Metrické vlastnosti boolovských funkcií s daným počtom jednotiek

Ján Reguli

2008

Metrické vlastnosti boolovských funkcií s daným počtom jednotiek

DIPLOMOVÁ PRÁCA

Ján Reguli

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
KATEDRA INFORMATIKY

Vedúci dipl. práce:
Doc. RNDr. Eduard Toman, Csc.

BRATISLAVA 2008

Prehlasujem, že som diplomovú prácu vypracoval samostatne s odbornou pomocou školiteľa a s využitím uvedenej literatúry.

Bratislava, máj 2008 Ján Reguli

Poďakovanie

Ďakujem Doc. RNDr. Eduardovi Tomanovi, CSc za sprístupnenie literatúry, odborné konzultácie, ako aj cenné pripomienky a rady pri písaní diplomovej práce.

Motto:

Chuť k práci je prvou pomôckou k úspechu, vytrvalosť druhou.

(S. Marden)

Abstrakt

Skúmame náhodné boolovské funkcie *n* premenných, ktorých počet jednotiek je daný funkciou $m(n)$, $0 \leqslant m(n) \leqslant 2^n$. Táto práca prezentuje asymptotické odhady maximálnej dĺžky iredundantnej disjunktívnej normálnej formy a počtu iredundantných disjunktívnych normálnych foriem náhodnej boolovskej funkcie.

Kľúčové slová: Náhodná boolovská funkcia, disjunktívna normálna forma, minimalizácia, pravdepodobnostné metódy.

Obsah

1.	**Úvod**	**1**
2.	**Predbežné kroky**	**5**
3.	**Cieľ práce**	**17**
4.	**Intervaly**	**20**
5.	**Hlavný dôkaz**	**39**
6.	**Záver**	**47**
7.	**Literatúra**	**49**

Kapitola 1

Úvod

N-árna boolovská funkcia je ľubovoľné zobrazenie z množiny $\{0, 1\}^n$ do množiny $\{0, 1\}$. Z tohto dôvodu existuje práve 2^{2^n} *n*-árnych boolovských funkcií. Každú boolovskú funkciu (okrem $f \equiv 0$) možno vyjadriť pomocou disjunktívnej normálnej formy (DNF), pričom pre jednu boolovskú funkciu môže existovať viacero vyjadrení pomocou DNF. Konkrétne pre 2^{2^n} *n*-árnych boolovských funkcií existuje až 2^{3^n} disjunktívnych normálnych foriem. Teda môžeme hovoriť o zložitosti aj o minimalizácii DNF. Dôležitú úlohu teórie boolovských funkcií tvorí práve hľadanie čo najjednoduchšieho vyjadrenia boolovskej funkcie v danej triede formúl. Okrem samotného matematického hľadiska je motiváciou riešenia problému i fyzikálne hľadisko. Každej DNF odpovedá určitý elektrický obvod, pričom komplikovanosť schémy daného obvodu priamo súvisí so zložitosťou jemu

prislúchajúcej DNF. Vlastnosti boolovských funkcií, ktoré vyjadrujú kvantitatívnu stránku minimalizácie a zložitosť jednotlivých krokov, nazývame metrické vlastnosti boolovských funkcií.

Na určenie zložitosti disjunktívnej normálnej formy slúži tkz. index jednoduchosti. Ide o funkcionál, ktorý nie je konkrétne určený, avšak sú naňho kladené štyri podmienky (axiómy) a to nezápornosť, monotónnosť (vzhľadom na násobenie), vypuklosť (vzhľadom na sumáciu) a invariantnosť. V práci budeme používať počet elementárnych konjunkcií v disjunktívnej normálnej forme ako index jednoduchosti danej DNF (ozn. $L(N)$). Disjunktívnu normálnu formu, ktorá je minimálna vzhľadom na index jednoduchosti $L(N)$ budeme nazývať najkratšia DNF. Je zrejmé, že každá boolovská funkcia má len konečný počet rôznych DNF, a teda konštrukciu minimálnej disjunktívnej normálnej formy možno uskutočniť konečným počtom krokov. Problém je, že zložitosť úplného prehľadávania je priveľká už pre malé hodnoty *n*. Preto je vhodnejšie pristupovať k minimalizácii postupne, v niekoľkých krokoch.

