Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

**RNDr. LUCIA HAVIAROVÁ**

**Autoreferát dizertačnej práce**

# Geometrická štruktúra Booleovských funkcií

**na získanie akademického titulu philosophiae doctor**

**v odbore doktorandského štúdia: 9.2.1. informatika**

**Bratislava 2015**

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na Katedre informatiky Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave.

**Predkladateľ:** RNDr. Lucia Haviarová
Katedra Informatiky
Fakulta matematiky, fyziky a informatiky
Univerzity Komenského
Mlynská dolina
842 48 Bratislava

**Školiteľ:** doc. RNDr. Eduard Toman, CSc.
Katedra informatiky FMFI UK
Bratislava

**Oponenti:** ................................................
................................................
................................................
................................................
................................................
................................................

Obhajoba dizertačnej práce sa koná ..................... o ............. h
pred komisiou pre obhajobu dizertačnej práce v odbore doktorandského štúdia vymenovanou predsedom odborovej komisie .......................................

v študijnom odbore 9.2.1. informatika

na Fakulte matematiky, fyziky a informatiky UK, Mlynská dolina, miestnosť

**Predseda odborovej komisie:**
Prof. RNDr. Branislav Rovan, PhD.
Fakulta matematiky, fyziky a informatiky
Univerzity Komenského
Mlynská dolina
842 48 Bratislava

# Predhovor

Úloha minimalizácie booleovských funkcií spočíva v tom, ako pre ľubovoľnú booleovskú funkciu zostrojiť formulu tvaru disjunkcia konjunkcií, ktorá ju realizuje a obsahuje minimálny počet premenných. Už v 19. storočí vzbudili pozornosť špecialistov v oblasti matematickej logiky rôzne úvahy súvisiace s týmto problémom.

Matematické smery v oblasti výskumu disjunktívnych normálnych foriem pozostávajú zo štúdia okruhu otázok, dotýkajúcich sa najmä algoritmických problémov, ktoré vznikajú pri minimalizácii, štúdiom číselných charakteristík booleovských funkcií, kvantitatívnych vzťahov medzi rôznymi typmi disjunktívnej normálnej formy a klasifikáciou booleovských funkcií.

Osobitný vklad do matematických smerov výskumu predstavujú práce S. V. Jablonskeho, v ktorých sa systematizovali základné pojmy, definície a metódy minimalizácie booleovských funkcií v triede disjunktívnych normálnych foriem.

S booleovskými funkciami sa spája niekoľko typov grafov. Najväčšia pozornosť je venovaná štúdiu grafu indukovaného vrcholmi $n$-rozmernej kocky, na ktorých booleovská funkcia nadobúda hodnotu 1 (S. V. Jablonski).

Ďalší typ grafu, ktorý reprezentuje booleovské funkcie je intervalový graf (A. A. Sapozhenko).

Je to graf, ktorého vrcholy odpovedajú maximálnym intervalom booleovskej funkcie, pričom dva vrcholy tohto grafu sú spojené hranou práve vtedy, keď príslušné maximálne intervaly majú neprázdny prienik. Parametre, ako sú veľkosť a počet komponentov súvislosti polomer a priemer intervalových grafov bezprostredne súvisí s lokálnymi algoritmami (J. I. Zhuravlev).

Istý vklad do štúdia grafov spojených s booleovskými funkciami priniesli aj slovenskí informatici E. Toman, M. Škoviera, D. Olejár, M. Stanek, J. Daubner, T. Kulich, Ľ. Baník, J. Hromkovič, J.Šiška… O ich výsledkoch, tiež o výsledkoch iných autorov hovoríme nižšie.

# Úvod

Úloha minimalizácie zohrala hlavnú úlohu pri tvorbe logických obvodov a ich syntéze a analýze. Vznik a rozvoj teórie bol ovplyvnený najmä problémami pri návrhu reléovo-kontaktových obvodov pri stavbe telekomunikačných a riadiacich zariadení. Základy tejto teórie položili najmä práce C. E. Shannona. Významnejší rozvoj teórie logických systémov nastáva po 2. svetovej vojne najmä v súvislosti s rozvojom počítačov.

V súvislosti s týmto problémom sa rozvíjali aj iné oblasti teoretickej informatiky, napríklad teória kódovania, teória testov, teória oddeliteľnosti množín, teória rozpoznávania obrazcov, ... V nasledujúcej časti uvedieme niektoré z problémov.

