МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2004
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2004
Proceedings of the Thirty Third Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 1–4, 2004

A LOCATING SCHEME OF THE BOOLEAN FUNCTIONS FROM THE POST CLASSES

Valentin Bakoev

A locating scheme of the Boolean functions from the Post classes is proposed here. It is deduced by solving a proper sequence of known problems and combining their solutions, represented by Euler-Venn diagrams.

1. Introduction. The theory of Boolean functions takes an important place in Discrete mathematics teaching. Several topics are devoted to studying of Post classes and completeness, so they are included in each of the textbooks [11,7,12,5,8,10,4]. To master these topics students must solve many problems like these, given in [6] and in some of the textbooks. A big part of them concerns the enumeration of all functions in the sections among the Post classes (the cardinalities of the classes are derived in most of the textbooks). Our experience shows that solving similar problems without proper illustrations of their solutions often yields to confusions among the students.

Here we propose a scheme (an Euler-Venn diagram), which represents the mutual location of Post classes towards the set of all Boolean functions. We build this scheme consecutively by solving a sequence of problems and combining their solutions. We investigate functions of n variables, but we represent the results in general case, because the corresponding schemes resemble each other for $n > 1$. "Resemble" means that the scheme represents the cardinalities only for the classes T_0 and T_1, for each n. For the rest classes this is possible only for a given (not large) n, as we shall see further. Their actual cardinalities cannot be represented on the scheme in the general case, because the ratio between each of them and the number of all Boolean functions exponentially tends to zero when n grows to infinity.

2. Basic notions and assertions. We recall some necessary terms and assertions in accordance with the most popular Bulgarian textbook [11].

Further, n will always be an integer greater than zero. Let $J_2^n = \{0,1\}^n$ be the n-dimensional Boolean cube, i. e. the set of all n-dimensional binary vectors. We assume that the vectors of J_2^n are in lexicographic order. A *Boolean function* (or simply a *function*) of n variables $x_1, x_2, \ldots, x_n$ is a mapping $f : J_2^n \to J_2$. For a given n, the set of all functions of n variables is denoted by $\mathcal{F}^n$, i. e. $\mathcal{F}^n = \{f | f : J_2^n \to J_2\}$, and $\mathcal{F} = \bigcup_{n=1}^{\infty} \mathcal{F}^n$ denotes the set of all Boolean functions. When $f(\alpha) = 0$ (resp. $= 1$) for each vector $\alpha \in J_2^n$, then f is called a *constant* 0 (resp. 1) and it is denoted by $\tilde{0}$ (resp. $\tilde{1}$). If for some $i, 1 \leq i \leq n$, $f(\alpha) = x_i \ \forall \alpha \in J_2^n$ (the value of f always coincides with the value of its i-th variable), we denote $f(x_1, \ldots, x_n) = x_i$ and f is called an *i-th identity function.*

Let $f(x_1, x_2, \dots, x_n) \in \mathcal{F}^n$ and $g(y_1, y_2, \dots, y_m) \in \mathcal{F}^m$. The function

$$h(x_1, \dots, x_{i-1}, y_1, \dots, y_m, x_{i+1}, \dots, x_n) = f(x_1, \dots, x_{i-1}, g(y_1, \dots, y_m), x_{i+1}, \dots, x_n)$$

belongs to $\mathcal{F}^{n+m-1}$ and it is called a *superposition of g in f in the place of the variable x_i*. For a given set $F = \{f_1, \dots, f_k\}$ of Boolean functions, $[F]$ denotes the set of all possible superpositions of the functions from F. The set F is said to be a *closed set* (or simply a *class*) if $[F] = F$, i. e. all superpositions of the functions from F remain in F. The next theorem states a sufficient condition for a given set of Boolean functions to be a class.

Theorem 1. *Let $F \in \mathcal{F}$ and:* 1) $f(x_1, \dots, x_n) = x_i \in F$, $i = 1, \dots, n$; 2) *for all $f, g_1, \dots, g_n \in F$ it follows that $h = f(g_1, \dots, g_n) \in F$. Then F is a class.*

The set F is said to be *complete* if $[F] = \mathcal{F}$, i. e. if each Boolean function can be represented as a superposition of functions in F.

