Properties of Symmetric Boolean functions

L. HAVIAROVÁ AND E. TOMAN

Abstract

In the present paper we consider symmetric Boolean functions with special property. We study properties of the maximal intervals of these functions. Later we show characteristics of corresponding interval graphs and simplified interval graphs. Specifically we prove, that these two graphs are isomorphic for symmetric Boolean function. Then we obtain the vertex degree of these graphs. We discuss also disjunctive normal forms.

Mathematics Subject Classification 2000: 05C80 (Random graphs), 60C05 (Combinatorial probability), 68R10 (Graph theory), 06E30 (Boolean function)
Additional Key Words and Phrases: Symmetric Boolean function, interval graph, disjunctive normal form.

1 INTRODUCTION

A Boolean function can be represented by several types of graphs. Among them, the greatest attention has been devoted to the study of the graph $G(f)$ induced by the vertices of the n-cube, on which the Boolean function f takes the value 1. This geometric representation has been introduced by Jablonski in [1]. The concept of the interval graph and simplified interval graph of a Boolean function has been defined by Sapozhenko in [3].

In the present paper we study properties of symmetric Boolean functions. Boolean function is a symmetric Boolean function, if there exists a set $\{P_1,\dots,P_k\}$, where $1 \le k \le n$ and $P_i \in \{0,1,\dots,n\}$ while the function gains value 1 in the vertices which contain value 1 on P_i positions. We denote level of Boolean cube B^n as P_i and symmetric Boolean function with levels $P_1,\dots,P_k$ as $B^n_{P_1,\dots,P_k}$.

The complexity of symmetric Boolean function was studied by Fagin, Klawe, Pippenger and Stockmeyer [6] and Denenberg, Gurevich and Shelah [7]. Their results were improved by Wegener [5]. Symmetric Boolean functions, expecially their cryptografic properties were studied by Canteaut and Videau [8].

Some results regarding disjunctive normal forms have already been obtained for almost all Boolean functions and were presented by Jablonski and Lupanov in [2]. In addition they described an algorithm for finding minimal d.n.f. for symmetric Boolean

Supported by VEGA grant No 1/1005/12

10.1515/jamsi-2016-0001

functions $B^n_{P_i,\ldots,P_j}$, where $i = j$. The principle of the algorithm is the numbering of the literals and cyclic movement of the indices. In this paper we extend this approach and prove results also for case $i \neq j$. Jablonski and Lupanov furthermore present asymptotic estimate for cases $i = \frac{n}{3}$ a $i = \frac{n}{4}$. It can be interesting to compare with our results.

2 PRELIMINARIES AND NOTATION

We use the standard notation from Boolean function theory. An n-ary Boolean function is a function f: $\{0,1\}^n \to \{0,1\}$.

We use an algebraic representation of Boolean functions - disjunctive normal form. A d.n.f. with minimal number of literals in this class is called the minimal d.n.f. of f and the one with minimal length in this class is called the shortest d.n.f. of f.

We also use a geometric representation of Boolean functions. The Boolean n-cube is the graph B^n with 2^n vertices $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \{0,1\}$, in which those pairs of vertices that differ in exactly one coordinate are joined with an edge. For an n-ary Boolean function f let N_f denote the subset $\{\tilde{\alpha}; f(\tilde{\alpha}) = 1\}$ and N_f^- denote the subset $\{\tilde{\alpha}; f(\tilde{\alpha}) = 0\}$ of all vertices $\tilde{\alpha}$. Notice that there is a one-to-one correspondence between the sets N_f and Boolean functions f. The subgraph of the Boolean n-cube induced by the set N_f is called the graph of f and is denoted by $G(f)$.

The set of vertices $N_i \subseteq \{0,1\}^n$ corresponding to an elementary conjunction K_i of rank r is called the interval of rank r. Notice that to every elementary conjunction $K = x_{i_1}^{\alpha_{i_1}} \wedge \ldots \wedge x_{i_r}^{\alpha_{i_r}}$ there corresponds an interval of rank r consisting of all vertices $(\beta_1, \ldots, \beta_n)$ of B^n such that $\beta_{i_j} = \alpha_{i_j}$ for $j = 1, \ldots, r$ and values of other vertex coordinates are arbitrary. In the present paper, we often work with intervals corresponding to elementary conjunctions.

In the geometric model, every interval of rank r represents an $(n-r)$-dimensional subcube of B^n. Therefore we call the interval of rank r also the $(n-r)$-dimensional interval. An interval N is called the maximal interval of Boolean function f if $N \subseteq N_f$ and there is no interval $N' \subseteq N_f$ such that $N \subseteq N'$. A d.n.f. which consists of all elementary conjunctions corresponding to maximal intervals is called the abbreviated d.n.f. and it is denoted by $D_A(f)$.

For an arbitrary Boolean function f and each of its d.n.f.s $K_1 \vee \ldots \vee K_s$, we have

that

$$N_f = \bigcup_{j=1}^{s} N_j.$$

In other words, every d.n.f. of a Boolean function f corresponds to a covering of N_f by intervals $N_1, \ldots, N_s$ such that $N_j \subseteq N_f$. Conversely, every covering of N_f by intervals $N_1, \ldots, N_s$ contained in N_f corresponds to some d.n.f. of f. Using the geometric interpretation of d.n.f.s, we can express the irreducibility of d.n.f.. The d.n.f. D of a Boolean function f cannot be simplified if every interval N_j of the covering corresponding to D contains at least one vertex belonging to just this one interval of the covering. Such a d.n.f. is called an irredundant d.n.f..

Let r_j denote the order of the interval N_j. Then the number of literals in d.n.f. is $r = \sum_{j=1}^{s} r_j$ and the construction of a minimal d.n.f. in the geometric model can be formulated as a problem of constructing a covering of N_f by intervals $N_j \subseteq N_f$ with minimal r. On the other hand, the construction of a covering corresponding to the shortest d.n.f. requires to minimize the number of intervals in a covering of N_f.

