Algebraic Properties of the Zhegualkin Transformation

Krassimir N. Manev

[1] Department of Mathematics and Computer Science, Sofia University,
1164 Sofia, Bulgaria
[2] American University in Bulgaria, 2700 Blagoevgrad, Bulgaria

Abstract. Usually Boolean functions are presented with Disjunctive Normal Forms (DNF). I. I. Zhegualkin introduced in consideration the complete set of Boolean functions - conjunction, addition modulo 2 and both constants. The formulae over this set are the polynomials modulo 2, called *Zhegualkin polynomials* (or *reduced polynomials* too). Zhegualkin polynomials have some advantages comparing with DNF's. For example, they have good algebraic properties - the set of polynomials of n variables could be considered as a group, ring, linear space, etc. This paper presents some algebraic properties of the polynomials modulo 2, considered as a linear vector space, which could be used for deriving of efficient algorithms.

1 Introduction

In the theory of the Boolean functions the formulae over disjunction, conjunction and negation are preferred to present functions, as well as for implementing them in electronic circuits. There are many reasons for this. Historically this was the first set of Boolean functions proved to be complete, e.i. each Boolean function is presented with a formula over the set. Given the table of the function it is too easy to write the corresponding formula - the perfect Disjunctive Normal Form (DNF). These three functions, plus implication, equivalence and both constants were enough to formalize the traditional logic in natural way. And last but not the least, in the programming languages disjunction, conjunction and negation are used for composing logical expressions, that is why in the world of programmers these three functions are well known.

In late 20's I. I. Zhegualkin [1] started to use another complete set of Boolean functions - conjunction, addition modulo 2 and both constants. The formulae over this set are the polynomials modulo 2, called *Zhegualkin polynomials* (or *reduced polynomials* too). Zhegualkin polynomials have some advantages comparing with DNF's. For example, they have good algebraic properties - the set of polynomials of n variables could be considered as a group, ring, linear space, etc. Very important class of error correcting codes - the codes of Read-Muller are defined in terms of Zhegualkin polynomials and any result in the arrea is important for the development of the theory.

The main purpose of this paper is to present some algebraic properties of the polynomials modulo 2, considered as a linear vector space, which could be used for deriving of efficient algorithms.

2 Definitions and Preliminary Results

Let N be the set of the natural numbers, $N = \{0, 1, 2, \ldots\}$. For each $i \in N$, $0 \leq i < 2^n$, $n \in N$,$n \geq 1$, let $\sigma_{n-1}\sigma_{n-2}\ldots\sigma_0$ be the binary presentation of i, i.e. $i = \sigma_{n-1}2^{n-1} + \sigma_{n-2}2^{n-2} + \cdots + \sigma_0 2^0$, where $\sigma_i \in \{0, 1\}$ for $i = n-1$,$n-2, \ldots, 0$. We will call i an *index* of the binary vector $(\sigma_{n-1}, \sigma_{n-2}, \ldots, \sigma_0) \in \{0, 1\}^n$ and will denote $i = \nu(\sigma_{n-1}, \sigma_{n-2}, \ldots, \sigma_0)$. If $i \neq 0$ then at least one of $\sigma_{n-1}, \sigma_{n-2}, \ldots, \sigma_0$ is not zero, so we could define a *carrier* of i as $car(i) = \{i_1, i_2, \ldots, i_r\}$, where $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_r}$ are all non zero coefficients in the binary presentation of i. Even if it does not mater, we will supose $i_1 > i_2 > \ldots > i_r$. We will denote with $\#(i)$ the number r of the nonzero binary digits of i. For $i = 0$ we have $car(0) = \emptyset$ and $\#(0) = 0$. Let $2^f X$ be the family of all finite subsets of the set X. The function $car : N \longrightarrow 2^{fN}$ is bijective one and we can define its inverse function $car^{-1} : 2^{fN} \longrightarrow N$, such that $car^{-1}(\{i_1, i_2, \ldots, i_r\}) = i$.