Známe algoritmy na hľadanie minimálnej DNF v danej triede formúl pracujú vo viacerých etapách. Ako prvá sa skonštruuje skrátená DNF pomocou nejakej jednoducho konštruovateľnej reprezentácie DNF, ako je úplná disjunktívna normálna forma, úplná konjunktívna normálna forma, prípadne tabuľka. Odstránením nadbytočných implikantov zo skrátenej DNF dostávame iredundantné DNF. Následne prehľadávaním všetkých iredundantných DNF nájdeme požadovanú minimálnu DNF

vzhľadom na daný index jednoduchosti. Metrické vlastnosti charakterizujú obtiažnosť jednotlivých krokov minimalizácie, poukazujú na počet variantov, ktoré treba navzájom porovnať, či prehliadnuť a tým umožňujú zvoliť v konkrétnych prípadoch správny postup riešenia a vo všeobecnosti dať komplexný pohľad na problematiku s cieľom nájdenia nových účinnejších minimalizačných algoritmov. Počiatky skúmania v oblasti minimalizácie siahajú až do 50 rokov minulého storočia, dokonca existuje aj niekoľko skorších prác, napriek tomu je skúmanie stále aktuálne.

Vo všeobecnom modeli sa odhadujú zložitosti na množine všetkých boolovských funkcií o n premenných (ozn. B_n) a náhodný výber boolovskej funkcie závisí od parametra p_n. Ide o parameter, ktorý možno charakterizovať ako pravdepodobnosť, že ľubovoľný vrchol $\alpha \in \{0, 1\}^n$ patrí generovanej náhodnej boolovskej funkcii f, teda že $f(\alpha) = 1$. Cieľom tejto práce je nájsť asymptotický odhad zložitosti maximálnej iredundantnej DNF a počtu iredundantných DNF náhodnej boolovskej funkcie s daným počtom jednotiek. Boolovské funkcie s daným počtom jednotiek (ozn. F_m^n, prípadne len F_m) tvoria podmnožinu množiny všetkých boolovských funkcií B_n, kde pre $f \in F_m$ platí podmienka $|f^{-1}(1)| = m(n)$, teda práve $m(n)$ prvkov množiny $\{0, 1\}^n$ patrí do množiny identifikovanej funkciou f, čiže do N_f. Model náhodných boolovských funkcií, s ktorým pracujeme, zaviedli F. Mileto a G. Putzolu [5]. V ďalšom texte budeme často používať namiesto $m(n)$ len m, neznamená to však, že sa jedná o konštantu.

M. Škoviera riešil obdobné otázky pre iný model pravdepodobnosti [10], o ktorý sa v tejto práci opierame. Ďalej využívame výsledky dosiahnuté M. Kovalíkovou [4], ktoré nám slúžia ako pomocné tvrdenia.

Kapitola 2

Predbežné kroky

Definície a základné pojmy

Nech je daná abeceda premenných $\{x_1, ..., x_n\}$. Nech $D = \{0, 1\}$.

Nech $\bar{x}$ označuje negáciu *x*.

Nech $x^\sigma = x\sigma \vee \bar{x}\bar{\sigma}$.

Definícia: (elementárna konjunkcia, rád elementárnej konjunkcie)

Výraz $K = x_{i_1}^{\sigma_1} \wedge x_{i_2}^{\sigma_2} \wedge ... \wedge x_{i_r}^{\sigma_r}$, kde $i_j \neq i_k$ pre $j \neq k$, sa nazýva elementárna konjunkcia. Číslo *r* sa nazýva rád elementárnej konjunkcie. Definitoricky považujeme konštantu 1 za konjunkciu rádu 0.

Definícia: (disjunktívna normálna forma)

Výraz $\bigvee_{i=1}^{s} K_i$, kde $K_i \neq K_j$ pre $i \neq j$ a K_i pre $i = 1, ..., s$ je elementárna konjunkcia, sa nazýva disjunktívna normálna forma (DNF).

Zavedieme teraz formálne už spomínaný index jedn. $L(N)$ charakterizujúci zložitosť DNF. Od funkcionálu $L(N)$ vyžadujeme splnenie týchto štyroch axióm:

1. Axióma nezápornosti. Pre ľubovoľnú DNF $L(N) \geqslant 0$.
2. Axióma monotónnosti (vzhľadom na násobenie). Nech $N = N' \vee x_i^{\sigma_i} K'$. Potom $L(N) \geqslant L(N' \vee K')$.
3. Axióma vypuklosti (vzhľadom na sumáciu). Nech $N = N_1 \vee N_2$. Ak $N_1 \wedge N_2 \equiv 0$, tak platí $L(N) \geqslant L(N_1) + L(N_2)$.
4. Axióma invariantnosti (vzhľadom na izomorfizmus). Nech DNF N' bola získaná z DNF N premenovaním premenných (bez stotožnenia). Potom $L(N) = L(N')$.