The set of all conjuctions K_j from $K_1, \ldots, K_s$ corresponding to intervals for which

$$N_j \not\subseteq \bigcup_{\substack{i=1 \\ i \neq j}}^{s} N_i.$$

is called the core of d.n.f. $D = \bigvee_{j=1}^{s} K_j$ of a Boolean function f. It is denoted by $\gamma(D(f))$.

Now we can define the interval graph $\Gamma(f)$ as the graph associated with a Boolean function f as follows: its vertices correspond to maximal intervals of f and the vertices corresponding to intervals N_i and N_j are joined with an edge in $\Gamma(f)$ if $K_i \wedge K_j$ is nonempty.

Let us introduce the graph of Boolean function f which we get from $\Gamma(f)$ by omitting all vertices corresponding to maximal intervals such that they belong to $\gamma(D_A(f))$ or do not belong to any irreducible covering. Such a graph is called a symplified interval graph.

For more information about Boolean functions we suggest to see [11], as this paper is its extension.

3 PROPERTIES OF SYMMETRIC BOOLEAN FUNCTIONS

In this section we study properties of symmetric Boolean function $B^n_{P_i,\dots,P_{n-j}}$, $i+j<n$. We do not consider the trivial case $i+j=n$. We evaluate the number, dimension, radius and diameter of its maximal intervals. Then we discuss the characteristics of graphs Γ and Γ' corresponding to $B^n_{P_i,\dots,P_{n-j}}$. In the end we count the vertex degrees of interval and simplified interval graphs.

Let α be $(\underbrace{1,\dots,1}_{n})$ and β be $(\underbrace{0,\dots,0}_{n})$.

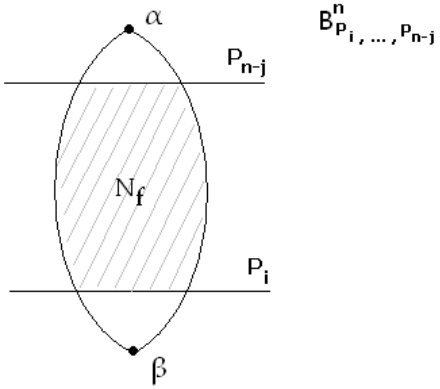


Fig. 1. Function $B^n_{P_i,\dots,P_{n-j}}$

THEOREM 3.1. *The dimension of maximal intervals of* $B^n_{P_i,\dots,P_{n-j}}$ *is*

$$n-(i+j).$$

PROOF. We know that j levels from vertex α and i levels from vertex β belong to N_f^-. Therefore each vertex belonging to N_f contains at least i coordinates with value 1 and j different coordinates with value 0. The rest of the coordinates are arbitrary. It generates the intervals of dimension $n-(i+j)$. Inequality $i+j<n$ implies existence of such intervals.

COROLLARY 3.2. *The dimension of maximal intervals of* $B^n_{P_i,\dots,P_{n-i}}$ *is*

$$n-2i.$$

The Theorem also implies, that all maximal intervals have the same dimension. Therefore all corresponding vertices in Interval graph have the same vertex degree.

The graph $\Gamma(B^n_{P_i,\ldots,P_{n-i}})$ is uniquely determined by the number of maximl interval and the vertex degree.

Let $\alpha' \in N_f$ and $\beta' \in N_f$ be the vertices of maximal interval containing at least i coordinates with value 1 and at least j coordinates with value 0, respectively. Distance between α' and β' is $n-(i+j)$. It is easy to see that α' is situated on level $n-j$ and β' on level i.

THEOREM 3.3. *The number of maximal intervals of $B^n_{P_i,\ldots,P_{n-j}}$ is*

$$\binom{n-i}{n-(i+j)}.\binom{n}{i}.$$

PROOF. The number of edges between α' and level $n-j+1$ is $n-j$. We already know that the dimension of all maximal intervals is $n-(i+j)$. Each maximal interval of dimension k starting in α' is uniquely determined by choosing k edges between α' and level $n-j+1$. Thus the number of different maximal intervals which contain vertex α' and have the dimension $n-(i+j)$ is $\binom{n-j}{n-(i+j)}$. As there are $\binom{n}{j}$ possibilities of choosing α' on level $n-j$, we get the result $\binom{n-j}{n-(i+j)}.\binom{n}{n-j}$.

Result for vertex β' on level i can be obtained analogicaly.

It holds that

$$\binom{n-i}{n-(i+j)}.\binom{n}{i} = \binom{n-j}{n-(i+j)}.\binom{n}{n-j},$$

which validate the Theorem.

COROLLARY 3.4. *The number of maximal intervals of $B^n_{P_i,\ldots,P_{n-i}}$ is*

$$\binom{n-i}{n-2i}.\binom{n}{i}.$$

THEOREM 3.5.

$$\binom{n-[pn]}{n-([pn]+[qn])}.\binom{n}{[pn]} \sim \frac{1}{2\pi n}.\frac{1}{p^{[pn]+1/2}}.\frac{1}{q^{[qn]+1/2}}.\frac{1}{(1-p-q)^{n-[pn]-[qn]}},$$

where $i = p.n$, $p < \frac{1}{2}$, $p,q \in Q$, $[x]$ stands for nearest integer to x.

PROOF. For the sake of simplicity let us assume pn, qn are already their rounded versions in the remainder of this paper.

$$\binom{n-pn}{n-(pn+qn)}.\binom{n}{pn} = \frac{n!}{pn!.qn!.(n-(pn+qn))!}$$

Using Stirling formula we get

$$\frac{n!}{pn!.qn!.(n-(pn+qn))!} \sim$$

$$\sim \frac{(\frac{n}{e})^n\sqrt{2.\pi.n}}{(\frac{qn}{e})^{qn}\sqrt{2\pi qn}(\frac{pn}{e})^{pn}\sqrt{2\pi pn}(\frac{n-(pn+qn)}{e})^{n-(pn+qn)}\sqrt{2\pi(n-(pn+qn))}} =$$

$$= \frac{\sqrt{2\pi n}}{\sqrt{2\pi(n-(pn+qn))}\sqrt{2\pi qn}\sqrt{2\pi pn}} \cdot \frac{1}{p^{pn}q^{qn}} \cdot \frac{1}{(1-p-q)^{n-(pn+qn)}} =$$

$$= \frac{1}{2\pi n} \cdot \frac{1}{p^{pn+1/2}} \cdot \frac{1}{q^{qn+1/2}} \cdot \frac{1}{(1-p-q)^{n-pn-qn}}$$

THEOREM 3.6. *For graphs* Γ *and* Γ' *associated with the function* $B^n_{P_i,\ldots,P_{n-j}}$ *it holds that* $\Gamma \cong \Gamma'$.

