \end{cases}$$

where for any nonnegative integer n $\mathbf{B}^{(n)}$ is the Jordan matrix of $\mathbf{A}^{(n)}$.

Proof. $c^{(0)}(\lambda) = \lambda + 1 = \mu^{(0)}(\lambda)$ and $c^{(1)}(\lambda) = \lambda^2 + 1 = \mu^{(1)}(\lambda)$, that is the 2^0- and the 2^1-dimensional linear spaces over $\mathbf{F}_2$ are cyclic and invariant with respect to $\mathbf{A}^{(0)}$ and $\mathbf{A}^{(1)}$, respectively. In such a case the Jordan matrix of $\mathbf{A}^{(0)}$ and $\mathbf{A}^{(1)}$ is equal to the companion matrix of their minimal polynomial, and then $\mathbf{B}^{(0)} = (1)$ and $\mathbf{B}^{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Now if $n > 1$, then by Corollary 3 the 2^n-dimensional linear space over $\mathbf{F}_2$ is the direct sum of 2^{n-1} two-dimensional cyclic spaces invariant to the transform represented by $\mathbf{A}^{(n)}$ in the canonical basis of the space. The Jordan matrix of such a transform is the hypermatrix containing 2^{n-1} blocks equal to $\mathbf{B}^{(1)}$ in the main diagonal, and the zero matrix of order two in the other positions of that matrix. But the structure of $\mathbf{B}^{(1)}$ corresponds to that form, and if the structure of $\mathbf{B}^{(n)}$, where $n \in \mathbf{N}$, satisfies this rule, then $\mathbf{B}^{(n+1)}$ satisfies, too.

Corollary 5.

$$\mathbf{A}^{(n)} \sim \begin{cases} \mathbf{C}^{(0)} = (1) = \mathbf{A}^{(0)}, \\ \mathbf{C}^{(1)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} \mathbf{C}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{0}^{(n-1)} & \mathbf{C}^{(n-1)} \end{pmatrix}, \quad 1 < n \in \mathbf{N}, \end{cases}$$

where $\mathbf{C}^{(n)}$ *is the classical canonical matrix of* $\mathbf{A}^{(n)}$.

Proof. $c^{(0)}(\lambda) = \lambda + 1 = \mu^{(0)}(\lambda)$, and then the classical canonical matrix of $\mathbf{A}^{(0)}$ is the identity matrix of order 1, that is $\mathbf{C}^{(0)} = (1)$.

Over $\mathbf{F}_2$ $\mu^{(2)}(\lambda) = \lambda^2 + 1 = (\lambda + 1)^2$, so the classical canonical matrix of $\mathbf{A}^{(1)}$ is $\mathbf{C}^{(1)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and for $n > 1$ we can argue similarly as we do it in the proof of Corollary 4, substituting the Jordan matrix by the classical canonical matrix, and $\mathbf{B}^{(1)}$, $\mathbf{B}^{(n)}$ and $\mathbf{B}^{(n+1)}$ by $\mathbf{C}^{(1)}$, $\mathbf{C}^{(n)}$ and $\mathbf{C}^{(n+1)}$, respectively.

Now we can give a basis of the 2^n-dimensional linear space over $\mathbf{F}_2$, in which the matrix of the transform represented by $\mathbf{A}^{(n)}$ in the canonical basis of the space is equal to $\mathbf{B}^{(n)}$. For $n \in \mathbf{N}$ and $2^n > i \in \mathbf{N}_0$ let $\underline{e}^{(n;i)}$ be the i-th vector of the canonical basis of the 2^n-dimensional linear space over $\mathbf{F}_2$, that is the j-th component of $\underline{e}^{(n;i)}$, where $2^n > j \in \mathbf{N}_0$, is equal to

$$e_j^{(n;i)} = \delta_{i,j} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Let us denote the i-th column of an arbitrary matrix $\mathbf{M}$ either by $\underline{M}_i$ or by $(\mathbf{M})_i$, and let $\mathbf{U}^{(n)}$ be that 2^n by 2^n matrix, in which for $2^n > i \in \mathbf{N}_0$

$$\underline{U}_i^{(n)} = \begin{cases} \underline{e}^{(n;i)}, & \text{if } i \equiv 0 \ (2) \\ \underline{A}_i^{(n)}, & \text{if } i \equiv 1 \ (2). \end{cases}$$

Theorem 6. *The matrix of the transform represented by* $\mathbf{A}^{(n)}$ *in the canonical basis of the* 2^n*-dimensional linear space over* $\mathbf{F}_2$ *is equal to* $\mathbf{B}^{(n)}$ *in the basis given by the columns of* $\mathbf{U}^{(n)}$.