V úvode už bolo spomenuté, že naším indexom jednoduchosti $L(N)$ bude počet elementárnych konjunkcií v danej disjunktívnej normálnej forme a minimálnu DNF vzhľadom na index jednoduchosti L budeme nazývať najkratšia DNF.

Teraz definujeme dva typy transformácií disjunktívnej normálnej formy. Nech N je ľubovoľná disjunktívna normálna forma, nech $N = N' \vee K$ a $N = N' \vee x_i^{\sigma_i} K'$, kde K je nejaká elementárna konjunkcia z N, N' je disjunktívna normálna forma vytvorená z ostatných konjunkcií nachádzajúcich sa v N, $x_i^{\sigma_i}$ je určitý činiteľ z K a K' je logický súčin zvyšných činiteľov z K.

Transformácia A je operácia vynechania elementárnej konjunkcie. Prechod od DNF N ku DNF N' sa nazýva transformácia, ktorá spočíva vo vynechaní elementárnej konjunkcie K. Táto transformácia je definovaná vtedy a len vtedy, keď $N = N'$.

Transformácia B je operácia vynechania činiteľa. Prechodom od DNF N ku DNF $N' \vee K'$ je transformácia, ktorá spočíva vo vynechaní činiteľa $x_i^{\sigma_i}$. Táto transformácia je definovaná vtedy a len vtedy, keď $N = N' \vee K'$.

Definícia: (iredundantná DNF)

Disjunktívna normálna forma, ktorú nemožno zjednodušiť pomocou transformácií A a B (teda nemožno tieto transformácie aplikovať) sa nazýva iredundantná DNF (ozn. ir DNF) vzhľadom na transformácie A a B.

Definícia: (boolovská funkcia)

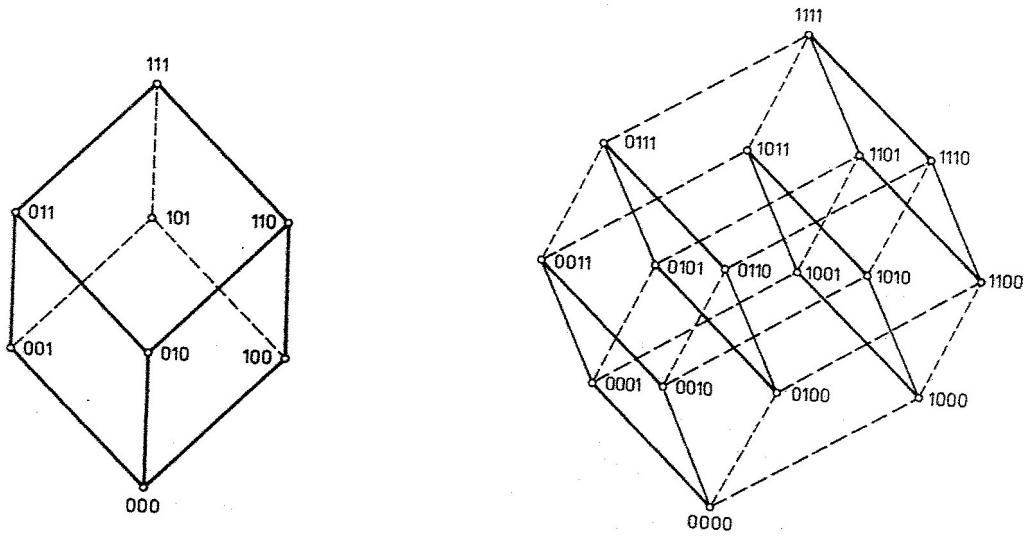
N-árna boolovská funkcia je ľubovoľné zobrazenie z množiny D^n do množiny D.

Definícia: (množina identifikovaná boolovskou funkciou a elementárnou konjunkciou)

Nech *f* je boolovská funkcia (*K* je konjunkcia). Potom

$$N_f = \{\alpha ; \alpha \in D \wedge f(\alpha) = 1\} \qquad \left(N_K = \{\alpha ; \alpha \in D \wedge K(\alpha) = 1\}\right).$$

Okrem algebraického prístupu je možné zvoliť i geometrický prístup. Kvôli názornosti budeme uprednostňovať práve geometrický prístup. Množinu všetkých binárnych *n*-tíc $(\alpha_1, \ldots, \alpha_n)$ považujeme za množinu (všetkých) vrcholov *n*-rozmernej jednotkovej kocky. Keďže žiadne iné body okrem vrcholov neuvažujeme, budeme množinu D^n nazývať *n*-rozmernou kockou a *n*-tice $(\alpha_1, \ldots, \alpha_n)$ vrcholy kocky. Dva vrcholy sú susedné, ak sa líšia v práve jednej súradnici. Potom zrejme n-rozmerná jednotková kocka má 2^n vrcholov a $n \cdot 2^{n-1}$ hrán.