PROOF. We divide the proof into two parts. First we show that none of maximal interval belongs to the core of $B^n_{P_i,\ldots,P_{n-j}}$. Then we proove that each maximal interval belongs to at least one irredundant d.n.f..

First part of the statement means that all vertices of each maximal interval are covered by another maximal interval of $B^n_{P_i,\ldots,P_{n-j}}$. Let N_I be an arbitrary maximal interval with dimension $n-(i+j)$. N_I contains $2^{n-(i+j)}$ vertices. Let $\delta \in N_I$ be an arbitrry vertex such that $\delta \in P_k$, $i \leq k \leq n-j$. Degree of vertex δ is n, with $n-(i+j)$ edges contained in N_I. Let us take a look at the remaining $i+j$ edges. According to the position of N_f in B^n, i and j of them are incident with vertices on level P_{k-1} and P_{k+1} respectively, or vice versa. It implies that i (j) edges are joined with level containing vertices from N_f^-. If we use one of these edges together with $n-(i+j)-1$ edges from N_I we obtain maximal interval N_I' with dimension $n-(i+j)$ containing vertex δ. Thus N_I do not belong to the core.

Maximal interval does not belong to any irredundant d.n.f. iff all of its vertices are covered by core intervals [1]. This together with the first part completes the proof.

THEOREM 3.7. *The degree of each vertex of* $\Gamma(B^n_{P_i,\ldots,P_{n-j}})$ *is*

$$\sum_{m=0}^{n-(i+j)-1}(-1)^m\sum_{k=0}^{n-(i+j)-m}\binom{n-(i+j)}{m}\binom{n-(i+j)-m}{k}\left[\binom{n-m-k-i}{n-m-k-(i+j)}\binom{k+i}{k}-1\right].$$

PROOF. Let N_I be a maximal interval corresponding to v_{N_I} in $\Gamma(B^n_{P_i,\ldots,P_{n-j}})$. In order to count a vertex degree of v_{N_I} we find out the number of maximal intervals which have nonempty intersection with N_I.

The process of evaluation consists of taking all intervals belonging to N_I, one at a time. Let the actual one be denoted as N_M. We count the maximal intervals different from N_I such that N_M is a subset of their intersection with N_I. Let m be a summation variable adressing to dimension of N_M. According to Theorem 3.1. m can gain values from 0 to $n-(i+j)-1$. To make sure that we count each maximal interval having nonempty intersection with N_I only once, we use the inclusion-exclusion principle.

Figure 2 shows possible location of N_M. There are $n-(i+j)-m$ fixed coordinates in N_I, thus we have $\binom{n-(i+j)}{m}$ possibilities to choose m arbitrary coordinates generating N_M. The other summation variable k determines the position of interval N_M, $0\le k\le n-(i+j)-m$. To do so, we choose k coordinates with value 0 from $n-(i+j)-m$ fixed coordinates. It ensures that we go through all levels.

To sum it up there is $\binom{n-(i+j)}{m}\binom{n-(i+j)-m}{k}$ possibilities to choose intersection N_M.

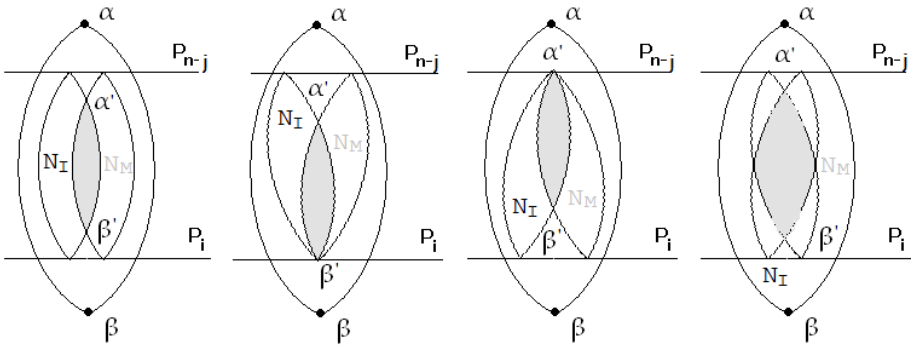


Fig. 2. Possible location of N_M in N_I

Each feasible maximal intervals (different from N_I and containing N_M) is uniquely defined by $n-(i+j)$ edges. m of them generate N_M so we need to choose aditional $n-(i+j)-m$ edges incident to $\alpha'\in N_M$ or $\beta'\in N_M$.

We have to choose these edges in such way that the location of maximal intervals is between i and $n-j$. Therefore we choose k out of $k+i$ edges from $\alpha' \in N_M$ towards α. We have to pick other $n-(i+j)-m-k$ from the edges joined with $\beta' \in N_M$ and leading to β. (There are $n-m-k-i$ such edges.)

The number $\left[\binom{n-m-k-i}{n-m-k-(i+j)}\binom{k+i}{k}-1\right]$ expresses the number of ways to choose other $n-(i+j)-m$ edges except the case when we choose interval N_I itself.

