Zhegalkin polynomials (May. 05, 2020.)

(A) The equivalence of Boolean rings and Boolean algebras

The theorems below show us that Boolean rings and Boolean algebras can be trasformed each into other.

Theorem 1. *Let* $(B, \vee, \wedge, -, \mathbf{0}, \mathbf{1})$ *be a Boolean algebra, and let us define the operations*

$a + b := (a \wedge \overline{b}) \vee (\overline{a} \wedge b)$ *and*
$a \cdot b := a \wedge b$

for all $a, b \in B$*. Then* $(B, +, \cdot)$ *is a Boolean ring.*

Proof. $+$ and $\cdot$ are binary interior operations by their definitions. Clearly, they are commutative also. "$\cdot$" is assoiative, since $a \wedge b$ is associative. It is not hard to check that

$(a + b) + c = a + (b + c)$, for any $a, b, c \in B$,

hence $+$ is also associative.
We have $a + 0 = (a \wedge \mathbf{1}) \vee (\overline{a} \wedge 0) = a \vee 0 = a$, and

$a + a = (a \wedge \overline{a}) \vee (\overline{a} \wedge a) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$.

The latter equality means that for any element $a \in B$, its additive inverse $-a$ there exists and $-a = a$.
It can be also easily checked that $a \cdot (b + c) = a \cdot b + a \cdot c$, and because $\cdot$ is commutative it follows also:

$(b + c) \cdot a = b \cdot a + c \cdot a$.

Therefore, $(B, +, \cdot)$ satisfies the axioms of a commutative ring. We are going to prove that $(B, +, \cdot)$ is Boolean ring. Indeed, we have $a \cdot \mathbf{1} = a \wedge \mathbf{1} = a$, for all $a \in B$, i.e. $\mathbf{1}$ is the unit of $\cdot$. Moreover,

$a^2 = a \cdot a = a \wedge a = a$,

and all these together mean that $(B, +, \cdot)$ is a Boolean ring. □

Theorem 2. *Let* $(B, +, \cdot)$ *be a Boolean ring and define:*

$a \vee b := a + b + a \cdot b$;
$a \wedge b := a \cdot b$;
$\overline{a} = 1 + a$

for all $a, b \in B$*. Then* $(B, \vee, \wedge, -, 0, 1)$ *be a Boolean algebra, where* 0 *denotes the neutral element of* $+$ *and* 1 *stands for the neutral element of* $\cdot$*.*

Proof. We check the distributive lattice axioms for the operations $\vee$ and $\wedge$ and then the equalities: $a \vee \mathbf{0} = a$,

$a \wedge 1 = a$; $a \wedge 0 = 0$, $a \vee 1 = 1$.
$a \vee \overline{a} = 1$, $a \wedge \overline{a} = 0$, $\overline{\overline{a}} = a$.

(This is a routine to check: for instance $a \wedge \overline{a} = a \cdot (1 + a) = a + a^2 = a + a = 0$ and $\overline{\overline{a}} = 1 + (1 + a) = (1 + 1) + a = 0 + a = a$. in any Boolean ring.) □

Let us observe that the transformations given in the above two theorems are, in fact, inverses each of other.

Theorem 3.(i) *Let* $(B, \vee, \wedge, -, \mathbf{0}, \mathbf{1})$ *be a Boolean algebra, and* $(B, +, \cdot)$ *the a Boolean ring corresponding to it by Theorem 1. Then the Boolean algebra constructed from* $(B, +, \cdot)$ *by using the transformations given in Theorem 2, is the same as the starting algebra* $(B, \vee, \wedge, -, \mathbf{0}, \mathbf{1})$.
(ii) *Let* $(B, +, \cdot)$ *be a Boolean ring and* $(B, \vee, \wedge, -, 0, 1)$ *the Boolean algebra corresponding to it by Theorem 2. Then the Boolean ring constructed from* $(B, \vee, \wedge, -, 0, 1)$ *by using the transformations given in Theorem 1, is the same as the starting ring* $(B, +, \cdot)$.