Function $\# : N \longrightarrow N$ is defined by the recurrence equation:

$$\begin{aligned}
&\#(0) = 0;\\
&\#(i) = \#(i - 2^{n-1}) + 1,\ 2^{n-1} \leq i < 2^n, n \geq 1
\end{aligned}$$

and the function $car : N \longrightarrow 2^{fN}$ - with the recurrence equation:

$$\begin{aligned}
&car(0) = \emptyset;\\
&car(i) = car(i - 2^{n-1}) \cup \{n-1\},\ 2^{n-1} \leq i < 2^n, n \geq 1.
\end{aligned}$$

The functions $\mathcal{F}_2 = \{f | f : \{0, 1\}^i \longrightarrow \{0, 1\}, i = 1, 2, \ldots\}$ are called *Boolean functions* of n variables. We will denote by $\mathcal{F}_2^n$ the set of Boolean functions of n variables. For each Boolean function $f(x_{n-1}, x_{n-2}, \ldots, x_0)$ exists a formula over the set of Boolean functions $\{xy, x \oplus y, \tilde{0}, \tilde{1}\}$ where xy and $x \oplus y$ are the multiplication and the addition of the finite field $GF(2)$ (the modulo 2 field) and $\tilde{0}$ and $\tilde{1}$ are the both constant functions. Using the obvious properties: $f \oplus f = 0$, $g \oplus 0 = g$ and $xx = x$, each such formula is easy reducible to a polynomial of the n variables and coefficients from $\{0, 1\}$, such that each monomial is included no more than once and each variable included is of degree one. We will call this polynomial *reduced* or *Zhegualkin polynomial* of the function. Each Boolean function have unique Zhegualkin polynomial. For fixed n there are 2^n different possible monomials (using the value 1 for denoting the monomial without variables). Let denote the corresponding coefficients with $a_0, a_1, \ldots, a_{2^n-1}$, where a_i is the coefficient of the monomial $x_{j_1}x_{j_2}\ldots x_{j_{\#(i)}}$, $\{j_1, j_2, \ldots j_{\#(i)}\} = car(i)$. We will denote by $P_n[a_0, a_1, \ldots, a_{2^n-1}]$ the general form of the reduced polynomial of n variables with coefficients $a_0, a_1, \ldots, a_{2^n-1}$. For example the general forms of the polynomials of 1,2 and 3 variables are:

$$\begin{aligned}
&a_0 \oplus a_1x_0\\
&a_0 \oplus a_1x_0 \oplus a_2x_1 \oplus a_3x_1x_0\\
&a_0 \oplus a_1x_0 \oplus a_2x_1 \oplus a_3x_1x_0 \oplus a_4x_2 \oplus a_5x_2x_0 \oplus a_6x_2x_1 \oplus a_7x_2x_1x_0
\end{aligned}$$

If $f \neq \tilde{0}$ we will not write the monomials with zero coefficients in the formula and will omit the coefficients which are ones. In the polynomial of the constant $\tilde{0}$ all coefficients are 0 and we will denote it with 0. For example, if the function is conjunction $a_0 = a_1 =$

$a_2 = 0$ and the corresponding polynomial is just $x_1 x_0$. If the function is disjunction then $a_0 = 0$ and the corresponding polynomial is $x_0 \oplus x_1 \oplus x_1 x_0$. Finally, the polynomial of negation is $1 \oplus x_0$.

3 Zhegualkin Transformation

Let $f(x_{n-1}, x_{n-2}, \ldots, x_0) \in \mathcal{F}_2^n$. Let $\tilde{a}(a_0, a_1, \ldots, a_{2^n-1})$ be the vector of coefficients of its Zhegualkin polynomial and $f(\sigma_{n-1}, \sigma_{n-2}, \ldots, \sigma_0) = b_{\nu(\sigma_{n-1}, \sigma_{n-2}, \ldots, \sigma_0)}$, so $\tilde{b}(b_0, b_1, \ldots, b_{2^n-1})$ is the vector of values of the function f. In this section we will study the properties of the function $ZH_n : \{0,1\}^{2^n} \longrightarrow \{0,1\}^{2^n}$ such that $ZH_n(\tilde{b}) = \tilde{a}$, i.e. the function that calculate the polynomial of a given Boolean function. The function ZH_n is well defined and bijective because of the uniqueness of the Zhegualkin polynomial for each Boolean function.

It is obvious that ZH_n is a linear transformation of the n-dimensional linear vector spaces $GF(2)^n$ over the field $GF(2)$. Really, replacing each of the elements of $\{0,1\}^n$ in the general form of the Zhegualkin polynomial of n variables and equalizing to the values of the given function for the corresponding elements of $\{0,1\}^n$ we will obtain a system of 2^n linear equations for the unknown coefficients of the polynomial of the function. The system has unique solution because of the existence and the uniqueness of the polynomial. We will call ZH_n *Zhegualkin transformation.*

Let $M_n = ||m_{i,j}||, i = 0, 1, \ldots, 2^n - 1$ and $j = 0, 1, \ldots, 2^n - 1$ is the matrix of the linear transformation ZH_n, i.e. $M_n \tilde{b} = \tilde{a}^t$. Below the matrices M_1 and M_2 are given explicitly:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Theorem 31 *Let* $2^{car(i)} = \{S_0, S_1, \ldots, S_{2^{\#(i)}-1}\}$. *Then* $m_{i,j} = 1$ *iff* $j \in \{car^{-1}(S_0), car^{-1}(S_1), \ldots, car^{-1}(S_{2^{\#(i)}-1})\}$, *i.e. iff* $car(j) \subseteq car(i)$.