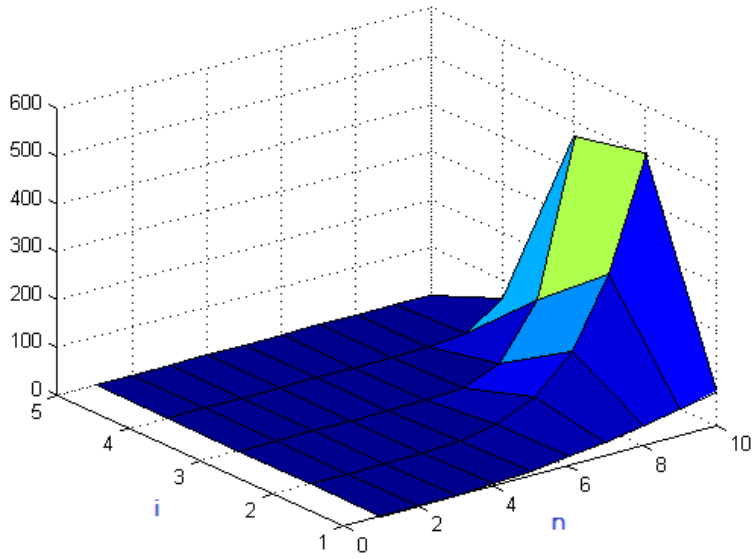
Putting it all together we can see that the vertex degree of v_{N_I} in $\Gamma(B^n_{P_i,\ldots,P_{n-j}})$ is

$$\sum_{m=0}^{n-(i+j)-1}(-1)^m \sum_{k=0}^{n-(i+j)-m}\binom{n-(i+j)}{m}\binom{n-(i+j)-m}{k}\left[\binom{n-m-k-i}{n-m-k-(i+j)}\binom{k+i}{k}-1\right].$$

COROLLARY 3.8. *The degree of each vertex of* $\Gamma(B^n_{P_i,\ldots,P_{n-j}})$ *is*

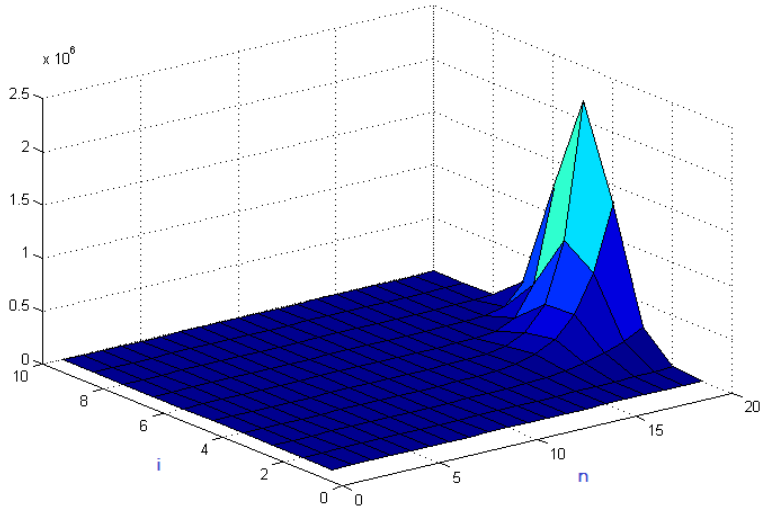
$$\sum_{m=0}^{n-2i-1}(-1)^m \sum_{k=0}^{n-2i-m}\binom{n-2i}{m}\binom{n-2i-m}{k}\left[\binom{n-m-k-i}{n-m-k-2i}\binom{k+i}{k}-1\right].$$

Vertex degree as a function of parameters i and n is computed and shown in the following Figure.



n \ i	1	2	3	4	5
1	0	0	0	0	0
2	0	0	0	0	0
3	2	0	0	0	0
4	6	0	0	0	0
5	12	4	0	0	0
6	20	18	0	0	0
7	30	54	6	0	0
8	42	130	36	0	0
9	56	270	146	8	0
10	72	504	470	60	0

Fig. 3. Vertex degree, cases when $1 < n < 10$, $1 < i < 5$



n \ i	1	2	3	4	5	6	7	8	9
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	2	0	0	0	0	0	0	0	0
4	6	0	0	0	0	0	0	0	0
5	12	4	0	0	0	0	0	0	0
6	20	18	0	0	0	0	0	0	0
7	30	54	6	0	0	0	0	0	0
8	42	130	36	0	0	0	0	0	0
9	56	270	146	8	0	0	0	0	0
10	72	504	470	60	0	0	0	0	0
11	90	868	1280	308	10	0	0	0	0
12	110	1404	3066	1250	90	0	0	0	0
13	132	2160	6636	4250	560	12	0	0	0
14	156	3190	13236	12558	2750	126	0	0	0
15	182	4554	24690	33110	11252	922	14	0	0
16	210	6318	43560	79458	39732	5320	168	0	0
17	240	8554	73326	176250	124222	25492	1414	16	0
18	272	11340	118586	365750	350682	104958	9380	216	0
19	306	14760	185276	716958	907752	380730	51562	2056	18
20	342	18904	280910	1337960	2181256	1240398	242844	15420	270

Fig. 4. Vertex degree, cases when $1 < n < 20$, $1 < i < 10$

In Figures $3-4$ we illustrate obtained result. Red color represents N_f^-.