3. The Post classes and building up the scheme. The following five classes are called *Post classes* in honour of Emil Post. Proofs that they are classes and calculations of their cardinalities are given in [11, 7, 12, 8].

3.1. The classes T_0 and T_1. We say that the function $f \in \mathcal{F}$ *preserves the zero* (resp. *preserves the unit*), if $f(0, \dots, 0) = 0$ (resp. $f(1, \dots, 1) = 1$). Let $T_0 = \{f | f \in \mathcal{F}, f(0, \dots, 0) = 0\}$ (resp. $T_1 = \{f | f \in \mathcal{F}, f(1, \dots, 1) = 1\}$) denotes the set of all functions preserving the zero (resp. the unit). Let also T_0^n (resp. T_1^n) denotes the subset of T_0 (resp. of T_1), which contains functions of n variables only. It is known that $|T_0^n| = |T_1^n| = 2^{2^n-1}$.

All following problems, which we state and solve, are problems from [6], Chapter II. So we refer to their numbers only. Problem 4.5 puts many questions, among them $|T_0^n \cap T_1^n| =?$ and $|T_0^n \cup T_1^n| =?$

To answer the first of them we note that $f \in T_0^n \cap T_1^n$ iff the vector of its values has the form $f(x_1, \dots, x_n) = (0, a_1, \dots, a_{2^n-2}, 1)$, $a_i \in \{0, 1\}$, $i = 1, \dots, 2^n - 2$. So $|T_0^n \cap T_1^n| = 2^{2^n-2}$, i. e. a quarter of $|\mathcal{F}^n|$. By analogy we obtain $|\mathcal{F}^n \backslash (T_0^n \cup T_1^n)| = |(T_0^n \backslash T_1^n)| = |(T_1^n \backslash T_0^n)| = 2^{2^n-2}$. Hence $|(T_0^n \cup T_1^n)| = 3.2^{2^n-2}$. Since $\mathcal{F}^n$ splits to quarters for each n, $\mathcal{F}$ splits to quarters too, as it is shown on Figure 1.

3.2. Self-dual functions and the class S. If $\alpha = (a_1, \dots, a_n) \in J_2^n$, then the vector $\bar{\alpha} = (\bar{a}_1, \dots, \bar{a}_n)$ is called an *inverse vector* of α. Let $f \in \mathcal{F}^n$. The function $f^*(x_1, x_2, \dots, x_n) = \bar{f}(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$ is called the *dual function* of f. The inverse vectors in J_2^n are symmetrical to each other with respect to the imaginary axis, which divides the vectors beginning with 0 and the vectors beginning with 1 in J_2^n. So, if $f(x_1, \dots, x_n) = (a_1, a_2, \dots, a_{2^n-1}, a_{2^n})$, then $f^*(x_1, \dots, x_n) = (\bar{a}_{2^n}, \bar{a}_{2^n-1}, \dots, \bar{a}_2, \bar{a}_1)$ (see Problem 2.2). When f and f^* coincide (i. e. $f = f^*$), the function f is called *self-dual*. The set of all self-dual functions of n variables is denoted by S^n, and $S = \bigcup_{n=1}^{\infty} S^n$ is the set of all self-dual functions. So f is self-dual iff f takes inverse values on each pair of inverse vectors, i. e. each $f \in S^n$ has the form $f(x_1, \dots, x_n) = (a_1, \dots, a_{2^{n-1}}, \bar{a}_{2^{n-1}}, \dots, \bar{a}_1)$. Therefore S^n contains exactly $2^{2^{n-1}}$ functions (see problems 2.11 and Chapter I, 2.1). Other questions, which the problem 4.5 sets are: $|T_1^n \cap S^n| =?$, $|T_0^n \backslash S^n| =?$, $|S^n \cap (T_0^n \cup T_1^n)| =?$, $|S^n \cap (T_0^n \backslash T_1^n)| =?$, $|S^n \backslash (T_0^n \cup T_1^n)| =?$ and $|(S^n \backslash T_0^n) \cap T_1^n)| =?$