Proof. We prove only (ii), the proof of (i) being completely analogous.
Clearly, the underlying set of the first and the last ring is the same set B. We wiil show that the operatons in the last ring are the same as in the first. Denote the operations in the last ring by $\oplus$ and $\odot$. Then for any $a, b \in B$ we have:

$a \odot b = a \wedge b = a \cdot b$,

hence $\cdot$ and $\odot$ are the same. We obtain also:

$a \oplus b = (a \wedge \overline{b}) \vee (\overline{a} \wedge b) = a \cdot \overline{b} \vee \overline{a} \cdot b = a \cdot \overline{b} + \overline{a} \cdot b + a \cdot \overline{b} \cdot \overline{a} \cdot b =$

$a(1+b)+(1+a)\cdot b+a(1+b)\cdot(1+a)\cdot b = a+a\cdot b+b+a\cdot b+a\cdot b(1+a+b+a\cdot b) =$

$= a+b+a\cdot b+a^2\cdot b+a\cdot b^2+a^2\cdot b^2 = a+b+a\cdot b+a\cdot b+a\cdot b+a\cdot b = a+b.$

Thus $+$ and $\oplus$ are also the same, and hence the two rings are the same. □

Examples for the above equivalence.

1) Let us consider the Boolean algebra $(\wp(X), \cup, \cap, -, \emptyset, A)$ considered in the last lecture. Then for any $A, B \in \wp(X)$ we have.

$A + B = (A \cap \overline{B}) \cup (\overline{A} \cap B) = (A \setminus B) \cup (B \cap \overline{A}) = (A \setminus B) \cup (B \setminus A) = A \triangle B$,

and

$A \cdot B = A \cap B$.

Hence, in view of Theorem 1, $(B, \triangle, \cap)$ is a Boolean ring.

2) Let $(T^{(n)}, \vee, \wedge, \neg, \mathbf{0}, \mathbf{1})$ be the Boolean algebra of the truth functions with at most n-variables. Then gor any $f.g \in T^{(n)}$ we have:

$f + g := (f \wedge \neg g) \wedge (\neg f \wedge g) = f \oplus g$ (where $\oplus$ stands for the antivalence opreration.), and

$f \cdot g = f \wedge g$.

Therefore, according to Theorem 1, $(T^{(n)}, \oplus, \wedge)$ is a Boolean ring.

3) Now let $(\mathbb{Z}_2, \oplus, \cdot)$ the Boolean ring with two elements, $\mathbb{Z}_2 = \{0, 1\}$
Then by definying the operations:

$a \vee b := a \oplus b \oplus a \cdot b$,

$a \wedge b := a \cdot b$,

$\overline{a} = 1 \oplus a$.

we obtain the Boolean algebra with two elements $(\{0, 1\}, \vee, \wedge, -, 0, 1)$.

Application. By applying Theorem 1 and 2 to the Boolean algebra of the truth functions, for any $f, g \in T^{(n)}$ we obtain the following identities:

$f \vee g = f \oplus g \oplus (f \wedge g)$ and $\neg f = 1 \oplus f$

Corollary 1. Any truth function can be expressed using only the operations $\oplus$, $\wedge$ and the constant 1.

Proof. The assertion follows from Theorem 2, where $\vee$,$\wedge$ and $\neg$ are exprseed only by the mean of these operations. □

(B) Zhegalkin polynomials

Let $(A, +\cdot)$ be a ring. A unary polynomial over A is an expression

$p(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + ... + a_{n-1} \cdot x + a_n$,

built with the ring operations, where $a_0, a_1, ..., a_n \in A$. Their set will be denoted by $A[x]$.