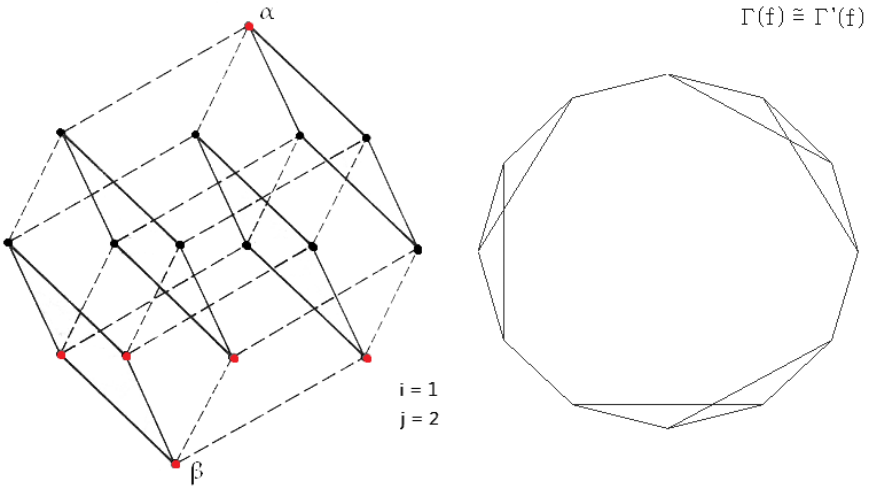


Fig. 5. Geometric representation of $B^4_{P_2,P_3}$

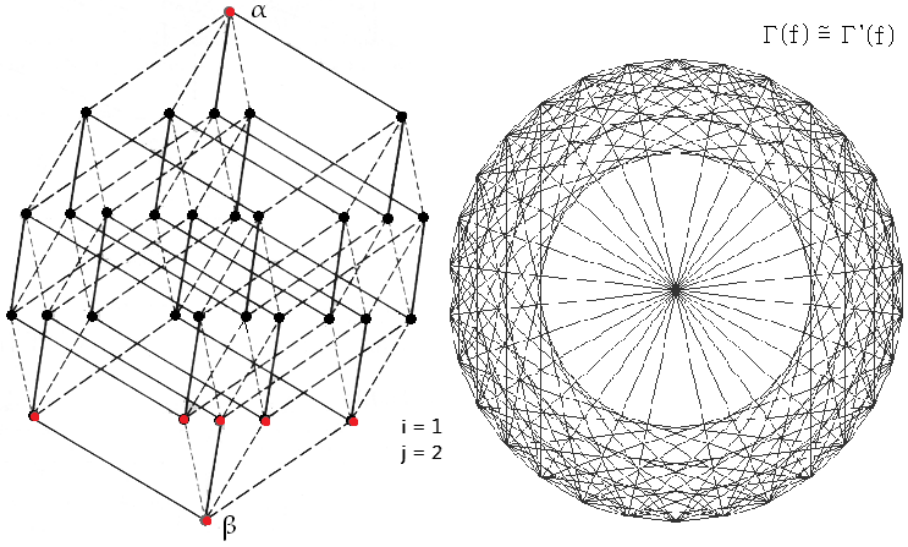


Fig. 6. Geometric representation of $B^5_{P_2,P_3,P_4}$

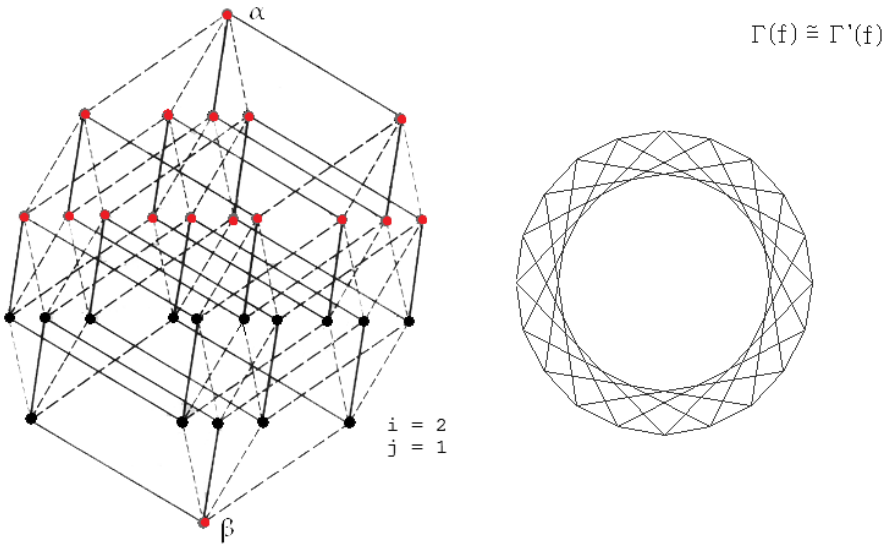


Fig. 7. Geometric representation of $B^5_{P_1,P_2}$

Definition 3.9. Let G be a graph and let $\alpha,\beta \in G$. **The distance from α to β** is the length of a shortest path from α to β. It is denoted by $d(\alpha,\beta)$.

Definition 3.10. The number $e(\alpha) = max\{d(\alpha,\beta)|\beta \in G\}$ is called the **excentricity** of vertex α.

Definition 3.11. The number $r(G)_{\alpha\in G} = \min\{e(\alpha)\}$ is called the **radius** of G.

Definition 3.12. The number $d(G)_{\alpha\in G} = \max\{e(\alpha)\}$ is called the **diameter** of G.

LEMMA 3.13. *The excentricity of all vertices of an n-cube is equal to n.*

PROOF. Distance between two vertices in an n-cube is given by the number of coordinates where the vertices differ. For each vertex in an n-cube there exists an "opposite" vertex which differs in all n coordinates. It implies our statement. □

Using this Lemma we directly obtain the following results.

THEOREM 3.14. *The diameter of maximal intervals of $B^n_{P_i,\ldots,P_{n-j}}$ is $n-(i+j)$.*

THEOREM 3.15. *The radius of maximal intervals of $B^n_{P_i,\ldots,P_{n-j}}$ is $n-(i+j)$.*

THEOREM 3.16. *The diameter of subgraph of B^n induced by N_f of $B^n_{P_i,\ldots,P_{n-j}}$ is* $\min(n, 2n-2\max(i,j))$.

PROOF. We divide the proof into two cases.

First let us assume that $i \leq \lfloor n/2 \rfloor \wedge j \leq \lfloor n/2 \rfloor$. It implies that N_f contains all vertices from level $n/2$ (for n even) or from levels $(n-1)/2$ and $(n+1)/2$ (for n odd). For every vertex α from level $n/2$ there exists vertex α' with opposite coordinates from the same level (for n even). Similarly for every vertex β from level $(n-1)/2$ there exists a vertex β' with opposite coordinates from level $(n+1)/2$ (for n odd). It is clear that in this case the diameter equals n.