**Teória testov:** Nech $M$ je množina navzájom rôznych funkcií $f(x_1, x_2, \ldots, x_n)$ definovaných na množine $A$ a nadobúdajúcich hodnoty z množiny $B$. Nech $N$ je daná podmnožina neusporiadaných dvojíc rôznych funkcií. Množina $T$, $T \subset A$ nazývame testom vzhľadom na $A$, $M$ a $N$, ak pre ľubovoľnú dvojicu funkcií platí $\{f, g\} \in N$, $f(x_1, \ldots, x_n) \neq g(x_1, \ldots, x_n)$ na množine $T$. Mohutnosť množiny $T$ nazývame dĺžka testu.

**Oddeliteľnosť množín:** Nech $B^n$ je booleovská kocka.

Uvažujme čiastočnú booleovskú funkciu danú predpisom:

$$f(x_1,\dots,x_n) = \begin{cases} 0, \text{ ak } (x_1,\dots,x_n) \in N_f^- \\ 1, \text{ ak } (x_1,\dots,x_n) \in N_f \\ \text{nie je definovaná, ak } (x_1,\dots,x_n) \in B^n \setminus (N_f \cup N_f^-) \end{cases}$$

kde $N_f \cap N_f^- = \emptyset$, $N_f^- \subset B^n$, $N_f \subset B^n$. Nech $P_2(n)$ je množina booleovských funkcií $n$-premenných a nech $P(f)$ je číselná funkcia na $P_2(n)$. Túto funkciu budeme nazývať funkcia zložitosti charakterizujúca funkciu $f \in P_2(n)$. Funkciu $f' \in P_2(n)$ nazývame prípustnou vzhľadom na $f$, ak pre všetky $\alpha \in N_f^-$, $f'(\alpha) = 0$ a pre všetky $\beta \in N_f$, $f'(\beta) = 0$. Úloha oddeliteľnosti množín spočíva v nájdení takej $f^*$ spomedzi všetkých, pre ktorú funkcia zložitosti $P^*(f)$ nadobúda minimálnu hodnotu. Táto úloha sa dá interpretovať na rôzne typy zložitosti funkcií.

# Vlastnosti intervalového grafu booleovskej funkcie

V práci ukážeme, že ak je intervalový graf booleovskej funkcie kompletný, skrátená d.n.f. prislúchajúcej funkcie je zároveň minimálna. Tiež ukážeme, že pre ľubovoľný konečný jednoduchý graf vieme zostrojiť booleovskú funkciu, ktorej skrátená d.n.f. je súčasne minimálna a jej intervalový graf je izomorfný s týmto grafom. Skúmame aj otázku počtu premenných hľadanej booleovskej funkcie.

**Veta 0.1** *Ak $\Gamma(f)$ booleovskej funkcie $f$ je kompletný, potom prienik jej maxi-málnych intervalov je neprázdny.*

**Veta 0.2** *Nech $f$ je booleovská funkcia $n$ premenných. Ak $\Gamma(f)$ je kompletný, potom $D_A(f) = D_M(f)$.*

V práci uvádzame aj obrátené tvrdenie a protiplíkad, ktorým ukáže, že neplatí.

**Veta 0.3** *Nech $G$ je graf rádu $n$. Potom existuje booleovská funkcia $f(x_1, \ldots, x_n)$ taká, že $D_A(f) = D_M(f)$ a $\Gamma(f) \cong G$.*

Tvrdenie dokážeme matematickou indukciou s konštruktívnym charakterom vzhľadom na $n$.

# Počet monotónnych a samoduálnych booleovských funkcií

V tejto kapitole ukážeme, že intervalový graf monotónnej booleovskej funkcie je kompletný. Z toho vyplýva, že skrátená d.n.f. tejto funkcie je zároveň minimálna a najkratšia. Ďalej ukážeme, ako vyzerá najzložitejšia d.n.f. monotónnej booleovskej funkcie a ukážeme, koľko konjunkcií takáto d.n.f. obsahuje.

**Veta 0.4** *Intervalový graf* $\Gamma(f)$ *monotónnej booleovskej funkcie* $f$ *je úplný.*

**Veta 0.5** *Nech* $f$ *je monotónna booleovská funkcia* $n$ *premenných s najväčším počtom* $m$ *konjunkcií v* $D_A(f)$ *(počtom maximálnych intervalov v* $B^n$*). Potom* $m = \binom{n}{\lfloor n/2 \rfloor}$.

Tiež uvedieme počty monotónnych booleovských funkcií, ktorých maximálne intervaly spĺňajú špeciálne podmienky. Doteraz známe výsledky týkajúce sa určenia počtu monotónnych booleovských funkcií používajú metódu založenú na dodefinovaní monotónnej funkcie na rastúcich po dvoch disjunktných cestách v $B^n$ (Hansel, Kleitman, Korshunov). My sa na tento problém pozeráme z hľadiska monotónnych funkcií s predpísanými vlastnosťami maximálnych intervalov - maximálne intervaly s rovnakým rozmerom a maximálne intervaly s predpísaným prienikom.