The proof of the theorem follows directly from the definition of the general form of the reduced polynomial of n variables.

Theorem 32 *For the elements of* M_n *the following properties hold:*

a. $m_{i,0} = m_{2^n-1,i} = 1, i = 0, 1, \ldots, 2^n - 1$;
b. $m_{i,i} = 1, i = 0, 1, \ldots, 2^n - 1$;
c. $m_{i,j} = 0, i = 0, 1, \ldots, 2^n - 1, j > i$;
d. $m_{i,2^n-1-i} = 0, i = 0, 1, \ldots, 2^n - 2$;
e. $m_{i,j} = m_{2^n-1-j,2^n-1-i}, i, j \in \{0, 1, ..., 2^n - 1\}$.

Proof: The proofs of all these properties are based on Theorem 21.

a. $m_{i,0} = 1$, because $car(0) = \emptyset \in car(i), i = 0, 1, \ldots, 2^n - 1$. From $car(2^n - 1) = \{n-1, n-2, \ldots, 0\}$ it follows that $\forall i, 0 \leq i \leq 2^n - 1(car(i) \subseteq car(2^n - 1))$ and then $m_{2^n-1,i} = 1$.

b. $m_{i,i} = 1$ because $\forall i, 0 \leq i \leq 2^n - 1(car(i) \subseteq car(i))$.

c. $m_{i,j} = 0$ when $j > i$ because $car(j) \not\subseteq car(i)$.

d. $m_{i,2^n-1-i} = 0$ because $car(i) \cap car(2^n - 1 - i) = \emptyset$ and then $car(2^n - 1 - i) \not\subseteq car(i), i = 0, 1, \ldots, 2^n - 2$.

e. If $i+j = 2^n-1$ then $m_{i,j}$ and $m_{2^n-1-j,2^n-1-i}$ are the same element of the matrix, so the equality holds. Let $i + j \neq 2^n - 1$. It is clear that $\{car(k), car(2^n - 1 - k)\}$ is a partition of $\{0, 1, \ldots, 2^n - 1\}$ and each x of $\{0, 1, \ldots, 2^n - 1\}$ belongs to exactly one of the parts. If $m_{i,j} = 0$ then $car(j) \not\subseteq car(i)$ and then $\exists x \in car(j), x \notin car(i)$. But then $x \in car(2^n-1-i), x \notin car(2^n-1-j)$, that means $car(2^n-1-i) \not\subseteq car(2^n-1-j)$ and $m_{2^n-1-j,2^n-1-i} = 0$ too. If $m_{i,j} = 1$ then $car(j) \subseteq car(i)$, that means $car(2^n-1-i) \subseteq car(2^n - 1 - j)$ and $m_{2^n-1-j,2^n-1-i} = 1$ too. $\diamondsuit$

Theorem 33 *For each $n > 1$ the matrix M_n of the Zhegualkin transformation is defined by*

$$M_n = \begin{pmatrix} M_{n-1} & O_{n-1} \\ M_{n-1} & M_{n-1} \end{pmatrix}$$

where O_{n-1} is the matrix of size $2^{n-1} \times 2^{n-1}$ consisting of zeros.

Proof: First 2^{n-1} lines of M_n are obtained from the vectors of $\{0,1\}^n$ for which $x_{n-1} = 0$. This will reduce the general form of the polynomial of n variables to the general form of the polynomials of $n - 1$ variables, which will result to M_{n-1} in first 2^{n-1} columns. We will obtain O_{n-1} in the last 2^{n-1} columns because of Theorem 22.c. The last 2^{n-1} lines of M_n will be obtained from the vectors for which $x_{n-1} = 1$. In this case the general form of the polynomial will be reduced to

$$P[a_0, a_1, \ldots, a_{2^{n-1}-1}] \oplus P[a_{2^{n-1}}, a_{2^{n-1}+1}, \ldots a_{2^n-1}]$$

which will give us M_{n-1} in the first 2^{n-1} columns as well as in the last $2^{n-1} ones.\diamondsuit$