Na obrázku je ukážka 3-rozmernej a 4-rozmernej jednotkovej kocky.

Definícia: (*n-r* rozmerná hrana)

Nech $\left(\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_r}\right)$ je pevne zvolená *r*-tica čísel z *D* taká, že $1 \leqslant i_1 < i_2 < \ldots < i_r \leqslant n.$ Množina všetkých vrcholov $(\alpha_1, \ldots, \alpha_n)$ kocky D^n takých, že $\alpha_{i_1} = \sigma_{i_1}, \alpha_{i_2} = \sigma_{i_2}, \ldots, \alpha_{i_r} = \sigma_{i_r}$ sa nazýva *n-r* rozmerná hrana.

Definícia: (interval, rád intervalu)

Množina N_K odpovedajúca konjunkcii $K = x_{i_1}^{\sigma_1} \wedge x_{i_2}^{\sigma_2} \wedge \ldots \wedge x_{i_r}^{\sigma_r},$ sa nazýva interval *r*-tého rádu. V *n*-rozmernom priestore je interval *r*-tého rádu taktiež *n-r* rozmerným intervalom (alebo aj intervalom dimenzie *n-r*).
Tiež je zrejmé, že *n-r* rozmerná hrana je zároveň interval *r*-tého rádu.

Definícia: (maximálny interval)

Nech *f* je *n*-árna boolovská funkcia, nech *K* je konjunkcia. Interval N_K obsiahnutý v N_f sa nazýva maximálny (vzhľadom na N_f), ak neexistuje interval $N_{K'}$ menšieho rádu ako N_K taký, že $N_K \subseteq N_{K'} \subseteq N_f$.

Definícia: (prostý implikant)

Konjunkcia *K*, odpovedajúca maximálnemu intervalu N_K množiny N_f, sa nazýva prostý implikant funkcie *f*.

Z definície ir DNF vyplýva, že všetky implikanty nachádzajúce sa v ir DNF sú prosté.

Definícia: (skrátená DNF)

DNF, ktorá je disjunkciou všetkých prostých implikantov funkcie *f*, sa nazýva skrátená disjunktívna normálna forma boolovskej funkcie *f*.

Kľúčová vec pre náš prístup je, že ľubovoľná boolovská funkcia *f* identifikuje podgraf N_f kocky D^n, rovnako ľubovoľný podgraf N_g kocky D^n identifikuje boolovskú funkciu *g*. Podobne pre ľubovoľný implikant *K* rádu *k* platí, že množina N_K tvorí (*n-k*) rozmernú podkocku kocky D^n a naopak pre ľubovoľnú podkocku existuje implikant *K* taký, ktorý ju cez N_K identifikuje. Zo zavedeného priradenia $f \Leftrightarrow N_f$ vypývajú aj ďalšie dôležité vlastnosti:

Ak $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \vee h(x_1, \ldots, x_n)$ tak:

1. $N_g \subseteq N_f, N_h \subseteq N_f$
2. $N_f = N_g \cup N_h$

Konkrétne, ak je funkcii $f(x_1, \ldots, x_n)$ priradená DNF *N*, kde $N = K_1 \vee \ldots \vee K_s$, tak potom $N_{K_i} \subseteq N_f$ pre $i = \{1, 2, \ldots, s\}$. Inak povedané, obraz konjunkcie K_i disjunktívnej normálnej formy funkcie *f*, je intervalom, nachádzajúcim sa vnútri množiny N_f a $N_f = N_{K_1} \cup N_{K_2} \cup \ldots \cup N_{K_s}$. Teda disjunktívnej normálnej forme funkcie *f* odpovedá pokrytie množiny N_f intervalmi $N_{K_1}, N_{K_2}, \ldots, N_{K_s}$. Platí aj opačné

tvrdenie, každému pokrytiu množiny N_f intervalmi, nachádzajúcimi sa vnútri množiny N_f, odpovedá DNF funkcie *f*.

Pre úplnosť doplníme ešte dve definície.

Definícia: (ireducibilné pokrytie)

Pokrytie množiny N_f, pozostávajúce z maximálnych hrán (intervalov) vzhľadom na N_f, sa nazýva ireducibilné, ak množina hrán, ktorá sa získa z pôvodnej množiny vynechaním ľubovoľnej hrany, nebude pokrytím N_f.

Definícia: (iredundantná DNF v geometrickom zmysle)

DNF, odpovedajúca ireducibilnému pokrytiu množiny N_f, sa nazýva iredundantná disjunktívna normálna forma v geometrickom zmysle.