Let $f \in T_0^n \cap S^n$, i. e. $f(0, \dots, 0) = 0$ and $f = f^*$. Then $0 = f(0, \dots, 0) = f^*(0, \dots, 0) = \bar{f}(\bar{0}, \dots, \bar{0}) = \bar{f}(1, \dots, 1)$. Therefore $f(1, \dots, 1) = 1$ and $f \in T_1^n$. So $f \in T_0^n \cap S^n$ implies $f \in T_1^n$, or (by analogy) $f \in T_1^n \cap S^n \Rightarrow f \in T_0^n$. And vice versa: $f \in S^n \backslash T_0^n$ implies $f \notin T_1^n$, or $f \in S^n \backslash T_1^n \Rightarrow f \notin T_0^n$. We partition the class S^n into two subclasses: $S^n = S^n_+ \cup S^n_-$, $S^n_+ = \{f | f \in T^n_0 \cap T^n_1 \cap S^n\}$ and $S^n_- = \{f | f \in S^n \backslash (T^n_0 \cup T^n_1)\}$. Hence $|S^n_+| = |S^n_-| = |S^n|/2 = 2^{2^{n-1}-1}$ and also $|S^n_+| < |T^n_0 \cap T^n_1|$ for $n > 1$. The location of the set(s) $S^n = S^n_+ \cup S^n_-$ is illustrated on Figure 2.

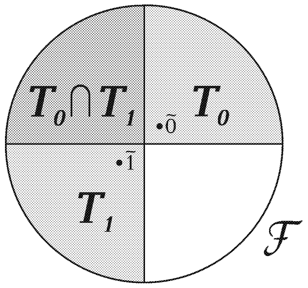


Fig. 1. T_0 and T_1 into $\mathcal{F}$

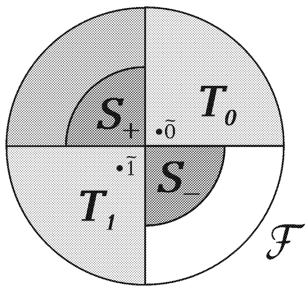


Fig. 2. T_0, T_1 and S into $\mathcal{F}$

3.3. Monotone functions and the class *M*. Let $\alpha, \beta \in J^n_2$ and $\alpha = (a_1, \ldots, a_n)$, $\beta = (b_1, \ldots, b_n)$. The relation "$\preceq$" is defined over $J^n_2 \times J^n_2$ as follows: $\alpha \preceq \beta$ iff $a_i \leq b_i$ for $i = 1, 2, \ldots, n$. If $\alpha, \beta \in J^n_2$ and $\alpha \preceq \beta$ always implies $f(\alpha) \leq f(\beta)$, then the function f is called *monotone*. Let M^n be the set of all monotone functions of n variables, and $M = \bigcup_{n=1}^{\infty} M^n$ be the set of all monotone functions. The so called *Dedekind's problem* [3] is a problem of enumerating the set M^n. It is still open, there is no exact formula for $|M^n|$ in the general case, and the values of $|M^n|$ are known only for $1 \leq n \leq 8$. Precise asymptotic estimations of $|M^n|$ are given in [9].

Problem 5.22 sets the questions $|M^n \backslash (T^n_0 \cap T^n_1)| =?$ and $|M^n \backslash (T^n_0 \cup T^n_1)| =?$ Let $f \in M^n \backslash T^n_0$. So $f(0, \ldots, 0) = 1$. Since the vector $(0, \ldots, 0) \preceq \alpha$ $\forall \alpha \in J^n_2$ and f is monotone, it follows that $f(\alpha) = 1$ $\forall \alpha \in J^n_2$, i. e. $f \equiv \tilde{1}$. By analogy, $f \in M^n \backslash T^n_1$ implies $f \equiv \tilde{0}$. So, each $f \in M^n \backslash \{\tilde{0}, \tilde{1}\}$ satisfies $f(0, \ldots, 0) = 0$ and $f(1, \ldots, 1) = 1$, and therefore $(M^n \backslash \{\tilde{0}, \tilde{1}\}) \subset (T^n_0 \cap T^n_1)$, $M^n \subset (T^n_0 \cup T^n_1)$.