Proof. For any two quadratic matrices $\mathbf{M}^{(1)}$ and $\mathbf{M}^{(2)}$ of order 2^n, where n is a nonnegative integer, and for any $2^n > i \in \mathbf{N}_0$,

$$\left(\mathbf{M}^{(1)}\mathbf{M}^{(2)}\right)_i = \left(\mathbf{M}^{(1)}\mathbf{M}^{(2)}\right)\underline{e}^{(n;i)} = \mathbf{M}^{(1)}\left(\mathbf{M}^{(2)}\underline{e}^{(n;i)}\right) = \mathbf{M}^{(1)}\underline{M}_i^{(2)},$$

$\left(\mathbf{A}^{(n)}\right)^2 = \mathbf{I}^{(n)}$, so $\mathbf{A}^{(n)}\underline{A}_j^{(n)} = \left(\mathbf{A}^{(n)}\mathbf{A}^{(n)}\right)_j = \left(\mathbf{I}^{(n)}\right)_j = \underline{e}^{(n;j)}$. Let us consider the columns of $\mathbf{B}^{(n)}$. $\mathbf{B}^{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so $\underline{B}_0^{(1)} = \underline{e}^{(1;1)}$ and $\underline{B}_1^{(1)} = \underline{e}^{(1;0)}$, that is for any nonnegative integer i less than $2^{1-1} = 1$ $\quad \underline{B}_{2i}^{(1)} = \underline{e}^{(1;2i+1)}$ and $\underline{B}_{2i+1}^{(1)} = \underline{e}^{(1;2i)}$. Now suppose if $n \in \mathbf{N}$, then for any $2^{n-1} > i \in \mathbf{N}_0$ $\underline{B}_{2i}^{(n)} = \underline{e}^{(n;2i+1)}$ and $\underline{B}_{2i+1}^{(n)} = \underline{e}^{(n;2i)}$, or with an ε equal to either 0 or 1, $\underline{B}_{2i+\varepsilon}^{(n)} = \underline{e}^{(n;2i+(1-\varepsilon))}$.

$$\underline{B}_{2i+\varepsilon}^{(n+1)} = \mathbf{B}^{(n+1)}\underline{e}^{(n+1;2i+\varepsilon)} = \begin{pmatrix} \mathbf{B}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{B}^{(n)} \end{pmatrix} \underline{e}^{(n+1;2i+\varepsilon)},$$

where $2^n > i \in \mathbf{N}_0$. If $2^{n-1} > i \in \mathbf{N}_0$, then

$$\begin{pmatrix} \mathbf{B}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{B}^{(n)} \end{pmatrix} \underline{e}^{(n+1;2i+\varepsilon)} =$$

$$= \begin{pmatrix} \mathbf{B}^{(n)}\mathbf{0}^{(n)} \\ \mathbf{0}^{(n)}\mathbf{B}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{e}^{(n;2i+\varepsilon)} \\ \underline{0}^{(n)} \end{pmatrix} = \begin{pmatrix} \mathbf{B}^{(n)} \\ \mathbf{0}^{(n)} \end{pmatrix} \underline{e}^{(n;2i+\varepsilon)} =$$

$$= \begin{pmatrix} \mathbf{B}^{(n)}\underline{e}^{(n;2i+\varepsilon)} \\ \mathbf{0}^{(n)}\underline{e}^{(n;2i+\varepsilon)} \end{pmatrix} = \begin{pmatrix} \underline{B}_{2i+\varepsilon}^{(n)} \\ \underline{0}^{(n)} \end{pmatrix} = \begin{pmatrix} \underline{e}^{(n;2i+(1-\varepsilon))} \\ \underline{0}^{(n)} \end{pmatrix} = \underline{e}^{(n+1;2i+(1-\varepsilon))}$$

and if i is an integer so, that $2^{n-1} \le i < 2^n$, that is if $2^{n-1} > i - 2^{n-1} \in \mathbf{N}_0$, then

$$\begin{pmatrix} \mathbf{B}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{B}^{(n)} \end{pmatrix} \underline{e}^{(n+1;2i+\varepsilon)} =$$

$$= \begin{pmatrix} \mathbf{B}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{B}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{0}^{(n)} \\ \underline{e}^{(n;2i-2^{n-1}+\varepsilon)} \end{pmatrix} = \begin{pmatrix} \mathbf{0}^{(n)} \\ \mathbf{B}^{(n)} \end{pmatrix} \underline{e}^{(n;2i-2^{n-1}+\varepsilon)} =$$

$$= \begin{pmatrix} \mathbf{0}^{(n)}\underline{e}^{(n;2i-2^{n-1}+\varepsilon)} \\ \mathbf{B}^{(n)}\underline{e}^{(n;2i-2^{n-1}+\varepsilon)} \end{pmatrix} = \begin{pmatrix} \underline{0}^{(n)} \\ \underline{B}_{2i+\varepsilon}^{(n)} \end{pmatrix} = \begin{pmatrix} \underline{0}^{(n)} \\ \underline{e}^{(n;2i-2^{n-1}+(1-\varepsilon))} \end{pmatrix} =$$

$$= \underline{e}^{(n+1;2i+(1-\varepsilon))}.$$

Joining together these two results we get that $\underline{B}_{2i+\varepsilon}^{(n+1)} = \underline{e}^{(n+1;2i+(1-\varepsilon))}$ is true, too. Applying the equations $\mathbf{A}^{(n)}\underline{A}_j^{(n)} = \underline{e}^{(n;j)}$ and $\underline{B}_{2i+\varepsilon}^{(n+1)} = \underline{e}^{(n+1;2i+(1-\varepsilon))}$ for $2^{n-1} > i \in \mathbf{N}_0$, where n is an arbitrary positive integer,

$$\left(\mathbf{A}^{(n)}\mathbf{U}^{(n)}\right)_{2i} = \mathbf{A}^{(n)}\underline{U}_{2i}^{(n)} = \mathbf{A}^{(n)}\underline{e}^{(n;2i)} = \underline{A}_{2i}^{(n)} =$$