Otherwise all vertices from N_f contain at most $\lfloor n/2 \rfloor$ coordinates with value 0 (or 1). Let us refer to this value as k and to its maximal appearance as m. Let us assume vertex δ which contains coordinate k exactly $s \leq m$ times. The opposite vertex $\delta' \in N_f$ can be found by negating as many coordinates as possible. It is possible to turn s coordinates k into $\bar{k}$ and m coordinates $\bar{k}$ can be switched into k. Therefore excentricity of δ is given by $s+m$. As $s \leq m$ it implies that diameter equals $2m$. It is clear that $m = n - \max(i, j)$ which completes the proof. □

THEOREM 3.17. *The radius of subgraph of B^n induced by N_f of $B^n_{P_i,\ldots,P_{n-j}}$ is $n - |i-j|$.*

PROOF. With the help of ideas from previous proof we obtain that vertices with the smallest excentricity are located on the level farthest from central levels. It can be the level i if $i \leq j$ or $n-j$ if $i \geq j$. The vertex on level $n-j$ contains exactly j zeros, vertex on level i contains exactly i ones. Let us look for the vertices with the maximal distance. Without loss of generality, let us choose $\alpha = \{\underbrace{1,\ldots,1}_{n-j},\underbrace{0,\ldots,0}_{j}\}$ and $\beta = \{\underbrace{0,\ldots,0}_{n-i},\underbrace{1,\ldots,1}_{i}\}$. The length of the path between two vertices can be obtained as the number of identical coordinates subtracted from n. In the representation of vertices α and β exists a section where coordinates of α and β are equal. Its length is given by the difference between i and j, in other words $|i-j|$. This facts implies that the diameter of subgraph is $n - |i-j|$. □

Diameter and radius of graph induced by the set N_f of Boolean function $B^5_{P_2,P_3,P_4}$ is illustrated in the following figure.

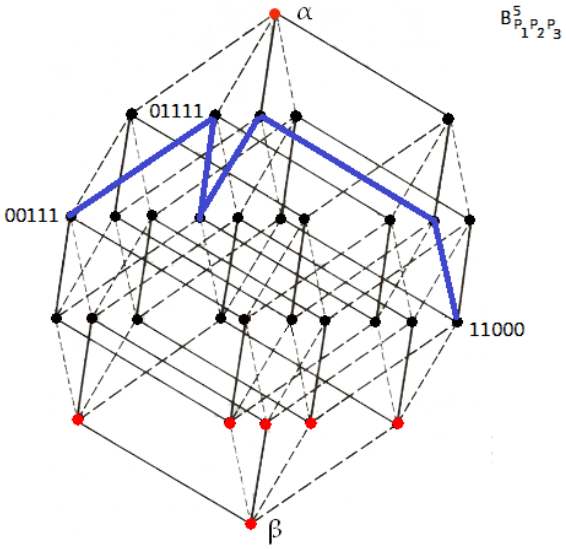


Fig. 8. An illustration of of radius and diameter

4 DISJUNCTIVE NORMAL FORM

In this section we take a look at disjunctive normal forms of $B^n_{P_i,\ldots,P_{n-j}}$.

REMARK 4.1. *The fact that no maximal interval belongs to the core together with the definition of Quin's d.n.f gives us* $D_A = D_Q$.

THEOREM 4.2. *The number of conjunctions of an abbreviated d.n.f. of function* $B^n_{P_i,\ldots,P_{n-j}}$ *is*

$$\binom{n-i}{n-(i+j)} \cdot \binom{n}{i}.$$

PROOF. Straigthforward from Theorem 3.2. □

According to the previous sections the following holds

$$\binom{n-pn}{n-(pn+qn)} \cdot \binom{n}{pn} \sim \frac{1}{2\pi n} \cdot \frac{1}{p^{pn+1/2}} \cdot \frac{1}{q^{qn+1/2}} \cdot \frac{1}{(1-p-q)^{n-pn-qn}},$$

where $i = p.n$, $j = q.n$, $p < \frac{1}{2}$, $p \in Q$.

THEOREM 4.3. *The number of conjunctions of a minimal d.n.f. of function*

$B^n_{P_i,\ldots,P_{n-j}}$ *is*

$$\binom{n}{i}, \qquad if \qquad i > j,$$

$$\binom{n}{j}, \qquad if \qquad i < j.$$

PROOF. Let us divide the proof into two parts. In the first part we describe construction of minimal d.n.f. of the function $B^n_{P_i,\ldots,P_{n-j}}$ and verify its correctness for case $i < j$ and in the second part we repeat it for case $i > j$.

The dimension of maximal intervals corresponding to the conjunctions of minimal d.n.f. is $n-(i+j)$. It implies, that the number of literals in each conjunction is $i+j$. Maximal intervals are located between levels i and $n-j$. As all vertices between these levels contain at least i coordinates with value 1 and at least j with value 0, each conjunction contains i non-negated variables and j negated variables. Independently of the choice of arbitrary coordinates we never get the vertex from levels $0,\ldots,i-1,n-j+1,\ldots,n$.

In the first part we consider the case $i < j$. There are $\binom{n}{j}$ different ways to choose j negated variables out of n variables. We get $\binom{n}{j}$ incomplete conjunctions, to which we add i non-negated variables. They can be obtained by shifting the indices of negated variables. Let us perform this operation for i variables with the biggest indices in a descending order. The index of each negated variables in the current conjunction is decreased to the closest suitable value. It means that there cannot be the same variable in negated and non-negated form at the same time in one conjunction. The shift operation is also cyclic. It is easy to see, that the set of non-negated and negated variables have an empty intersection. We join these two sets with operation AND. Using this construction we get $\binom{n}{j}$ different conjunctions.

Now we show the correctness of our construction. To achieve that, each vertex δ belonging to levels $i,\ldots,n-j$ is contained in at least one maximal interval corresponding to conjunction in our minimal d.n.f.. As there is at least one coordinate with value 1 and one with value 0, there has to exist the pair of coordinates $(1,0)$ (indices are cyclic). In case that more such pairs exist, we always take one with the biggest index of variable corresponding to 0. We omit this pair and repeat this operation i times. As there are at least i coordinates with each value, we can find i such pairs, let us refer to these 0s and 1s as special 1s and 0s. If we take those i special zeros together with other $j-i$ randomly chosen ones and shift i biggest ones of them as described above, we get the positions of i special 1s. Hence

δ is covered by the maximal interval with negated variables on places of chosen 0s (i special and $j-i$ random) and non-negated variables on places of special 1s.