Pojmy iredundantnej DNF vzhľadom na transformácie A a B a iredundantnej DNF v geometrickom zmysle sú ekvivalentné. Každá iredundantná disjunktívna normálna forma boolovskej funkcie *f* je prepojená s iredundantným pokrytím množiny N_f maximálnymi podkockami (intervalmi, hranami) a naopak, každé iredundantné pokrytie množiny N_f maximálnymi podkockami identifikuje iredundantnú DNF funkcie *f*. Preto budeme ďalej v práci používať len spojenie iredundantná DNF.

Pravdepodobnostné metódy

V práci budeme používať štandardné označenie strednej hodnoty $E(X)$ a disperzie $D(X)$ náhodnej premennej *X*. Využijeme aj dobre známy vzťah

$D(X)=E(X^2)-(E(X))^2$.

Tvrdenie (Markovova nerovnosť)

Nech $\xi \geqslant 0$ je náhodná premenná, nech $E(\xi)$ je jej stredná hodnota, nech $\varepsilon > 0$.

Potom $P(\xi \geqslant \varepsilon) \leqslant \frac{E(\xi)}{\varepsilon}$.

Tvrdenie (Čebyševova nerovnosť)

Nech $\xi \geqslant 0$ je náhodná premenná, nech $E(\xi)$ je jej stredná hodnota, $D(\xi)$ jej disperzia, nech $\varepsilon > 0$, potom $P(|\xi - E(\xi)| \geqslant \varepsilon) \leqslant \frac{D(\xi)}{\varepsilon^2}$.

Notácie

V práci budeme používať *O*-notáciu.

Nech *g*(*n*) je funkcia. Potom

$o(g(n)) = \{ f(n) ; (\forall c > 0)(\exists N_0 > 0)(\forall n \geqslant N_0)(0 \leqslant f(n) < c \cdot g(n)) \}$.

$$O(g(n)) = \{ f(n); (\exists c,\ N_0 > 0)(\forall n \geqslant N_0)(0 \leqslant f(n) \leqslant c \cdot g(n)) \}.$$

Definujme klesajúcu mocninu: $(a)^{\underline{k}} = a \cdot (a-1) \cdot \ldots \cdot (a-k+1)$, kde $k \in \mathbb{N}$.

Formula 1

Nech $k \leqslant b \leqslant a$. Potom $\dfrac{\binom{a-k}{b-k}}{\binom{a}{b}} = \dfrac{(b)^{\underline{k}}}{(a)^{\underline{k}}} \leqslant \left(\dfrac{b}{a}\right)^k$.

Naviac keď $k = o(a^{1/2})$ a $k = o(b^{1/2})$ platí vzťah $\dfrac{\binom{a-k}{b-k}}{\binom{a}{b}} \sim \left(\dfrac{b}{a}\right)^k$.

V práci využijeme okrem iných aj nasledujúce zjednodušenia a vzťahy:

Namiesto $log_2(x)$ budeme písať len $lg(x)$.

Nech $a \in \mathbb{N}$, $b \in \mathbb{N}$, $b \geqslant a$. Potom $\binom{a}{b} = 0$.

Nech symbol $\lfloor x \rfloor$ (dolná celá časť) označuje najväčšie prirodzené číslo menšie alebo rovné x. Symbol $\lceil x \rceil$ definujeme $\lceil x \rceil = -\lfloor -x \rfloor$ (horná celá časť). Zrejme ide o najmenšie prirodzené číslo väčšie alebo rovné x.

Formula 2

Nech (X_n, φ_n, Q_n) je postupnosť pravdepodobnostných priestorov. Nech

$Y_n, Z_n \in \varphi_n$ sú také udalosti, že $\lim_{n\to\infty} Q_n(Y_n) = 1 = \lim_{n\to\infty} Q_n(Z_n)$, nech $A_n \in \varphi_n$.

Potom

i) $\lim_{n\to\infty} Q_n(Y_n \cap Z_n) = 1$

ii) Ak $\lim_{n\to\infty} Q_n(A_n | Y_n) = 1$, tak $\lim_{n\to\infty} Q_n(A_n) = 1$.

Formula 3

Nech $n \geqslant k \geqslant 1$, potom

i) $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} \geqslant \frac{n^k}{k^k} \geqslant \left(\frac{n}{k}\right)^k$

ii) $\binom{n}{k} = \frac{n^{\underline{k}}}{k!} \leqslant \frac{n^k}{k!} \leqslant \left(\frac{e \cdot n}{k}\right)^k$, kde e je Eulerovo číslo.