**Veta 0.6** *Nech* $G = (V, E)$ *je kompletný graf rádu* $m$. *Potom počet monotónnych booleovských funkcií* $n$ *premenných, ktorých maximálne intervaly majú rovnaký rozmer a pre ktoré platí* $\Gamma(f) \cong G$ *je*

$$\sum_{i=0}^{n} \binom{\binom{n}{i}}{m},$$

*kde* $m \leq \binom{n}{\lfloor n/2 \rfloor}$.

**Veta 0.7** *Nech* $G = (V, E)$ *je kompletný graf s* $m$ *vrcholmi. Potom počet monotónnych booleovských funkcií* $n$ *premenných, ktoré majú predpísaný prienik maximálnych intervalov* $I = \{\underbrace{(1, \ldots, 1)}_{n}\}$ *a pre ktoré platí*

$\Gamma(f) \equiv G$ *je*

$$\frac{\sum\limits_{i=0}^{m} (-1)^i . \binom{m}{i} . (m + 1 - i)^n}{m!},$$

*kde* $1 \leq m \leq n - 1$.

**Veta 0.8** *Nech* $S_m = \frac{\sum\limits_{i=0}^{m} (-1)^i . \binom{m}{i} . (m+1-i)^n}{m!}$. *Platí*

$$\frac{1}{2}((m + 1)^2 + m + 3)(m + 1)^{n-m-1} - 1 \leq S_m \leq \frac{1}{2} \binom{n + 1}{m + 1} (m + 1)^{n-m},$$

*pre* $n \geq 2$ *a* $1 \leq m \leq n - 1$.

Tiež uvedieme horný a dolný odhad počtu monotónnych a zároveň samoduálnych booleovských funkcií.

# Symetrická booleovská funkcia

V tejto kapitole sa zaoberáme parametrami pre funkciu $B^n_{P_i,\ldots,P_{n-j}}$, $i \neq j$, $i + j < n$. Ukážeme, čo platí pre počet, rozmer, polomer a priemer maximálnych intervalov funkcie. Charakterizujeme vlastnosti grafov $\Gamma$ a $\Gamma'$ funkcie a získame hodnotu stupňa vrchola týchto grafov. Pre zaujímavé hodnoty uvádzame aj asymptotické hodnoty získaných parametrov.

**Veta 0.9** *Rozmer maximálnych intervalov booleovskej funkcie $B^n_{P_i,\ldots,P_{n-j}}$ je*

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

**Veta 0.10** *Počet maximálnych intervalov booleovskej funkcie $B^n_{P_i,\ldots,P_{n-j}}$ je*

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

**Veta 0.11** *Pre graf $\Gamma$ a graf $\Gamma'$ funkcie $B^n_{P_i,\ldots,P_{n-j}}$ platí $\Gamma \cong \Gamma'$.*

**Veta 0.12** *Stupeň ľubovoľného vrchola grafu $\Gamma(B^n_{P_i,\ldots,P_{n-j}})$ je*

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

**Veta 0.13** *Priemer grafu indukovaného množinou $N_f$ booleovskej funkcie $B^n_{P_i,\ldots,P_{n-j}}$ je* $\min(n, 2n - 2\max(i, j))$.

**Veta 0.14** *Polomer grafu indukovaného množinou $N_f$ booleovskej funkcie $B^n_{P_i,\ldots,P_{n-j}}$ je $n - |i - j|$.*

Zaoberáme sa aj disjunktívnymi normálnymi formami symetrickej booleovskej funkcie $B^n_{P_i,\ldots,P_{n-j}}$.

# Záver

V teórii disjunktívnych normálnych foriem autori vyriešili mnoho problémov. Zostrojili algoritmy na konštrukciu rôznych typov d.n.f.: skrátených, iredundantných, minimálnych a iných d.n.f. uvedených v kapitole Základné pojmy. Nemalá časť štúdia je venovaná skúmaniu problémov zložitosti univerzálnych prístupov k úlohe minimalizácie jednak na kvalitatívnej úrovni - teória lokálnych algoritmov a tiež na kvantitatívnej úrovni - metrická teória. Podarilo sa získať dostatočne veľa modelových funkcií, metód, konštrukcií umožňujúcich zostrojiť booleovské funkcie a d.n.f. s danými vlastnosťami. Naďalej sa rozvíjajú metódy na získavanie odhadov parametrov pre skoro všetky funkcie s extremálnymi hodnotami parametrov.