It is easy to see that the number of maximal intervals cannot be lower than $\binom{n}{j}$ as at least one of the vertices on level $n-j$ would not be covered.

Second part of the proof can be obtained analogicaly.

It implies that the number of conjunctions of a minimal d.n.f. of function $B^n_{P_i,\ldots,P_{n-j}}$ is

$$\binom{n}{i}, \qquad if \qquad i > j,$$

$$\binom{n}{j}, \qquad if \qquad i < j.$$

REMARK 4.4. *As all maximal intervals have the same dimension (the number of literals in corresponding conjunctions), minimal d.n.f. of function $B^n_{P_i,\ldots,P_{n-j}}$ is also the shortest one.*

Without loss of generality, let as asume that $i > j$.

THEOREM 4.5. *It holds that*

$$\binom{n}{pn} \sim \frac{1}{2\pi n}.\frac{1}{p^{pn+1/2}}.\frac{1}{(1-p)^{n-pn+1/2}},$$

where $i = p.n$, $p < \frac{1}{2}$, $p \in Q$.

PROOF. Applying Stirling's formula we get

$$\binom{n}{pn} \sim \frac{(\frac{n}{e})^n\sqrt{2\pi n}}{(\frac{n-pn}{e})^{n-pn}.\sqrt{2\pi(n-pn)}.(\frac{pn}{e})^{pn}.\sqrt{2\pi pn}} =$$

$$= \frac{1}{\sqrt{2\pi pn}\sqrt{1-p}}.\frac{1}{p^{pn}}.\frac{1}{(1-p)^{n-pn}} = \frac{1}{2\pi n}.\frac{1}{p^{pn+1/2}}.\frac{1}{(1-p)^{n-pn+1/2}}.$$

These results can be further applied to evaluation of parameters of symmetric Boolean function $B^n_{P_{i_1},\ldots,P_{i_2},\ldots,P_{i_{k-1}},\ldots,P_{i_k}}$ shown in the following Figure.

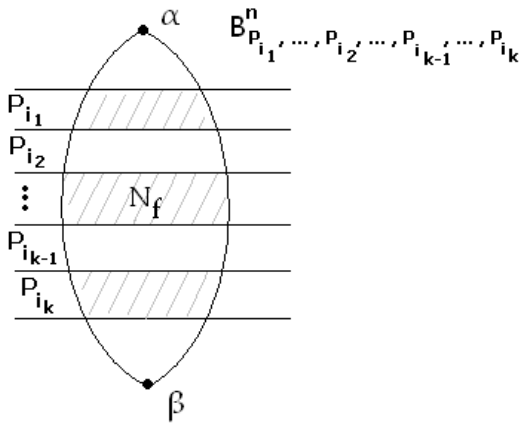


Fig. 9. Function $B^n_{P_{i_1},\dots,P_{i_2},\dots,P_{i_{k-1}},\dots,P_{i_k}}$

5 EXAMPLES

In this section we use obtained results to find asymptotic properties of maximal intervals, interval graphs and d.n.f.s of some chosen functions.

$\mathbf{i = j = n/4}$

The number of maximal intervals, the length of abbreviated d.n.f., the number of vertices of Γ:

$$\binom{3n/4}{n/2}\cdot\binom{n}{n/4} = \frac{n!}{\left(\frac{n}{2}\right)!\left(\frac{n}{4}!\right)^2} \sim \frac{\left(\frac{n}{e}\right)^n\sqrt{2.\pi.n}.e^{\frac{1}{12.n}}}{\left(\frac{n}{2e}\right)^{\frac{n}{2}}\sqrt{\pi.n}.e^{\frac{1}{6.n}}\left(\frac{n}{4e}\right)^{\frac{n}{2}}\frac{\pi.n}{2}.e^{\frac{2}{3.n}}} =$$

$$= \frac{2^{3n/2}.\sqrt{2}.2}{\pi n}.e^{1/12n-2/6n} = \frac{2^{\frac{3}{2}(n+1)}}{\pi n.e^{1/4n}}$$

The dimension of maximal intervals: $n/2$

The radius and diameter of maximal intervals: $\lceil\frac{n}{4}\rceil$

Full d.n.f.:

$$\sum_{k=1/4}^{3/4}\binom{n}{k} = 2^n - 2.\sum_{k=0}^{1/4}\binom{n}{k}$$

Using

$$\sum_{k\le\alpha.n}\binom{n}{k} = 2^{n.H(\alpha)-\frac{1}{2}.\log n+O(1)},$$

where $0 < \alpha < \frac{1}{2}$ and $H(\alpha) = \alpha.\log\frac{1}{\alpha} + (1-\alpha).\log\frac{1}{1-\alpha}$, from [9] for $\alpha = 1/4$ we obtain

$$2^n - 2.\left(2^{n.(1/4\lg 4+3/4\lg 4/3)-\frac{1}{2}\lg n/4+O(1)}\right) =$$

$$= 2^n - 2^{1+\frac{n}{2}+\frac{3n}{2}+3n\ over 4\lg 3+1-\frac{1}{2}\lg n+O(1)} =$$

$$= 2^n - 2^{2n-\frac{3}{4}n\lg 3-\frac{1}{2}\lg n+O(1)}$$

$\mathbf{i = j = \sqrt{n}\log n}$

The number of maximal intervals, the length of abbreviated d.n.f., the number of vertices of Γ:

$$\left(\frac{n-\sqrt{n}\lg n}{n-2\sqrt{n}\lg n}\right).\left(\frac{n}{\sqrt{n}\lg n}\right) = \frac{n!}{(n-2\sqrt{n}\lg n)!\left[(\sqrt{n}\lg n)!\right]^2} =$$