Trieda F_m

V práci sa zaoberáme triedou boolovských funkcií F_m. Ide o podmnožinu množiny všetkých boolovských funkcií B_n, s predpisom $F_m = \{f \in B_n ; |N_f| = m\}$. Táto

podmnožina obsahuje práve $\binom{2^n}{m}$ prvkov (funkcií), a kedže predpokladáme rovnocennosť v zmysle pravdepodobnosti výberu, každá funkcia má pravdepodobnosť výberu práve $P_0(\{f\}) = \binom{2^n}{m}^{-1}$. Tiež platí, že $P_0(A) = \sum_{f \in A} P_0(\{f\})$.

Pravdepodobnostné priestory

Základný pravdepodobnostný priestor tejto práce je priestor (F_m, P_0). Limity a asymptoty uvažujeme len pre *n* idúce do nekonečnu. Niektoré tvrdenia neplatia, pokiaľ *n* nie je dostatočne veľké. Aby sme sa vyhli častému opakovaniu v ďalšom texte, zmieňujeme sa o tom tu.

Nech *V* je nejaká vlastnosť boolovských funkcií. Hovoríme, že náhodná boolovská funkcia má vlastnosť *V* práve vtedy, keď

$\lim_{n\to\infty} P_0\left(\left\{f \in F_m^n ; f \text{ má vlastnosť } V\right\}\right) = 1$. V takom prípade budeme hovoriť, že náhodná boolovská funkcia (triedy F_m) spĺňa danú vlastnosť skoro isto.

Podobne ako vo všeobecnom modeli, aj v našom modeli definujeme pravdepodobnosť p_n, že ľubovoľný vrchol patrí do N_f. Pôjde o ohraničenie podielu

$\binom{2^n-1}{m(n)-1}\cdot\binom{2^n}{m(n)}^{-1}=\frac{m(n)}{2^n}$. Je rozumné predpokladať, že postupnosť $\left(\frac{m}{2^n}\right)_{n=1}^{\infty}$ konverguje k nejakému $p\in(0,1)$. V krajných prípadoch budeme musieť dať obmedzenia na rast funkcií $\frac{1}{p_n}=\binom{2^n}{m(n)}$ a $\frac{1}{(1-p_n)}=\binom{2^n}{2^n-m(n)}$.

Okrem pravdepodobnostného priestoru (F_m, P_0) budeme pracovať aj v iných pravdepodobnostných priestoroch. Budú zohrávať len vedľajšiu rolu, no pomôžu nám získať výsledky súvisiace s priestorom (F_m, P_0).

Kapitola 3

Cieľ práce

Ešte predtým ako začneme so samotnými výpočtami, presnejšie popíšeme cieľ tejto práce a už dosiahnuté výsledky, ktoré preberáme z iných prác.

Ako pomocné tvrdenia nám budú slúžiť výsledky, ktoré dosiahla M. Kovalíková vo svojej diplomovej práci [4]. Preberané výsledky zhrnieme do tvrednia 0.

Tvrdenie 0

Nech $i_{n,k}$ označuje náhodnú premennú na (F_m, P_0) takú, že $i_{n,k}(f)$ je rovné počtu k-roznerných intervalov funkcie $f \in F_m$.

i) Potom $E i_{n,k} = \binom{n}{k} \cdot 2^{n-k} \cdot \binom{2^n - 2^k}{m - 2^k} \cdot \binom{2^n}{m}^{-1}$. (0. i)

Nech $\left(\frac{2^n}{m}\right)=o(n)$ a $\left(\frac{2^n}{2^n-m}\right)=o(n)$. S pravdepodobnosťou idúcou k 1 (pre $n\to\infty$) platí:

ii) Náhodná boolovská funkcia neobsahuje intervaly dimenzie väčšej ako

$$\mu=\left\lfloor lg(n)-lg\,lg\left(\frac{2^n}{m}\right)\right\rfloor+1. \qquad (0.\text{ ii})$$

iii) Dĺžka skrátenej DNF náhodnej boolovskej funkcie $s(f)$ spĺňa nerovnosť

$$n^{(1-\varepsilon_1(n))lg\,log_{\frac{2^n}{m}}(n)}\cdot 2^n \leqslant s(f) \leqslant n^{(1+\varepsilon_2(n))lg\,log_{\frac{2^n}{m}}(n)}\cdot 2^n, \qquad (0.\text{ iii})$$

kde $\varepsilon_1\to 0$, $\varepsilon_2\to 0$. Ak $\left(\frac{m}{2^n}\right)\to p\in(0,1)$, potom $\varepsilon_1(n),\ \varepsilon_2(n)=O\left(\frac{1}{lg\,log_{\frac{2^n}{m}}n}\right)$.