Theorem 34 *For each natural $n \geq 1$, $M_n^{-1} = M_n$.*

Proof: Let I_n be the matrix of size $2^n \times 2^n$ with 1's on the main diagonal and all other elements equal 0. For $n = 1$ obviously $M_1^2 = I_1$ and then $M_1^{-1} = M_1$. Suppose the statement is true for $n = k - 1$. We will prove that it is true for $n = k$. Really, using the Theorem 23. we will obtain

$$M_k^2 = \begin{pmatrix} M_{k-1} & O_{k-1} \\ M_{k-1} & M_{k-1} \end{pmatrix} \begin{pmatrix} M_{k-1} & O_{k-1} \\ M_{k-1} & M_{k-1} \end{pmatrix} =$$

$$= \begin{pmatrix} M_{k-1}^2 \oplus O_{k-1}M_{k-1} & M_{k-1}O_{k-1} \oplus O_{k-1}M_{k-1} \\ M_{k-1}^2 \oplus M_{k-1}^2 & M_{k-1}O_{k-1} \oplus M_{k-1}^2 \end{pmatrix} =$$

$$= \begin{pmatrix} I_{k-1} & O_{k-1} \\ O_{k-1} & I_{k-1} \end{pmatrix} = I_k,$$

the statement is true for $n = k$ too and the theorem was proved.$\Diamond$

Let n and q be natural numbers, $n \geq 1$ and $q \geq 1$. If we replace in M_n each 1 with M_q and each 0 with O_q we will Obtain a new matrix of size $2^{n+q} \times 2^{n+q}$ which will be called *q-expansion* of M_n. The 1-expansion of M_1 is obviously M_2, the 1-expansion of M_2 as well as the 2-expansion of M_1 is M_3. Using Theorem 23. it is easy to prove the following

Theorem 35 *For each natural n and q, $n \geq 1$, $q \geq 1$, the q-expansion of M_n is M_{n+q}.*

If, vice versa, we split the matrix M_{n+q} to submatrices of size $2^q \times 2^q$ we will obtain only two types - either M_q or O_q. Replacing each M_q with 1 and each O_q with 0 we will obtain a new matrix of size $2^n \times 2^n$ which is called *q-contraction* of M_{n+q}. As the previous statement suggests it is true the following

Theorem 36 *For each natural n and q, $n \geq 1$, $q \geq 1$, the q-contraction of M_{n+q} is M_n.*

The above mentioned properties demonstrated that the matrix M_n of the Zhegualkin transformation is a very symmetric one. Looking at the figure below, presenting only the 1's of M_4, it is easy to see the similarity to the famous fractal called *triangle of Serpinsky.* We will call this phenomenon *discrete fractal.*

```
1
11
1 1
1111
1   1
11  11
1 1 1 1
11111111
1       1
11      11
1 1     1 1
1111    1111
1   1   1   1
11  11  11  11
1 1 1 1 1 1 1 1
1111111111111111
```

Figure. The matrix of ZH_4

Studying the discrete fractals is far beyond the goals of this paper. But the analogy with the fractals suggests that the Zhegualkin transformation could have some good algorithmic properties. That is why in [2] these properties was studied and very efficient algorithm for applying the transformation was obtained. Briefly, if the table of the values of a Boolean function is given the coefficients of the corresponding reduced polynomial are just the result of the Zhegualkin transformation applied to the given values. That means the corresponding system of $m = 2^n$ linear equations have to be solved in the field $GF(2)$. Of course the matrix is triangular (see Theorem 22.c.) and instead of the usual $O(m^3)$ operation of the method of Gauss, only $O(m^2)$ are enough for the back passing of the method. But this algorithm do not use the properties of M_n. Using the properties of the matrix M_n we obtained the following

Algorithm:

```
integer n,m=2^n,k=1,i,j,s
binary b[0..2^n]
for i=1 to n do
{
   for s=k to m-k step 2*k
      for j=s to s+k-1 do b[j]=b[j] XOR b[j-k]
   k=2*k
}
```

The values of the function are given in the array b, the coefficients of the corresponding polynomial are obtained in the same array. No additional memory is necessary and the values of M_n are not used at all. The time complexity of this algorithm is $O(m \lg m)$ and it was conjectured that no algorithm which is asymptotically better. Moreover, from Theorem 24 it is clear that the same algorithm could be used for performing the inverse of the Zhegualkin transformation, i.e given the polynomial of a Boolean function to find the table of its values.