$$= \underline{U}_{2i+1}^{(n)} = \mathbf{U}^{(n)}\underline{e}^{(n;2i+1)} = \mathbf{U}^{(n)}\underline{B}_{2i}^{(n)} = (\mathbf{U}^{(n)}\mathbf{B}^{(n)})_{2i}$$

and

$$\left(\mathbf{A}^{(n)}\mathbf{U}^{(n)}\right)_{2i+1} = \mathbf{A}^{(n)}\underline{U}^{(n)}_{2i+1} = \mathbf{A}^{(n)}\underline{A}^{(n)}_{2i} = \underline{e}^{(n;2i)} =$$
$$= \underline{U}^{(n)}_{2i} = \underline{\mathbf{U}}^{(n)}\underline{e}^{(n;2i)} = \mathbf{U}^{(n)}\underline{B}^{(n)}_{2i+1} = \left(\mathbf{U}^{(n)}\mathbf{B}^{(n)}\right)_{2i+1}.$$

This means that for any $n \in \mathbf{N}$ and $2^n > i \in \mathbf{N}_0$ $(\mathbf{A}^{(n)}\mathbf{U}^{(n)})_i = (\mathbf{U}^{(n)}\mathbf{B}^{(n)})_i$, and then $\mathbf{A}^{(n)}\mathbf{U}^{(n)} = \mathbf{U}^{(n)}\mathbf{B}^{(n)}$. We have to prove that $\mathbf{U}^{(n)}$ is a regular matrix for every positive integer n.

We shall see that the set $\left\{\underline{U}^{(n)}_i \mid 0 \le i < 2^n\right\}$ spans the 2^n-dimensional linear space over $\mathbf{F}_2$. If it is true, then this set is a generator system of the 2^n-dimensional linear space over $\mathbf{F}_2$, and the cardinality of this set is less than or equal to 2^n. In this case the vectors of this set, so the columns of $\mathbf{U}^{(n)}$, are pairwise linearly independent, so $\mathbf{U}^{(n)}$ is regular, and the above-mentioned set is the basis of our space. Then with the preceding result, namely that $\mathbf{A}^{(n)}\mathbf{U}^{(n)} = \mathbf{U}^{(n)}\mathbf{B}^{(n)}$, we get that in that basis the transform determined by $\mathbf{A}^{(n)}$ in the canonical basis is equal to $\mathbf{B}^{(n)}$.

We put now to use that if $0 \le i < 2j < 2^n$, then $A_{i,2j} = 0$, $A_{2j,2j} = e$, and $A_{2j+1,2j} = e$. By the definition of $\mathbf{U}^{(n)}$ given above, we get that $\underline{U}^{(n)}_{2^n-2} = \underline{e}^{(n;2^n-2)}$, and $\underline{U}^{(n)}_{2^n-2} + \underline{U}^{(n)}_{2^n-1} = \underline{e}^{(n;2^n-2)} + \underline{A}^{(n)}_{2^n-2} = \underline{e}^{(n;2^n-1)}$. Now suppose that for an integer k, for which $2^{n-1}-1 > k \in \mathbf{N}_0$, $\left\langle \underline{U}^{(n)}_i \mid 2k+1 < i < 2^n \right\rangle = \left\langle \underline{e}^{(n;i)} \mid 2k+1 < i < 2^n \right\rangle$, where the angle brackets denote the space spanned by the vectors in the angle brackets. Then $\underline{U}^{(n)}_{2k} = \underline{e}^{(n;2k)}$ and $\underline{U}^{(n)}_{2k+1} = \underline{A}^{(n)}_{2k}$, and

$$\underline{U}^{(n)}_{2k} + \underline{U}^{(n)}_{2k+1} + \sum_{i=2k+2}^{2^n-1} A^{(n)}_{i,2k}\underline{e}^{(n;i)} = \underline{e}^{(n;2k)} + \underline{A}^{(n)}_{2k} + \sum_{i=2k+2}^{2^n-1} A^{(n)}_{i,2k} + \underline{e}^{(n;i)} =$$
$$= \underline{A}^{(n)}_{2k} + \sum_{\substack{i=0 \\ i\neq 2k+1}}^{2^n-1} A^{(n)}_{i,2k}\underline{e}^{(n;i)} = \underline{e}^{(n;2k+1)},$$

that is

$$\left\langle \underline{U}^{(n)}_i \mid 2k \le i < 2^n \right\rangle = \left\langle \underline{e}^{(n;i)} \mid 2k \le i < 2^n \right\rangle$$

and from this follows that $\left\{\underline{U}^{(n)}_i \mid 0 \le i < 2^n\right\} = \left\langle \underline{e}^{(n;i)} \mid 0 \le i < 2^n \right\rangle$.

For $n \in \mathbf{N}$ we can give a recursive form for generating the sequence of the matrices $\mathbf{U}^{(n)}$ as follows.

Theorem 7. *Let* $\mathbf{V}^{(1)} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ *and* $\mathbf{V}^{(n+1)} = \begin{pmatrix} \mathbf{V}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{V}^{(n)} \end{pmatrix}$ *for* $n \in \mathbf{N}$. *Then* $\mathbf{U}^{(1)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *and for any positive integer* n $\mathbf{U}^{(n+1)} = \begin{pmatrix} \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix}$.