A tak dostávame $lg\,s(f)\sim n+(lg\,n)\cdot lg\,log_{\frac{2^n}{m}}n$.

iv) Nech $I_{n,k}(f)$ je počet k-rozmerných maximálnych intervalov funkcie f, nech

$$\lambda_1=lg\,log_{\frac{2^n}{m}}n-1=lg\,lg(n)-lg\,lg\left(\frac{2^n}{m}\right)-1, \qquad \lambda_2=lg\,log_{\frac{2^n}{m}}n+lg\,lg\,log_{\frac{2^n}{m}}n+\varepsilon,\ \varepsilon>0,$$

nech $I^-_{n,\lambda_1}=\sum_{k<\lambda_1} I_{n,k}$ a $I^+_{n,\lambda_2}=\sum_{k>\lambda_2} I_{n,k}$. Potom $I^-_{n,\lambda_1},\ I^+_{n,\lambda_2}=o(2^n)$. (0. iv)

Dôkazy dvoch nasledujúcich tvrdení sú cieľom tejto diplomovej práce.

Tvrdenie 1

Nech $l(f)$ označuje maximálnu dĺžku (počet implikantov) iredundantnej DNF náhodnej boolovskej funkcie. Potom s pravdepodobnosťou idúcou k 1 (pre $n \to \infty$) platí, že $m(n) \cdot (1 - \varepsilon_3(n)) \leqslant l(f) \leqslant m(n)$, kde $\varepsilon_3(n) \to 0$. Teda $l(f) \sim m(n)$.

Naviac keď $\lim_{n\to\infty} \left(\frac{m}{2^n} \right) = p \in (0, 1)$, tak $\varepsilon_3(n) = O\left(\frac{1}{lg(n) \cdot lg\, lg(n)} \right)$.

Tvrdenie 2

S pravdepodobnosťou idúcou k 1 (pre $n \to \infty$) počet iredundantných DNF $\tau(f)$ náhodnej boolovskej funkcie $f \in F_m$ spĺňa nerovnosť

$2^{m \cdot lg(n) \cdot lg\, log_{\frac{2^n}{m}} n \cdot (1 - \varepsilon_4(n))} \leqslant \tau(f) \leqslant 2^{m \cdot lg(n) \cdot lg\, log_{\frac{2^n}{m}} n \cdot (1 + \varepsilon_5(n))}$, kde $\varepsilon_4(n), \varepsilon_5(n) \to 0$. Teda $lg\, \tau(f) \sim m \cdot lg(n) \cdot lg\, log_{\frac{2^n}{m}} n$. Ak naviac $\lim_{n\to\infty} \left(\frac{m}{2^n} \right) = p \in (0, 1)$, tak $\varepsilon_4(n), \varepsilon_5(n) = O\left(\frac{1}{lg\, log_{\frac{2^m}{n}} n} \right)$.

Kapitola 4

Intervaly

Ako bolo spomenuté v kapitole 2, kľúčovú úlohu v tejto práci zohráva pravdepodobnostný priestor (F_m, P_0), pričom pre každú $f \in F_m$ platí $P_0(\{f\}) = \binom{2^n}{m}^{-1}$. Definujme pravdepodobnostný priestor (B_n, P_0'), kde pre $f \in B_n$ platí $P_0'(\{f\}) = p_n^{|N_f|} \cdot (1-p_n)^{2^n - |N_f|}$, pričom $p_n = m \cdot 2^{-n}$.

Nech $F_m \times B_n$, kde $\times$ predstavuje Kartézsky (Karteziánsky) súčin, je množina dvojíc boolovských fukncií, na ktorej definujeme pravdepodobnosť $P_1 = P_0 \times P_0'$. Pre $(f_1, f_2) \in F_m \times B_n$ potom platí

$P_1(\{f_1, f_2\}) = P_0(\{f_1\}) \cdot P_0'(\{f_2\})$. Ďalej definujme množinu C_n ako podmnožinu priestoru $F_m \times B_n$, pričom C_n obsahuje iba také dvojice boolovských funkcií (f_1, f_2), pre ktoré platí $N_{f_2} \subseteq N_{f_1}$ (teda $f_2 \leqslant f_1$). Na množine C_n definujeme podmienenú pravdepodobnosť $P_2 = P_1(\cdot \mid C_n)$ a tak pre $A \subseteq C_n$ $\quad P_2(A) = \dfrac{P_1(A)}{P_1(C_n)}$.