V dizertačnej práci sme ukázali, že ak je intervalový graf booleovskej funkcie kompletný, skrátená d.n.f. danej funkcie je zároveň minimálna. Ďalej sme ukázali, že pre ľubovoľný jednoduchý graf vieme zostrojiť booleovskú funkciu, ktorej skrátená d.n.f. je súčasne minimálna a jej intervalový graf je izomorfný s týmto grafom. Skúmali sme aj otázku počtu premenných hľadanej booleovskej funkcie.

Ďalej sme sa zaoberali monotónnymi a samoduálnymi booleovskými funkciami. Ukázali sme, že intervalový graf monotónnych booleovských funkcií je kompletný. Tiež sme uviedli, ako vyzerá najzložitejšia d.n.f. monotónnej booleovskej funkcie a ukázali sme, koľko konjunkcií takáto d.n.f. obsahuje.

Odhadli sme aj počet monotónnych booleovských funkcií, ktorých maximálne intervaly majú špeciálne vlastnosti a počet monotónnych a zároveň samoduálnych funkcií.

V ďalšej časti sme sa zaoberali vlastnosťami symetrickej booleovskej funkcie. V práci uvádzame, čo platí pre počet, rozmer, polomer a priemer maximálnych intervalov funkcie. Tiež sme charakterizovali vlastnosti intervalového a zjednodušeného intervalového grafu funkcie a zistili hodnotu stupňa vrcholov týchto grafov. Zaoberali sme sa aj príslušnými disjunktívnymi normálnymi formami.

Zaujímavým problémom je získať na základe charakterizácie intervalového grafu, resp. zjednodušeného intervalového grafu prípadne iných typov grafov isté triedy grafov a určiť ich vzťah k skrátenej d.n.f., Quinovej d.n.f. prípadne k optimálnym vyjadreniam booleovskej funkcie a tiež charakterizovať, na základe výsledkov odhadu veľkosti stupňa intervalového grafu a veľkostí okolí konjunkcií, zložitosť istých lokálnych algoritmov. K takým problémom v oblasti metrickej teórie patria: získať asymptotický odhad maximálnej dĺžky skrátenej d.n.f. pre skoro všetky funkcie, upresnenie odhadu maximálneho počtu iredundantných d.n.f., získanie netriviálneho odhadu počtu minimálnych d.n.f. pre skoro všetky funkcie, zistiť počet ireducibilných pokrytí symetrickej booleovskej funkcie popísanej v práci a niektoré ďalšie. Táto problematika stále nie je uzavretá, existuje celý rad otvorených problémov, ktoré je možné riešiť.

# Literatúra


[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)

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

[4] Sapozhenko A. A., Geometric structure of almost all Boolean, Problemy kibernetiky, Vol. 30, 1975, 227-261, (in Russian)

[5] Sapozhenko A. A., Metric properties of almost all Boolean function, Diskret. Anal., 1967, (in Russian), Vol. 10, 91-119

[6] Zhuravlev J. I., Set theoretical methods in the algebra of logic, Problemy kibernetiki, Vol. 8, 1962, 5-44, (in Russian).

[7] Toman E., On the size of a neighbourhood of the first rank, Computers and Artificial Intelligence, Vol.12, No. 2, 1993, 123-130

[8] Daubner J. and Toman E., Vertex degree in the interval graph of a random Boolean function, Acta Mathematica Universitatis Comenianae, Vol. 79, No. 2, 2010, 151-164

[9] Toman E., Olejar D. and Stanek M., Average degree in the interval graph of a random Boolean function, Computing and Informatics, Vol. 27, 2008, 627-638

[10] Daubner J. and Toman E., Neighbourhood of the constant order in the interval graph of a random Boolean functionFundamenta Informaticae, 2012, Vol. 122, 1-21

[11] Toman E. and Tomanova J., Some estimates of the complexity of disjunctive normal forms of a random Boolean function, Computers and Artificial Intelligence, Vol. 10, No. 4, 1991, 327-340

[12] Toman E. and Stanek M., The Effectivity of some local algorithms for symplifying the random Boolean function, 1986, 48-49

[13] Toman E., Geometric structure of random Boolean function, Problemy Kibernetiki, 1979, (in Russian), Vol. 35, 111-132

[14] Skoviera M., On the minization of random Boolean function I., Computers and Artificial Intelligence, Vol. 5, No. 4, 1986, 321-334

[15] Skoviera M., On the minization of random Boolean function II., Computers and Artificial Intelligence, Vol. 5, No. 6, 1986, 493-509