For instance, if $(\mathbb{Z}, +\cdot)$ is the ring of the intigers, then $\mathbb{Z}[x]$ means the set of unary polynomials with integer coefficients. We present without proof the following

Proposition 1. *If $(A, +\cdot)$ is a ring then $(A[x], +, \cdot)$ is also a ring.*

We can consider also polynomials with several variables. For instance, $\mathbb{R}[x, y]$ means the set (in fact: the ring) of polynomials with real coefficients and at most two variables. Example: $\frac{1}{3}xy^2 - 5xy + \sqrt{2} \in \mathbb{R}[x, y]$. Similarly we can define polynomials with n-variables over the ring $(A, +\cdot)$; their set will be denoted by $A[x_1, x_2, ..., x_n]$ and it can be proved that $(A[x_1, x_2, ..., x_n], +, \cdot)$ *is also a ring*- where $+$ denotes the addition and $\cdot$ denotes the multiplication of these polynomial with coefficients in A.

Let us consider now the Boolean ring $(\mathbb{Z}_2, \oplus, \cdot)$ with two elements (where $\mathbb{Z}_2 = \{0, 1\}$). Now $a_0, a_1, ..., a_n \in \mathbb{Z}_2$ means, that these corfficients can be 0 or 1. We learned that $x^k = x$, for all $k \geq 1$ in $(\mathbb{Z}_2, \oplus, \cdot)$, i.e. any unary polynomial has at most degree one. 0 and 1 will be considered constant, i.e. nullary polynomials, their degree being 0. it is easy to see that the only unary ppolynomials with degree 1 are only x and $x + 1$. The polynomials with n-variables over $(\mathbb{Z}_2, \oplus, \cdot)$ will be simply some sums of the products of type $x_{i_1} \cdot x_{i_2} \cdot ... \cdot x_{i_k}$, where $i_1, i_2, ...i_k \in \{1, ..., n\}$ and $k \leq n$. For instance, $p(x_1, x_2, x_3) = x_1 \cdot x_2 \cdot x_3 \oplus x_2 \cdot x_3 \oplus 1$ is a ternary polynomial over $(\mathbb{Z}_2, \oplus, \cdot)$. The polynomials $p(x_1, x_2, ..., x_n) \in \mathbb{Z}_2[x_1, x_2, ..., x_n]$ with (at most) n variables over $(\mathbb{Z}_2, \oplus, \cdot)$ will be called as far as follows *Zhegalkin polynomials.*

For instance, for $n = 1$ we get that 0, 1, x, $x \oplus 1$ are the only Zhegalkin polynomials with at most one variable. Other examples are $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3 \oplus 1$, $g(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 \oplus x_1x_3x_4 \oplus x_1x_2 \oplus x_2x_3 \oplus x_4$. observe, that both the coefficients both the exponents in a Zhegalkin polynomial can be only 0 or 1, and the multiplication $\cdot$ several times is not marked (it might be noted or it might be not marked, as we like), like in the case of algebrical expressions.

Remark 1. An expresion built with the operations of the Boolean ring $(\mathbb{Z}_2, \oplus, \cdot)$ is considered to be a Zhegalkin polynomial, only in the case if there are no unefectuated operation, i..e. in the case when it can not be simplified. For instance $x_1x_2 \oplus x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_2x_3 \oplus x_1x_2 = x_1x_2 \oplus x_3$, therefore the right side is not a Zhegalkin polynomial (but the left side it is), and similarly $x_1^2x_2 \oplus x_1x_2x_3^2$ is not a Zhegalkin polynomial, because:
$x_1^2x_2 \oplus x_1x_2x_3^2 = x_1x_2 \oplus x_1x_2x_3$.

Theorem 4. *Any truth function can be expressed in the form of a Zhegalkin polynomial.*

Proof. Let $f(x_1, x_2, ..., x_n)$ be a truth function with n variables $(x_1, x_2, ..., x_n \in \{0, 1\})$. Then, as we learned, f can be written in the standard normal form:

$f(x_1, x_2, ..., x_n) = \left|\bigvee\{x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n} \mid f((i_1, i_2, ..., i_n) = 1\}\right|$.