4 Fixed Points of Zhegualkin Transformation

In this section we will study the fixed points of the Zhegualkin transformation. As usually the vector $\tilde{a}$ is called *fixed point* of the linear transformation if $M_n\tilde{a}^t = \tilde{a}$.

The constant function $\tilde{0}$ is a fixed point of ZH_n, because $M_n\tilde{0}^t = \tilde{0}$. Something more, the set of fixed points is closed under the addition modulo 2, because if $\tilde{a_1}$ and $\tilde{a_2}$ are fixed points then $M_n(\tilde{a_1} \oplus \tilde{a_2})^t = M_n\tilde{a_1}^t \oplus M_n\tilde{a_2}^t = \tilde{a_1} \oplus \tilde{a_2}$. In such a way we proved the following

Theorem 41 *The set of all fixed points of the linear transformation ZH_n is a subspace of the linear space of $GF(2)^n$.*

We will denote the linear subspace of the fixed points of ZH_n with $\mathcal{X}(ZH_n)$. For finding the dimension of $\mathcal{X}(ZH_n)$ we have to study the matrix $M_n \ominus I_n$, or $M_n \oplus I_n$, which is the same in $GF(2)$. We still have not an elegant proof of the following fundamental fact.

Theorem 42 *For each natural $n \geq 1$,* $\operatorname{rank}(M_n \oplus I_n) = 2^{n-1}$.

Now for the number of the fixed points of ZH_n we have

Theorem 43 *For each natural $n \geq 1$, $|\mathcal{X}(ZH_n)| = 2^{2^{n-1}}$.*

Proof: $|\mathcal{X}(ZH_n)|$ is exactly the number of solutions of the system of 2^n linear equations $(M_n \oplus I_n)\tilde{x} = \tilde{0}$. That is why $|\mathcal{X}(ZH_n)| = 2^{2^n - \mathrm{rank}(M_n \oplus I_n)} = 2^{2^n - 2^{n-1}} = 2^{2^{n-1}}$. $\diamondsuit$.

It is interesting to mention here some analogy with another set of Boolean functions. The function $f^*(x_{n-1}, x_{n-2}, \ldots, x_0) = f(x_{n-1} \oplus 1, x_{n-2} \oplus 1, \ldots, x_0 \oplus 1) \oplus 1$ is called *dual* of the function f. The function $D_n : \{0,1\}^{2^n} \longrightarrow \{0,1\}^{2^n}$, such that $D_n(f) = f^*$ is an affine transformation of $\{0,1\}^{2^n}$. The fixed points of D_n are called *self-dual* Boolean functions. The set of self-dual functions is not subspace of the linear space of $GF(2)^n$, because $D_n(\tilde{0}) = \tilde{1}$ and so $\tilde{0}$ is not self-dual. Nevertheless, there are exactly $2^{2^{n-1}}$ self-dual functions of n variables, a fact which is very interesting to be compared with Theorem 3.3.

Let now try to make some classification of the functions of $\mathcal{X}(ZH_n)$. For each $f(x_{n-1}, x_{n-2}, \ldots, x_0) \in \mathcal{F}_2^n$ we define its *0-subfunction* f_0 and its *1-subfunction* f_1 using the trivial equality

$$f(x_{n-1}, x_{n-2}, \ldots, x_0) = f_0(x_{n-2}, x_{n-3}, \ldots, x_0) \oplus x_{n-1} f_1(x_{n-2}, x_{n-3}, \ldots, x_0).$$

We will denote with $f = (f_0, f_1)$ the fact that f_0 and f_1 are the subfunctions of f.

Theorem 44 *If $f = (f_0, f_1) \in \mathcal{X}(ZH_n)$ then*

a. $f_0 \in \mathcal{X}(ZH_{n-1})$;
b. $ZH_{n-1}(f_0 \oplus f_1) = f_1$.