[16] Kulich T., The Diameter of a Random Subgraph of the Hypercube, Random Structures & Algorithms, 2012, Vol. 41, No. 2, 282-291

[17] Frištacký N., Kolesár M., Kolenička J., Hlavatý J., Logické systémy, Alfa, 1986

[18] Kostochka A. V., Sapozhenko A. A., Weber K., Radius and Diameter of Random Subgraph of the Hypercube, Random Structures and Algorithms, Vol. 4, No. 2, 1993

[19] Post E., Introduction to a general theory of elementary propositions, American Journal of Mathematics, 1921, Vol. 4, 163-185

[20] Altun M. and Riedel M. D., A Study on Monotone Self-dual Boolean Functions, SIAM Journal on Discrete Mathematics, 2012, 10 pages

[21] Kleitman D., On Dedekind's problem: the number of monotone Boolean functions, Proc. Amer. Math. Soc., 1969, Vol. 21, 677-682

[22] Dedekind R., Über Zerlegungen von Zahlen durch ihre größten gemeinsamen Teiler, Gesammelte Werke, 1897, Vol. 2, 103-148

[23] Church R., Numerical analysis of certain free distributive structures, Duke Mathematical Journal, 1940, Vol. 6, 732-734

[24] Ward M., Note on the order of free distributive lattices, Bulletin of the American Mathematical Society, 1946, Vol. 52, 423

[25] Gilbert E. N., Lattice theoretic properties of frontal switching functions, J. Math. Physics, 1954, Vol. 33, 57-67

[26] Yamamoto K., Note on the order of free distributive lattices, Science Reports of the Kanazawa University, 1953, Vol. 2, No. 1, 5-6

[27] Yamamoto K., Logarithmic order of free distributive lattice, Journal of the Mathematical Society of Japan, 1954, Vol. 6, 343-353

[28] Markowsky G., Combinatorial aspects of lattice theory with applications to the enumeration of free distributive lattices, Ph.D. Thesis, Harvard University, 1973

[29] Kleitman D., Markowsky G., On Dedekind's problem: the number of isotone Boolean functions. II, Transactions of the American Mathematical Society, 1975, Vol. 213, 373-390

[30] Korshunov, A. D., The number of monotone Boolean functions, Problemy Kibernetiki, 1981, Vol. 38, 5-108

[31] Hansel G., Sur le nombre des fonctions booléennes monotones de $n$ variables, C. R. Acad. Sci. Paris, 1966, Vol. 262, No. 20, 1088-1090 (French)

[32] Graham, Knuth, Patashnik, Concrete Mathematics a Foundation for Computer Science, Addison-Wesley Publishing Company, 1989

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

[34] E.Sperner, Ein Satz über Untermengen einer endlichen Menge, *Math.Z.*, 27(1928), pp. 544-548

[35] G. Grätzer, *Lattice Theory: Foundation*, Springer Basel AG, 2011

[36] Movsisyan Yu. M., Aslanyan V.A., A functional completeness theorem for De Morgan functions, *Discrete Appl. Math.*, 2014, 162, 1-16

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

[38] Fagin, Klawe, Pippenger and Stockmeyer, Bounded-depth, polynomial-size circuits for symmetric functions, Theoretical Computer Science, 1985

[39] Denenberg, Gurevich and Shelah, Definability by constant-depth polynomial-size circuits, Information and Control, 1986

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

# Publikačná činnosť autora so vzťahom ku skúmanej problematike

[1.] Toman E., Haviarová L., Properties of the interval graph of a Boolean function, Acta Mathematica Universitatis, 2013

[2.] Toman E., Haviarová L., The Number of Monotone and Self-Dual Boolean Functions, Journal of Applied Mathematics, Statistics and Informatics, 2014

# Abstrakt

Cieľom práce je štúdium intervalového grafu, prípadne ďalších typov grafov reprezentujúcich booleovské funkcie. Predovšetkým ide o skúmanie takých vlastností a parametrov uvedených typov grafov, ktoré majú vzťah k algoritmom minimalizácie booleovských funkcií v triede d.n.f a k určeniu počtu istých tried booleovských funkcií, respektíve k ich testovaniu.

KĽÚČOVÉ SLOVÁ: booleovská funkcia, disjunktívna normálna forma, intervalový graf, maximálny interval

# Abstract

The aim of the thesis is the study of interval graph, or further types of graphs representing Boolean functions. In the first place, the examination will concern those characteristics and parameters of the mentioned types of graphs, which have a relation to algorithms of minimization of Boolean functions in d.n.f class, as well as to enumeration of certain classes of Boolean functions or to their testing.

KEYWORDS: Boolean function, disjunctive normal form, interval graph, maximal interval