Proof. The first column of $\mathbf{U}^{(1)}$ is $\underline{e}^{(0)}$, and the second column of the matrix is apparently $\underline{A}_0^{(1)}$, so $\mathbf{U}^{(1)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$\underline{V}_{2i}^{(1)} = \underline{V}_0^{(1)} = \underline{0}^{(1)}$ and $\underline{V}_{2i+1}^{(1)} = \underline{V}_1^{(1)} = \underline{A}_0^{(1)} = \underline{U}_1^{(1)}$, if $n = 1$ and $2^{1-1} > i \in \mathbf{N}_0$. Suppose for an $n \in \mathbf{N}$ with any $2^{n-1} > i \in \mathbf{N}_0$ $\underline{V}_{2i}^{(n)} = \underline{0}^{(n)}$ and $\underline{V}_{2i+1}^{(n)} = \underline{U}_{2i+1}^{(n)}$. Then for any $2^n > i \in \mathbf{N}_0$

$$\begin{pmatrix} \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix} \underline{e}^{(n+1;i)} = \begin{pmatrix} \mathbf{U}^{(n)} \underline{e}^{(n;i)} \\ \mathbf{V}^{(n)} \underline{e}^{(n;i)} \end{pmatrix} = \begin{pmatrix} \underline{U}_i^{(n)} \\ \underline{V}_i^{(n)} \end{pmatrix} =$$

$$= \begin{cases} \begin{pmatrix} \underline{e}^{(n;2j)} \\ \underline{0}^{(n)} \end{pmatrix} = \underline{e}^{(n+1;2j)} = \underline{U}_{2j}^{(n+1)}, & \text{if } i = 2j, \\ \begin{pmatrix} \underline{A}_{2j}^{(n)} \\ \underline{A}_{2j}^{(n)} \end{pmatrix} = \underline{A}_{2j}^{(n+1)} = \underline{U}_{2j+1}^{(n+1)}, & \text{if } i = 2j+1, \end{cases}$$

and if $2^n \le i < 2^{n+1}$, that is if $2^n > i - 2^n \in \mathbf{N}_0$, then

$$\begin{pmatrix} \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix} \underline{e}^{(n+1;i)} = \begin{pmatrix} \mathbf{0}^{(n)} \underline{e}^{(n;i-2^n)} \\ \mathbf{U}^{(n)} \underline{e}^{(n;i-2^n)} \end{pmatrix} = \begin{pmatrix} \underline{0}^{(n)} \\ \underline{U}_{i-2^n}^{(n)} \end{pmatrix} =$$

$$= \begin{cases} \begin{pmatrix} \underline{0}^{(n)} \\ \underline{e}^{(n;2j-2^n)} \end{pmatrix} = \underline{e}^{(n+1;2j)} = \underline{U}_{2j}^{(n+1)}, & \text{if } i = 2j, \\ \begin{pmatrix} \underline{0}^{(n)} \\ \underline{A}_{2j-2^n}^{(n)} \end{pmatrix} = \underline{A}_{2j}^{(n+1)} = \underline{U}_{2j+1}^{(n+1)}, & \text{if } 2j+1, \end{cases}$$

so for an arbitrary positive integer n and for any $2^{n+1} > i \in \mathbf{N}_0$

$$\begin{pmatrix} \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix} \underline{e}^{(n+1;i)} = \underline{U}_i^{(n+1)}.$$

This means that every column of $\begin{pmatrix} \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix}$ is equal to the column of the same index of $\mathbf{U}^{(n+1)}$, that proves that $\begin{pmatrix} \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix} = \mathbf{U}^{(n+1)}$.

Similarly, if $2^n > i \in \mathbf{N}_0$ or $2^n > i - 2^n \in \mathbf{N}_0$, then

$$\underline{V}_i^{(n+1)} = \begin{pmatrix} \mathbf{V}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{V}^{(n)} \end{pmatrix} \underline{e}^{(n+1;i)} = \begin{pmatrix} \mathbf{V}^{(n)}\underline{e}^{(n;i)} \\ \mathbf{V}^{(n)}\underline{e}^{(n;i)} \end{pmatrix} = \begin{pmatrix} \underline{V}_i^{(n)} \\ \underline{V}_i^{(n)} \end{pmatrix} =$$

$$= \begin{cases} \begin{pmatrix} \underline{0}^{(n)} \\ \underline{0}^{(n)} \end{pmatrix} = \underline{0}^{(n+1)}, & \text{if } i = 2j, \\ \begin{pmatrix} \underline{A}_{2j}^{(n)} \\ \underline{A}_{2j}^{(n)} \end{pmatrix} = \underline{A}_{2j}^{(n+1)} = \underline{U}_{2j+1}^{(n+1)}, & \text{if } i = 2j+1, \end{cases}$$

and

$$\underline{V}_i^{(n+1)} = \begin{pmatrix} \mathbf{V}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{V}^{(n)} \end{pmatrix} \underline{e}^{(n+1;i)} = \begin{pmatrix} \mathbf{0}^{(n)}\underline{e}^{(n;i-2^n)} \\ \mathbf{V}^{(n)}\underline{e}^{(n;i-2^n)} \end{pmatrix} = \begin{pmatrix} \underline{0}^{(n)} \\ \underline{V}_{i-2^n}^{(n)} \end{pmatrix} =$$