Proof: If $f = (f_0, f_1)$ then for the vector $\tilde{a}$ of values of f we have $\tilde{a} = (\tilde{a_0}, \tilde{a_1})$, where $\tilde{a_0}$ and $\tilde{a_1}$ are the vectors of values of f_0 and f_1, respectively. Using Theorem 23 and $M_n \tilde{a}^t = \tilde{a} = (\tilde{a_0}, \tilde{a_1})$ we will obtain

$$\begin{aligned} M_n \tilde{a}^t &= M_n (\tilde{a_0}, \tilde{a_1})^t = \\ &= \begin{pmatrix} M_{n-1} & O_{n-1} \\ M_{n-1} & M_{n-1} \end{pmatrix} (\tilde{a_0}, \tilde{a_1})^t = \\ &= (M_{n-1}\tilde{a_0}^t \oplus O_{n-1}\tilde{a_1}^t, M_{n-1}\tilde{a_0}^t \oplus M_{n-1}\tilde{a_1}^t) = \\ &= (M_{n-1}\tilde{a_0}^t, M_{n-1}(\tilde{a_0} \oplus \tilde{a_1})^t) = \\ &= (\tilde{a_0}, \tilde{a_1}) \end{aligned}$$

i.e.

a. $M_{n-1}\tilde{a_0}^t = \tilde{a_0}$ and $f_0 \in \mathcal{X}(ZH_{n-1})$.
b. $M_{n-1}(\tilde{a_0} \oplus \tilde{a_1})^t = \tilde{a_1}$ and $ZH_{n-1}(f_0 \oplus f_1) = f_1$. $\diamondsuit$

As a side effect of the proof we obtained that if $f = (f_0, f_1) \in \mathcal{X}(ZH_n)$ then $f_1 = M_{n-1}(f_0 \oplus f_1)^t$ or $f_0 = (M_{n-1} \oplus I_{n-1}) f_1^t$. As we know from Theorem 32. there are exactly $2^{2^{n-2}}$ solutions of the equation mentioned above, when f_0 is given and f_1 is unknown.

Theorem 45 *If $f = (f_0, f_1) \in \mathcal{X}(ZH_n)$ and $g = (g_0, g_1) \in \mathcal{X}(ZH_n)$, $f \neq g$ then $f_1 \neq g_1$.*

Proof: Suppose the opposite, i.e $f_1 = g_1$. Then $f \oplus g = h \in \mathcal{X}(ZH_n)$ and $f \oplus g = (f_0, f_1) \oplus (g_0, g_1) = (h_0, \tilde{0})$. Applying Theorem 34.b we will obtain $ZH_{n-1}(h_0 \oplus \tilde{0}) = ZH_{n-1}(h_0) = \tilde{0}$. But $h_0 \in \mathcal{X}(ZH_{n-1})$ because $h \in \mathcal{X}(ZH_n)$ and so $h_0 = \tilde{0}$ and finally $f_0 = g_0$, which contradicts $f \neq g$. $\diamondsuit$.

Let now describe the "picture" of $\mathcal{X}(ZH_n)$ that is shown by the Previous two theorems. Each function $f = (f_0, f_1) \in \mathcal{X}(ZH_n)$ is composed of some $f_0 \in \mathcal{X}(ZH_{n-1})$ and unique function of $\mathcal{F}_2^{n-1}$. Each function $f_0 \in \mathcal{X}(ZH_{n-1})$ generates $2^{2^{n-2}}$ different functions of $\mathcal{X}(ZH_n)$. Then we could define two natural morphisms: the isomorphism $\zeta : \mathcal{X}(ZH_n) \longrightarrow \mathcal{F}_2^{n-1}$ such that if $f = (f_0, f_1)$ then $\zeta(f) = f_1$ and the homomorphism $\xi : \mathcal{X}(ZH_n) \longrightarrow \mathcal{X}(ZH_{n-1})$ such that $\xi(f) = f_0$. The final "line" of the picture is given by the following

Theorem 46 *$f \in \ker(\xi)$ iff $f_1 \in \mathcal{X}(ZH_{n-1})$.*

Proof: Let $f = (f_0, f_1) \in \ker(\xi)$, i.e. $f_0 = \tilde{0}$. Applying Theorem 34.b. we will have $f_1 = ZH_{n-1}(f_0 \oplus f_1) = ZH_{n-1}(\tilde{0} \oplus f_1) = ZH_{n-1}(f_1)$ and $f_1 \in \mathcal{X}(ZH_{n-1})$. Let now $f_1 \in \mathcal{X}(ZH_{n-1})$. Then from Theorem 3.4.b $f_1 = ZH_{n-1}^{-1} = f_0 + f_1$. So $f_0 = \tilde{0}$. $\diamondsuit$

References

1. Zhegualkin Į. I.: *Matematicheskiy Sbornik* (in Russian), 34:9-28, (1927)
2. Manev K., Bakoev V.: Algorithms for Performing the Zhegualkin Transformation, *Proceedings 23rd Spring Conference of the UBM*, Pleven, (1998), 229-233