The intersection between the classes S^n and M^n (see problems 5.23 and 5.26) is well studied ([1,2] etc.). For our goals it is enough to note:

1) $S^n \cap M^n = (S^n_+ \cup S^n_-) \cap M^n = (S^n_+ \cap M^n) \cup (S^n_- \cap M^n) = S^n_+ \cap M^n$.

2) If $f \in M^n$ then $f^* \in M^n$. This assertion follows directly from Problems 5.4 and 2.4. It also can be proved in this way: $f \in M^n$ means that $\forall \alpha, \beta \in J^n_2$, $\alpha \preceq \beta$ $\Rightarrow f(\alpha) \leq f(\beta)$. If $\alpha \preceq \beta$ then $\bar{\beta} \preceq \bar{\alpha}$ and so $f(\bar{\beta}) \leq f(\bar{\alpha})$. Therefore $\bar{f}(\bar{\beta}) \geq \bar{f}(\bar{\alpha})$, also $f^*(\alpha) = \bar{f}(\bar{\alpha}) \leq \bar{f}(\bar{\beta}) = f^*(\beta)$ and hence $f^* \in M^n$.

So some of the functions $f \in M^n$ satisfy $f = f^*$ and they are in $M^n \cap S^n_+$, the rest of them (such that $f \neq f^*$) are in $M^n \backslash S^n_+$. The location of the class M^n (towards the considered classes) is outlined by dash-line on the Figure 3. So we mark the unknown cardinality of M^n in the general case.

3.4. Linear functions and the class *L*. The completeness of the set of functions $\{xy, x \oplus y, \tilde{1}\}$ is proved in the textbooks and so each function $f \in \mathcal{F}^n$ can be expressed as a superposition over this set. After that f can be reduced to the form $f(x_1, \ldots, x_n)$ $= E_1 \oplus \cdots \oplus E_k$, where $E_i \neq E_j$ for $1 \leq i < j \leq k$ and each monomial is of the type $E_i = x_{i_1} \ldots x_{i_m}$, $x_{i_r} \neq x_{i_s}$, $1 \leq r < s \leq m$, or $E_i = \tilde{1}$. Such a formula is called a *Zhegalkin polynomial* of f. The Zhegalkin's theorem states that for each $f \in \mathcal{F}$ there

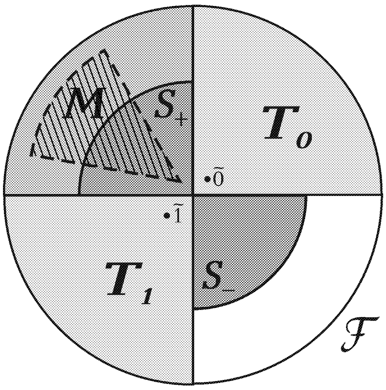
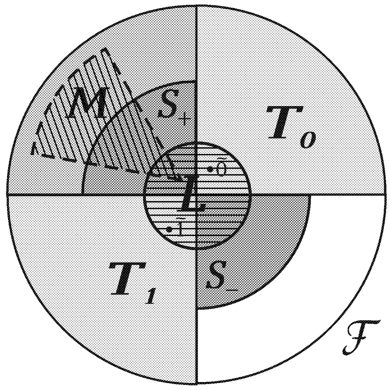


Fig. 3. T_0, T_1 and S into $\mathcal{F}$



All the classes into $\mathcal{F}$

exists a unique Zhegalkin polynomial. A function $f \in \mathcal{F}^n$, which Zhegalkin polynomial consists of linear terms only

(1) $$f(x_1, \ldots, x_n) = a_0 \oplus x_{i_1} \oplus \cdots \oplus x_{i_k},\ a_0 \in \{0,1\},\ 0 \le k \le n,$$

is called a *linear function*. The set of all linear functions of n variables is denoted by L^n, and $L = \bigcup_{n=1}^{\infty} L^n$ is the set of all linear functions. Each function $f \in L^n$ has the general form $f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n$, $a_i \in \{0,1\},\ 0 \le i \le n$, and hence $|L^n| = 2^{n+1}$.