$$= \begin{cases} \begin{pmatrix} \underline{0}^{(n)} \\ \underline{0}^{(n)} \end{pmatrix} = \underline{0}^{(n+1)}, & \text{if } i = 2j, \\ \begin{pmatrix} \underline{0}^{(n)} \\ \underline{A}_{2j}^{(n)} \end{pmatrix} = \underline{A}_{2j}^{(n+1)} = \underline{U}_{2j+1}^{(n+1)}, & \text{if } i = 2j+1, \end{cases}$$

respectively, so for any $2^{n+1} > i \in \mathbf{N}_0$,

$$\underline{V}_i^{(n+1)} = \begin{cases} \underline{0}^{(n+1)}, & \text{if } i = 2j, \\ \underline{U}_{2j+1}^{(n+1)}, & \text{if } i = 2j+1. \end{cases}$$

The next Corollary is a consequence of Theorem 1 again.

Corollary 8. *For any $n \in \mathbf{N}_0$, $\mathbf{A}^{(n)}$ has one and only one eigenvalue, which is equal to* 1.

Proof. The characteristic polynomial of $\mathbf{A}^{(n)}$ is $c^{(n)} = \lambda^{2^n} + 1$, and over $\mathbf{F}_2$ this polynomial is equal to $(\lambda + 1)^{2^n}$.

Now we deal with the eigenvectors belonging to the only eigenvalue 1 of the transform given by $\mathbf{A}^{(n)}$.

Theorem 9. $\mathbf{A}^{(0)} + \mathbf{I}^{(0)} = \mathbf{0}^{(0)}$, *and if* $n > 0$, *then* $\mathbf{A}^{(n+1)} + \mathbf{I}^{(n+1)} \equiv$ $\equiv \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \end{pmatrix}$. *The only eigenvector of* $\mathbf{A}^{(0)}$ *is* $\underline{e}^{(0;0)}$, *and the eigenvectors of* $\mathbf{A}^{(n)}$, *if* $n > 0$, *are all of the vectors of the* 2^{n-1}*-dimensional linear space spanned by the columns of the matrix* $\begin{pmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{I}^{(n-1)} \end{pmatrix}$.

Proof. $\mathbf{A}^{(0)} + \mathbf{I}^{(0)} = \mathbf{0}^{(n)}$ is obvious. If $n > 0$, then

$$\begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{A}^{(n)} \\ \mathbf{I}^{(n)} & \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \end{pmatrix} \begin{pmatrix} \mathbf{A}^{(n)} + \mathbf{I}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \end{pmatrix} = \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \end{pmatrix},$$

so

$$\mathbf{A}^{(n+1)} + \mathbf{I}^{(n+1)} \equiv \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)} + I^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \end{pmatrix},$$

and

$$\begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \end{pmatrix} \begin{pmatrix} \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix} = \begin{pmatrix} \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} \end{pmatrix}.$$

As $\operatorname{rank}\left(\mathbf{A}^{(n+1)} + \mathbf{I}^{(n+1)}\right) = \operatorname{rank}\left(\begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \end{pmatrix}\right) = \operatorname{rank}\left(\mathbf{I}^{(n)}\right) =$ $= 2^n$, and $\mathbf{A}^{(n+1)}$ is a regular quadratic matrix of order 2^{n+1}, so the nullspace of $\mathbf{A}^{(n+1)} + \mathbf{I}^{(n+1)}$ is a 2^n-dimensional linear space. But $\operatorname{rank}\left(\begin{pmatrix} \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix}\right) =$ $= \operatorname{rank}\left(\mathbf{I}^{(n)}\right) = 2^n$, and this proves the second half of the statement.

Corollary 10. *For $n > 0$ the eigenvectors of $\mathbf{A}^{(n)}$ are of the form $\begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu} \\ \underline{\nu} \end{pmatrix}$, where $\underline{\nu}$ is an arbitrary vector of the 2^{n-1}-dimensional linear space.*

Proof.

$$\begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu} \\ \underline{\nu} \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{I}^{(n-1)} \end{pmatrix} \underline{\nu},$$

so $\begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu} \\ \underline{\nu} \end{pmatrix}$ is a linear combination of the columns of

$$\begin{pmatrix} \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix}.$$

The form of the eigenvectors given above by $\begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu} \\ \underline{\nu} \end{pmatrix}$ shows, that if $\underline{\nu} = \begin{pmatrix} \underline{\nu}^{(0)} \\ \underline{\nu}^{(1)} \end{pmatrix}$ is an eigenvector of $\mathbf{A}^{(n)}$, then $\underline{\nu}^{(0)}$ is an eigenvector of $\mathbf{A}^{(n-1)}$. The details are in the next corollary.

Corollary 11. *Let* $n \in \mathbf{N}$, *and* $\underline{\nu} = \begin{pmatrix} \underline{\nu}^{(0)} \\ \underline{\nu}^{(1)} \end{pmatrix}$ *and* $\underline{\tilde{\nu}} = \begin{pmatrix} \underline{\tilde{\nu}}^{(0)} \\ \underline{\tilde{\nu}}^{(1)} \end{pmatrix}$ *two eigenvectors of* $\mathbf{A}^{(n)}$. *Then* $\underline{\nu}^{(0)} = \underline{\tilde{\nu}}^{(0)}$ *if and only if* $\underline{\nu}^{(1)} - \underline{\tilde{\nu}}^{(1)}$ *belongs to the nullspace of* $\mathbf{A}^{(n-1)}$.