First, observe that two different elementary conjunctions $x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n}$ and $x_1^{i_1} \cdot x_2^{j_2} \cdot ...x_n^{j_n}$ (where $(i_1, i_2, ..., i_n) \neq (j_1, i_{j2}, ..., j_n)$ exclude each other. Indeed, we know that $\mid x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n} \mid = 1 \Leftrightarrow (\mid x_1 \mid, \mid x_2 \mid, ..., \mid x_n \mid) = (i_1, i_2, ..., i_n)$, and
$\mid x_1^{i_1} \cdot x_2^{j_2} \cdot ...x_n^{j_n} \mid = 1 \Leftrightarrow (\mid x_1 \mid, \mid x_2 \mid, ..., \mid x_n \mid) = (j_1, i_{j2}, ..., j_n)$.
Hence $\mid x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n} \mid = 1$ implies $\mid x_1^{i_1} \cdot x_2^{j_2} \cdot ...x_n^{j_n} \mid = 0$, and conversely,

$\mid x_1^{i_1} \cdot x_2^{j_2} \cdot ...x_n^{j_n} \mid = 1$ implies $\mid x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n} \mid = 0$.

In such a case the operation $\vee$ can be substituted with the exclusive or, i.e. $\oplus$. Hence we can write

$f(x_1, x_2, ..., x_n) = \left|\bigoplus\{x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n} \mid f((i_1, i_2, ..., i_n) = 1\}\right|$.

Now let us examine an arbitrary term $x_1^{i_1} \cdot x_2^{i_2} \cdot ...x_n^{i_n}$. Without lost of generality we can assume that

$i_1 = 1, ...i_k = 1$ and $i_{k+1} = 0, ..., i_n = 0$. Then $x_1^{i_1} = x_1, ..., x_k^{i_k} = x_k$ and $x_{k+1}^{i_{k+1}} = x_{k+1}^0 = \neg x_{k+1}, ..., x_n^{i_n} = x_n^0 = \neg x_n$.
Since in $(\mathbb{Z}_2, \oplus, \cdot)$ we have $\neg x_{k+1} = 1 \oplus x_{k+1}, ..., \neg x_n = 1 \oplus x_n$, we obtain:

$f(x_1, x_2, ..., x_n) = |\bigoplus\{x_1 \cdot ... \cdot x_k \cdot (1 \oplus x_{k+1}) \cdot ... \cdot (1 \oplus x_n) \mid f((i_1, i_2, ..., i_n) = 1\}| =$
$=| \sum x_1 \cdot ... \cdot x_k \oplus x_1 \cdot ... \cdot x_k \cdot x_{k+1} \oplus ... \oplus x_1 \cdot x_2 \cdot ... \cdot x_n \mid$ -however this is a Zhegalkin polynomial. □

Example 2. We will illustrate the algorithm presented in the proof of the above theorem by the next example:
Let $f(x_1, x_2, x_3) = \left|x_1^1x_2^1x_3^0 \vee x_1^0x_2^1x_3^1\right|$ be the standard normal form of a fixed truth function $f(x_1, x_2, x_3)$. We will transform it into a Zhegalkin polinomial. Indeed, we can write:

$f(x_1, x_2, x_3) = |x_1x_2\neg x_3 \oplus \neg x_1x_2x_3| =| x_1x_2(1 \oplus x_3) \oplus (1 \oplus x_1)x_2x_3 \mid =$
$=| x_1x_2 \oplus x_1x_2x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \mid =| x_1x_2 \oplus x_2x_3 \mid$.

Thus $p(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3$ is the corresponding Zhegalkin polynomial.
We finish our exposition with the following:

Theorem 5. *The Zhegalkin polynomials with at most n-variables also form a Boolean ring, in other words, $(\mathbb{Z}_2[x_1, x_2, ..., x_n], \oplus, \cdot)$ is a Boolean ring.*