$$= \prod_{k=0}^{2\sqrt{n}\lg n} \frac{(n-i)}{\left[(\sqrt{n}\lg n)!\right]^2} =$$

$$= \frac{n(n-1)}{(\sqrt{n}\lg n)^2}.\frac{(n-2)(n-3)}{(\sqrt{n}\lg n-1)^2}.\frac{(n-2\sqrt{n}\lg n+2)(n-2\sqrt{n}\lg n+1)}{2} \sim$$

$$\sim \frac{\left(\frac{n}{e}\right)^n \sqrt{2.\pi.n}.e^{\frac{1}{12.n}}.e^{\frac{-1}{12(n-2\sqrt{n}\lg n)}}.e^{\frac{-1}{6(\sqrt{n}\lg n)}}}{\left(\frac{n-2\sqrt{n}\lg n}{e}\right)^{n-2\sqrt{n}\lg n}.\left(\frac{\sqrt{n}\lg n}{e}\right)^{2\sqrt{n}\lg n}.\sqrt{2\pi(n-2\sqrt{n}\lg n).(2\pi\sqrt{n}\lg n)}} =$$

$$= \frac{\left(\frac{1}{1-\frac{2}{\sqrt{n}}\lg n}\right)^{n-2\sqrt{n}\lg n+1/2}\left(\frac{\sqrt{n}}{\lg n}\right)^{2\sqrt{n}\lg n}}{2\pi\sqrt{n}\lg n}$$

The dimension of maximal intervals: $n - 2\sqrt{n}\lg n$

The radius and diameter of maximal intervals: $\lceil n/2 - \sqrt{n}\lg n\rceil$

Full d.n.f.:

$$\sum_{k=\sqrt{n}\lg n}^{n-\sqrt{n}\lg n}\binom{n}{k} = 2^n - 2.\sum_{k=0}^{\sqrt{n}\lg n}\binom{n}{k}$$

Using

$$\sum_{k\le\alpha.n}\binom{n}{k} = 2^{n.H(\alpha)-\frac{1}{2}.\log n+O(1)},$$

where $0 < \alpha < \frac{1}{2}$ and $H(\alpha) = \alpha.\log\frac{1}{\alpha} + (1-\alpha).\log\frac{1}{1-\alpha}$, z [9] for $\alpha = \frac{\lg n}{\sqrt{n}}$ we obtain

$$2^n - 2.\left(2^{n.\left(\frac{\lg n}{\sqrt{n}}\lg\frac{1}{\frac{\lg n}{\sqrt{n}}} + \left(1-\frac{\lg n}{\sqrt{n}}\right)\lg\left(1-\frac{\lg n}{\sqrt{n}}\right)\right) - \frac{1}{2}\lg\sqrt{n}\lg n + O(1)}\right) =$$

$$= 2^n - 2^{1-\sqrt{n}\lg n\lg\lg n + 1/2\sqrt{n}(\lg n)^2 - n\lg(1-\frac{\lg n}{\sqrt{n}}) + \sqrt{n}\lg n\lg(1-\frac{\lg n}{\sqrt{n}}) - 1/4(\lg\sqrt{n})^2 + O(1)} =$$

$$= 2^n - 2^{\sqrt{n}\lg n\lg\lg n + 1/2\sqrt{n}(\lg n)^2 + \sqrt{n}\lg n - 5/4(\lg n)^2 + O(1)}$$

We have chosen the case $i = \sqrt{n}\log n$ because the following holds [10]:

$$|\bigcup_{t=n/2-\sqrt{n}\log n}^{n/2+\sqrt{n}\log n} B_t^n| = |B^n| = 2^n.$$

6 CONCLUSION

In the present paper we have studied the properties of symmetric Boolean functions $B^n_{P_i,\ldots,P_{n-j}}$, $i + j < n$. We have evaluated the number, dimension, radius and diameter of its maximal intervals. We have also considered the characteristics of graphs Γ and Γ' corresponding to $B^n_{P_i,\ldots,P_{n-j}}$. Then we have counted the vertex degrees of interval and simplified interval graphs. We have got some result regarding disjunctive normal forms. Finally we have presented examples to illustrate obtained result.

REFERENCES

[1.] Jablonski S. V., Introduction into discrete mathematics, Moscow, Nauka, 1979 (in Russian).

[2.] Jablonski S. V. and Lupanov O. B., Discrete mathematics and Mathematical Problems of Cybernetics, Nauka, Moscow, 1974, (in Russian), pages 99148.

[3.] Sapozhenko A. A., Disjunctive Normal Forms, Moscow University Press, Moscow, 1975 (in Russian).

[4.] Toman E., Haviarova L., Properties of the interval graph of a Boolean function, Acta Mathematica Universitatis, 2013, Vol. LXXXII, 2 (2013), pages 191200.

[5.] Wegener I., The Complexity of Boolean Functions, New York: Wiley, 1987

[6.] Fagin R., Klawe M., Pippenger N. and Stockmeyer L., Bounded-depth, polynomial-size circuits for symmetric functions, Theoretical Computer Science, 1985, Vol. 36, pages 239250.

[7.] Denenberg L., Gurevich Y. and Shelah S., Definability by constant-depth polynomial-size circuits, Information and Control, 1986, Vol. 70(2/3), pages 216240.

[8.] Canteaut A. and Videau M., IEEE Transactions On Information Theory, Symmetric Boolean Functions, 2005.

[9.] Graham R., Knuth D., Patashnik O., Concrete Mathematics a Foundation for Computer Science, Addison-Wesley Publishing Company, 1989.

[10.] Nigmatulin R. G., The Complexity of Boolean Functions, Kazan, University Press, 1983.

[11.] Toman E., Haviarova L., The Number of Monotone and Self-Dual Boolean Functions, Journal of Applied Mathematics, Statistics and Informatics, 2014, Vol. 10, pages 93-111.

L. Haviarova and E. Toman
Comenius University
Faculty of Mathematics, Physics and Informatics
Department of Computer Science
Mlynska dolina, 842 48 Bratislava
Slovak Republic