Proof. $\left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu}^{(1)} = \underline{\nu}^{(0)} = \underline{\tilde{\nu}}^{(0)} = \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\tilde{\nu}}^{(1)}$ is true if and only if $\left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \left(\underline{\nu}^{(1)} - \underline{\tilde{\nu}}^{(1)}\right) = \underline{0}$, that is if and only if $\underline{\nu}^{(1)} - \underline{\tilde{\nu}}^{(1)}$ is an eigenvector of $\mathbf{A}^{(n-1)}$.

Earlier we saw that the 2^n-dimensional space is the direct sum of 2^{n-1} two-dimensional cyclic subspaces invariant to the transform of the space determined by $\mathbf{A}^{(n)}$ in the canonical basis of the space. We saw as well, that each element of the set of the vectors $\underline{e}^{(n;2i)}$, where $0 \leq i < 2^{n-1}$, belongs to different components of these subspaces, and these vectors are cyclic with respect to $\mathbf{A}^{(n)}$ in the subspaces containing them. Let $\mathcal{P}^{(n)}$ denote the nullspace of $\mathbf{A}^{(n)} + \mathbf{I}^{(n)}$. As we have altogether 2^{n-1} different vectors of the form $\underline{e}^{(n;2i)}$, and these vectors are pairwise linearly independent, the set of all of the linear combinations of these vectors, denoted by $\mathcal{E}^{(n)}$, is a 2^{n-1}-dimensional linear space over $\mathbf{F}_2$, containing therefore $2^{2^{n-1}}$ vectors. Let $\mathcal{T}^{(n)}$ denote the 2^n-dimensional linear space over $\mathbf{F}_2$. Then we get the following theorem.

Theorem 12. $\mathcal{E}^{(n)}$ *is a direct complementary subspace of* $\mathcal{P}^{(n)}$.

Proof. Suppose $\underline{u}$ is a common element of the two subspaces. Then on one hand $\underline{u} = \sum_{i=0}^{2^{n-1}-1} \lambda_i \underline{e}^{(n;2i)}$, and on the other hand $\left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right) \underline{u} = \underline{0}$, so

$$\underline{0} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right) \underline{u} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right) \sum_{i=0}^{2^{n-1}-1} \lambda_i \underline{e}^{(n;2i)} =$$

$$= \sum_{i=0}^{2^{n-1}-1} \lambda_i \left(\left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right) \underline{e}^{(n;2i)}\right) = \sum_{i=0}^{2^{n-1}-1} \lambda_i \left(\left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right) \underline{U}_{2i}^{(n)}\right) =$$

$$= \sum_{i=0}^{2^{n-1}-1} \lambda_i \left(\mathbf{A}^{(n)} \underline{U}_{2i}^{(n)} + \underline{U}_{2i}^{(n)}\right) = \sum_{i=0}^{2^{n-1}-1} \lambda_i \left(\underline{U}_{2i+1}^{(n)} + \underline{U}_{2i}^{(n)}\right) = \sum_{i=0}^{2^n-1} \mu_i \underline{U}_i^{(n)},$$

where for $2^{n-1} > i \in \mathbf{N}_0$ $\mu_{2i} = \lambda_i = \mu_{2i+1}$. But the columns of $\mathbf{U}^{(n)}$ are linearly independent, so $\sum_{i=0}^{2^n-1} \mu_i \underline{U}_i^{(n)} = 0$ is possible if and only if all of the coefficients μ_i, and then every λ_i, are equal to 0. This means that the intersection of the subspaces $\mathcal{E}^{(n)}$ and $\mathcal{P}^{(n)}$ contains one and only one element, the zero vector. As both $\mathcal{E}^{(n)}$ and $\mathcal{P}^{(n)}$ is a 2^{n-1}-dimensional linear space over $\mathbf{F}_2$, and

the dimension of $\mathcal{T}^{(n)}$ is equal to $2^n = 2 \cdot 2^{n-1} = 2^{n-1} + 2^{n-1}$, we get that $\mathcal{T}^{(n)} = \mathcal{E}^{(n)} + \mathcal{P}^{(n)}$.

Corollary 13. *For any* $n \in \mathbf{N}$

$$\mathcal{P}^{(n)} = \left\{ \begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu} \\ \underline{u} + \underline{\nu} \end{pmatrix} \;\middle|\; \underline{u} \in \mathcal{P}^{(n-1)} \wedge \underline{\nu} \in \mathcal{E}^{(n-1)} \right\}.$$

Proof. The elements of $\mathcal{P}^{(n)}$ are vectors of the form

$$\begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{w} \\ \underline{w} \end{pmatrix},$$

where $\underline{w}$ is an arbitrary element of $\mathcal{T}^{(n-1)}$. But there is exactly one $(\underline{u}, \underline{\nu}) \in \in \mathcal{E}^{(n-1)} \times \mathcal{P}^{(n-1)}$ pair so, that $\underline{w} = \underline{u} + \underline{\nu}$, and then

$$\left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{w} = \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) (\underline{u} + \underline{\nu}) = \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\nu},$$

as $\left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{u} = \underline{0}$.