The last questions in Problem 4.5 are: $|T_0^n \cap L^n| =?$, $|T_1^n \cup L^n| =?$, $|L^n \backslash (T_0^n \cap T_1^n)| =?$, $|L^n \backslash (T_0^n \cup T_1^n)| =?$, $|L^n \cap S^n \cap T_1^n)| =?$, $|L^n \backslash (T_0^n \cup (T_1^n \cap S^n))| =?$ and $|(L^n \cup S^n) \backslash (T_0^n \cup T_1^n)| =?$

Firstly, we consider the location of the class L^n towards the classes T_0^n and T_1^n. Let $f \in L^n$ be of the form (1). There are two cases: (i) $a_0 = 0$ and (ii) $a_0 = 1$, which split L^n into two subclasses with equal cardinalities. In case (i) $f(0, \ldots, 0) = 0$ and therefore $f \in L^n \cap T_0^n$, $|L^n \cap T_0^n| = 2^n$. In the same case the number k of variables in f can be odd or even. When k is odd $f(1, \ldots, 1) = 0 \oplus \underbrace{1 \oplus \cdots \oplus 1}_{k} = \bigoplus_{i=1}^{k} 1 = 1$ and so $f \in L^n \cap T_0^n \cap T_1^n$. When k is even $f(1, \ldots, 1) = 0$ and so $f \in L^n \cap T_0^n \backslash T_1^n$. About the ways of choosing k variables we recall that

$$\sum_{k=0}^{[n/2]} \binom{n}{2k} = \sum_{k=1}^{[n/2]} \binom{n}{2k-1} = \frac{1}{2} \sum_{k=0}^{n} \binom{n}{k} = 2^{n-1}.$$

Hence $|L^n \cap T_0^n \cap T_1^n| = |L^n \cap T_0^n \backslash T_1^n| = 2^{n-1}$. In case (ii) $f \in L^n \backslash T_0^n$. By analogy we obtain: if k is odd, then $f \in L^n \backslash (T_0^n \cup T_1^n)$, and if k is even, then $f \in L^n \cap T_1^n \backslash T_0^n$. And also $|L^n \backslash (T_0^n \cup T_1^n)| = |L^n \cap T_1^n \backslash T_0^n)| = 2^{n-1}$. Therefore L^n splits to quarters, which are subsets of $T_0^n \cap T_1^n$, $T_0^n \backslash T_1^n$, $T_1^n \backslash T_0^n$ and $\mathcal{F}^n \backslash (T_0^n \cup T_1^n)$ correspondently – see Figure 4.

Now we answer the questions, which include the class S^n (Problems 2.9, 3.6, 3.23, 3.24, 4.17 etc. also concern $L^n \cap S^n$). Let $f(x_1, \ldots, x_n) = a_0 \oplus x_{i_1} \oplus \ldots \oplus x_{i_k}$, $a_0 \in \{0,1\}$, $0 \le k \le n$. To express f^* we use the property $x \oplus 1 = \bar{x}$ and we obtain $f^*(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n) = \overline{(a_0 \oplus \bar{x}_{i_1} \oplus \cdots \oplus \bar{x}_{i_k})} = (a_0 \oplus (x_{i_1} \oplus 1) \oplus \cdots \oplus (x_{i_k} \oplus 1)) \oplus 1$

$= a_0 \oplus x_{i_1} \oplus \cdots \oplus x_{i_k} \oplus \bigoplus_{i=1}^{k+1} 1$, which means that $L^n \equiv (L^n)^*$. When the sum $\bigoplus_{i=1}^{k+1} 1 = 0$ then $f = f^*$, i. e. $f \in L^n \cap S^n$, and it holds for every odd k. Hence $|L^n \cap S^n| = |L^n|/2 = 2^n$. There are two subcases: if $a_0 = 0$ then $f \in T_0^n \cap T_1^n \cap L^n \cap S^n$ (or $f \in L^n \cap T_0^n \cap T_1^n$ implies $f \in S^n$), and if $a_0 = 1$ then $f \in (L^n \cap S^n)\backslash(T_0^n \cup T_1^n)$ (or $f \in L^n\backslash(T_0^n \cup T_1^n)$ implies $f \in S^n$). Analogously, the sum $\bigoplus_{i=1}^{k+1} 1 = 1$ for every even k and then $f \neq f^*$, $f \in L^n\backslash S^n$. Also $f \in (L^n \cap T_0^n)\backslash T_1^n$ implies $f \notin S^n$ and $f \in (L^n \cap T_1^n)\backslash T_0^n$ implies $f \notin S^n$. These conclusions can be seen on Figure 4.