Earlier we gave a generator system of $\mathcal{P}^{(n)}$ if $n > 0$, namely the columns of the matrix $\begin{pmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{I}^{(n-1)} \end{pmatrix}$. From the previous results follows, that the following set of vectors generates $\mathcal{P}^{(n)}$, too.

Corollary 14. *Let* $G^{(n)}$ *a basis of* $\mathcal{P}^{(n)}$ *for any nonnegative integer* n. *Then*

$$G^{(n+1)} := \left\{ \begin{pmatrix} \lambda \left(\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}\right) \\ \lambda \underline{U}_{2i}^{(n)} + \mu \underline{u} \end{pmatrix} \;\middle|\; 2^{n-1} > i \in \mathbf{N}_0 \wedge \underline{u} \in G^{(n)} \wedge \lambda + \mu = 1 \right\}$$

is a possible basis of $\mathcal{P}^{(n)}$.

Proof. With the n-dimensional $\underline{e}^{(n;2i)}$ vectors, $\left\{\underline{e}^{(n;2i)} \mid 2^{n-1} > i \in \mathbf{N}_0\right\} \cup \cup G^{(n)}$ is a basis of $\mathcal{T}^{(n)}$. As

$$\begin{aligned} &\left\{\lambda \underline{e}^{(n;2i)} + \mu \underline{u} \mid 2^{n-1} > i \in \mathbf{N}_0 \wedge \underline{u} \in G^{(n)} \wedge \lambda + \mu = 1\right\} = \\ &\quad = \left\{\underline{e}^{(n;2i)} \mid 2^{n-1} > i \in \mathbf{N}_0\right\} \cup \left\{\underline{u} | \underline{u} \in G^{(n)}\right\} = \\ &\quad = \left\{\underline{e}^{(n;2i)} \mid 2^{n-1} > i \in \mathbf{N}_0\right\} \cup G^{(n)}, \end{aligned}$$

so

$$G^{(n+1)} :=$$

$$:= \left\{ \begin{pmatrix} \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right)\left(\lambda \underline{e}^{(2i)} + \mu \underline{u}\right) \\ \lambda \underline{e}^{(2i)} + \mu \underline{u} \end{pmatrix} \;\middle|\; 2^{n-1} > i \in \mathbf{N}_0 \wedge \underline{u} \in G^{(n)} \wedge \lambda + \mu = 1 \right\}$$

is a basis of the nullspace of the 2^{n+1}-dimensional space over $\mathbf{F}_2$. But $\underline{e}^{(2i)} = \underline{U}_{2i}^{(n)}$, and

$$\left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right)\left(\lambda \underline{U}_{2i}^{(n)} + \mu \underline{u}\right) = \lambda \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right) \underline{U}_{2i}^{(n)} = \lambda \left(\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}\right),$$

that proves the statement of Corollary 14.

We give another two bases of $\mathcal{P}^{(n)}$.

Theorem 15. *$\left\{\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)} \mid 2^{n-1} > i \in \mathbf{N}_0\right\}$ and the columns of $\begin{pmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{A}^{(n-1)} \end{pmatrix}$ are bases of $\mathcal{P}^{(n)}$ for any positive integer n.*

Proof. $\begin{pmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{A}^{(n-1)} \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{I}^{(n-1)} \end{pmatrix} \mathbf{A}^{(n-1)}$, and $\mathbf{A}^{(n-1)}$ is regular, so the second statement of the theorem is true.

$\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)} = \underline{U}_{2j}^{(n)} + \underline{U}_{2j+1}^{(n)}$ if and only if $\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)} + \underline{U}_{2j}^{(n)} + \underline{U}_{2j+1}^{(n)} = \underline{0}$. This equality is possible if and only if two of the members of the sum on the left side are identical, and similar is true for the other two members of the sum (of course it is possible that all the four components are identical). Suppose $i \leq j$. As in $\underline{U}_{2i}^{(n)}$ and in $\underline{U}_{2j}^{(n)}$ there is exactly one nonzero value, and in the columns of $\mathbf{A}^{(n)}$ excluding the last one there are at least two nonzero components, $\underline{U}_{2i}^{(n)} \neq \underline{U}_{2i+1}^{(n)} \neq \underline{U}_{2j}^{(n)} \neq \underline{U}_{2j+1}^{(n)} \neq \underline{U}_{2i}^{(n)}$. In that case the only possibility is, that $\underline{U}_{2i}^{(n)} = \underline{U}_{2j}^{(n)}$ and $\underline{U}_{2i+1}^{(n)} = \underline{U}_{2j+1}^{(n)}$, and this is true if and only if $i = j$. That means, the elements of the set given in the theorem are pairwise linearly independent. The cardinality of that set is 2^{n-1}, so the space spanned by these vectors is a 2^{n-1}-dimensional linear subspace of $\mathcal{T}^{(n)}$. Finally, if we choose an arbitrary element of the set, for instance $\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}$, then

$$\mathbf{A}^{(n)}\left(\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}\right) = \mathbf{A}^{(n)}\underline{U}_{2i}^{(n)} + \mathbf{A}^{(n)}\underline{U}_{2i+1}^{(n)} =$$
$$= \underline{U}_{2i+1}^{(n)} + \underline{U}_{2i}^{(n)} = \underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)},$$

so $\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}$ is an eigenvector of the operator determined by $\mathbf{A}^{(n)}$ in the natural basis of $\mathcal{T}^{(n)}$, that is $\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}$ belongs to the nullspace of $\mathbf{A}^{(n)} + \mathbf{I}^{(n)}$.

Let us consider the 2^{n-1} cyclic invariant subspaces of the direct sum decomposition of $\mathbf{A}^{(n)}$ in which $\left\{\underline{U}_{2i}^{(n)}, \underline{U}_{2i+1}^{(n)}\right\}$ is a basis in the i-th subspace. Then $\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}$ is an eigenvector of that subspace, and from this follows the following corollary.

Corollary 16. *A possible basis for* $\mathbf{C}^{(n)}$ *is the set*

$$\left\{\underline{U}_{2i}^{(n)}, \underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)} \mid 0 \leq i < 2^{n-1}\right\}.$$

Now let us consider two properties of the eigenvectors of $\mathbf{A}^{(n)}$.

Corollary 17.

1. *For an arbitrary* $\underline{\nu} \in \mathcal{T}^{(n)}$, $\underline{\nu} + \mathbf{A}^{(n)}\underline{\nu}$ *is an eigenvector of* $\mathbf{A}^{(n)}$.
2. *If* $n > 0$, *and* $\underline{u}$ *is an eigenvector of* $\mathbf{A}^{(n)}$, *then* $u_0 = 0$, *and if* $\underline{u} \neq \underline{0}$, *then for at least one* $2^{n-1} \leq i < 2^n$, $u_i = 1$.

Proof.

1. $\mathbf{A}^{(n)}\left(\underline{\nu} + \mathbf{A}^{(n)}\underline{\nu}\right) = \mathbf{A}^{(n)}\underline{\nu} + \underline{\nu} = \underline{\nu} + \mathbf{A}^{(n)}\underline{\nu}$.
2. $\left\{\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)} \mid 0 \leq i < 2^{n-1}\right\}$ is a basis of the linear space of the eigenvectors of $\mathbf{A}^{(n)}$. As for any $2^{n-1} > i \in \mathbf{N}_0$, the 0-th component of $\underline{U}_{2i}^{(n)} + \underline{U}_{2i+1}^{(n)}$ is equal to 0, the 0-th component of every vector of the linear space of the eigenvectors of $\mathbf{A}^{(n)}$ is 0.

Any eigenvector $\underline{u}$ of $\mathbf{A}^{(n)}$ is of the form $\begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{\nu} \\ \underline{\nu} \end{pmatrix}$, where $\underline{\nu}$ is an arbitrary vector of $\mathcal{T}^{(n-1)}$. If $\underline{\nu} = \underline{0}$, then $\left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{\nu} = \underline{0}$, and then $\underline{u} = \underline{0}$.

The first part of the second statement means that every eigenvector of the transform given by $\mathbf{A}^{(n)}$ in the natural basis of $\mathcal{T}^{(n)}$ lies in the subspace of $\mathcal{T}^{(n)}$ generated of the vectors of the natural basis of $\mathcal{T}^{(n)}$, but $\underline{e}^{(n;0)}$.

Finally, let us consider the eigenvectors of $\mathbf{A}^{(n)}$, if $0 \leq n \leq 3$.

1) If $n = 0$, then $\mathbf{A}^{(0)} = (1) = \mathbf{I}^{(n)}$, so every vector of $\mathcal{T}^{(0)}$ is the eigenvector of $\mathbf{A}^{(0)}$. $\mathcal{T}^{(0)}$ has two vectors, $\underline{0}^{(0)}$ and $\underline{e}^{(0;0)} = (1)$.

2) If $n = 1$, then $\begin{pmatrix} \mathbf{A}^{(0)} + \mathbf{I}^{(0)} \\ \mathbf{I}^{(0)} \end{pmatrix} = \begin{pmatrix} 1+1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is a basis of the space of the eigenvectors of $\mathbf{A}^{(1)}$, so $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are the eigenvectors.

3) If $n = 2$, then $\begin{pmatrix} \mathbf{A}^{(1)} + \mathbf{I}^{(1)} \\ \mathbf{I}^{(1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ are the eigenvectors of $\mathbf{A}^{(2)}$.

4) If $n = 3$, then $\begin{pmatrix} \mathbf{A}^{(2)} + \mathbf{I}^{(2)} \\ \mathbf{I}^{(2)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, and the columns of the matrix

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

are the eigenvectors of $\mathbf{A}^{(3)}$.

References

[1] **Abbott J.C.,** *Sets, lattices, and Boolean algebras,* Allyn and Bacon, Boston, Mass., 1964.

[2] **Flegg H.G.,** *Boolean algebra and its application,* Wiley, New York, 1964.

[3] **Halmos P.R.,** *Finite-dimensional vector spaces,* Springer, New York, 1974.

[4] **Kérchy L.,** *Bevezetés a véges dimenziós vektorterek elméletébe (An introduction to the theory of the finite-dimensional vector spaces)*, Polygon, Szeged, 1997.

[5] **Akers S.H.,** On the theory of Boolean functions, *J. SIAM,* **7** (1959), 487-498.

[6] **Gonda J.,** Transformation of the canonical disjunctive normal form of a Boolean function to its Zhegalkin-polynomial and back, *Annales Univ. Sci. Budapest. Sect. Comp.,* **20** (2001), 147-156.

(Received September 24, 2002)

J. Gonda
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter s. 1/C
H-1117 Budapest, Hungary