Finally we consider $L^n \cap M^n$ in relation to Problems 5.22, 5.42 and 5.43. We take again $f \in L^n$, $f(x_1, \ldots, x_n) = a_0 \oplus x_{i_1} \oplus \cdots \oplus x_{i_k}$. When $k = 0$, we obtain $f(x_1, \ldots, x_n) = a_0$, i. e. $f \equiv \tilde{0}$ or $f \equiv \tilde{1}$, which are monotone. If $k > 0$ and $a_0 = 1$ then $f \notin T_0^n$, hence $f \notin M^n$ and so we consider only the functions in which $a_0 = 0$. When $k = 1$ we obtain the i-th identity function $f(x_1, \ldots, x_n) = x_i$ for $i = 1, \ldots, n$, i. e. n identity functions, which are in M^n (Theorem 1). When $k > 1$, without loss of generality, we accept that x_1 and x_2 are the first two of the variables of f. For the vectors $\alpha = (1, 0, 0, \ldots, 0)$ and $\beta = (1, 1, 0, \ldots, 0)$ we have $\alpha \preceq \beta$, but $f(\alpha) = 1 > 0 = f(\beta)$ and so $f \notin M^n$. Therefore $L^n \cap M^n = \{\tilde{0}, \tilde{1}\} \cup \{f | f(x_1, \ldots, x_n) = x_i, i = 1, \ldots, n\}$, or $n + 2$ function generally. The scheme on Figure 4 represents all obtained results about the mutual location of all Post classes.

4. Conclusions. For several years we have deduced the scheme in the exercises on the way, which was proposed here. The students understand and remember this scheme quickly and always use it. So, many of the problems, which they solve, become easier or even trivial. The scheme can be useful to everyone, whose work is related to Boolean functions and Post classes.

REFERENCES

[1] J. Bioch, T. Ibaraki, K. Makino. Minimum self-dual decompositions of positive dual-minor Boolean functions. *Discrete Applied Mathematics*, **97**, (1999), 307–326.

[2] M. Fredman, L. Khachiyan. On the complexity of dualization of monotone disjunctive normal forms. *J. of Algorithms*, **21**, (1996), 618–621.

[3] `http://mathpages.com/home/kmath030.htm`, Dedekind's Problem.

[4] I. Wegener. The Complexity of Boolean Functions. J. Wiley & Sons, and B. G. Teubner, Stuttgart, 1987.

[5] О. Е. Акимов. Дискретная математика. Логика, групы, графы. Лаборатория базовых знаний, Москва, 2001.

[6] Г. Гаврилов, А. Сапоженко. Сборник задач по дискретной математике. Наука, Москва, 1977.

[7] Й. Денев, Р. Павлов, Я. Деметрович. Дискретна математика. Наука и изкуство, София, 1984.

[8] Я. М. Ерусалимский. Дискретная математика: теория, задачи, приложения. Вузовская книга, Москва, 2001.

[9] А. Коршунов. О числе монотонных булевых функций. *Проблемы кибернетики*, **38**, (1981), 5–108.

[10] О. Кузнецов, Г. Адельсон-Велский. Дискретная математика для инженера. Енергия, Москва, 1980.

[11] К. Н. Манев. Увод в дискретната математика (III изд.) КЛМН, София, 2003.

[12] С. Яблонский. Введение в дискретную математику. Наука, Москва, 1979.

Valentin Penev Bakoev
Faculty of Pedagogy
University of Veliko Tarnovo
V. Tarnovo, Bulgaria

СХЕМА НА РАЗПОЛОЖЕНИЕТО НА БУЛЕВИТЕ ФУНКЦИИ ОТ КЛАСОВЕТЕ НА ПОСТ

Валентин П. Бакоев

В работата се предлага една схема на взаимното разположение на булевите функции от класовете на Пост. Тя се построява чрез решаване на подходяща последователност от известни задачи и комбиниране на решенията им, представени чрез техните диаграми на Ойлер-Вен.