Nech $\alpha \in D^n$, definujme množinu C_n^α ako podmnožinu množiny C_n, pre ktorú platí $\alpha \in N_{f_1}$. Formálne $C_n^\alpha = \{(f_1, f_2) \in C_n ; f_1(\alpha) = 1\}$. Zavedieme pravdepodobnosť P_3, kde $P_3 = P_2(\cdot \mid C_n^\alpha)$. Dostávame $P_3(A) = \dfrac{P_2(A)}{P_2(C_n^\alpha)} = \dfrac{P_1(A)}{P_1(C_n^\alpha)}$.

Tvrdenie 3

i) $P_1(C_n) = \left(\dfrac{2^n - m}{2^n}\right)^{2^n - m}$

ii) $P_1(C_n^\alpha) = \dfrac{m}{2^n}\left(\dfrac{2^n - m}{2^n}\right)^{2^n - m}$

iii) $P_2(C_n^\alpha) = \dfrac{m}{2^n}$

Dôkaz:

i) $P_1(C_n) = \sum_{f \in F_m} \sum_{\substack{g \in B_n \\ g \leqslant f}} P_1(\{(f, g)\}) = \sum_{f \in F_m} P_0(\{f\}) \sum_{\substack{g \in B_n \\ g \leqslant f}} P_0'(\{g\}) =$

$$= \sum_{i=0}^{m} \binom{m}{i} \left(\frac{m}{2^n}\right)^i \left(1 - \frac{m}{2^n}\right)^{2^n - i} = \left(\frac{2^n - m}{2^n}\right)^{2^n} \sum_{i=0}^{m} \binom{m}{i} \left(\frac{m}{2^n - m}\right)^i = \left(\frac{2^n - m}{2^n}\right)^{2^n - m}$$

ii) $P_1\left(C_n^\alpha\right) = \sum_{\substack{f \in F_m \\ f(\alpha)=1}} \sum_{\substack{g \in B_n \\ g \leqslant f}} P_1\left(\{(f, g)\}\right) =$

$$= \frac{m}{2^n} \sum_{i=0}^{m} \binom{m}{i} \left(\frac{m}{2^n}\right)^i \left(1 - \frac{m}{2^n}\right)^{2^n - i} = \left(\frac{m}{2^n}\right) \left(\frac{2^n - m}{2^n}\right)^{2^n - m}$$

iii) $P_2\left(C_n^\alpha\right) = \frac{P_1\left(C_n^\alpha\right)}{P_1\left(C_n\right)}$ z čoho dostávame požadované tvrdenie.

Sapozhenko vo svojej práci [7] aplikoval myšlienku uvažovať boolovskú funkciu $f \in B_n$ spolu s „význačnou“ podmnožinou $A_n \subseteq N_f$ a dokázal tak tvrdenie 1 a tvrdenie 2 pre prípad klasického modelu, keď $p_n = 1/2$. M. Škoviera aplikoval podobnú myšlienku a dokázal tvrdenia pre všeobecný model [10], t.j. pre $p_n \in (0, 1)$. My zrealizujeme podobný postup a dokážeme tak tvrdenia 1 a 2 pre triedu boolovských funkcií F_m. Myšlienka $A_n \subseteq N_f$ je zachytená v konštrukcií množiny C_n. Základ takéhoto postupu je vo využití algoritmu konštrukcie iredundantnej DNF uplatneného v dôkaze tvdrenia 1. Všetky tvrdenia v tejto kapitole sú iba pomocné tvrdenia, ich výsledky nám však umožnia dokázať dve hlavné tvrdenia tejto práce vyslovené v kapitole 3.

Začneme so skúmaním maximálnych intervalov obsahujúcich fixovaný vrchol $\alpha \in D^n$. Definujeme náhodnú premennú $M_{n,k}^\alpha(f)$, na $\left(C_n^\alpha, P_3\right)$ nasledovným

spôsobom:

Nech $f=(f_1, f_2)\in C_n^\alpha$. Potom $M_{n,k}^\alpha(f)$ je počet *k*-rozmerných maximálnych intervalov $K\subseteq N_{f_1}$ takých, že $\alpha\in K$ a $K-\{\alpha\}\subseteq N_{f_2}$. Pre každý *k*-rozmerný interval $K\subseteq D^n$, $\alpha\in K$ definujeme indikátor ξ_K na (C_n^α, P_3)

$\xi_K(f)=\begin{cases}1 & K \text{ je max. int. } f_1 \text{ a } K-\{\alpha\}\subseteq N_{f_2}\\ 0 & \text{inak}\end{cases}$. Interval *K*, pre ktorý $\xi_K(f_1, f_2)=1$ sa nazýva interval vnorený do N_{f_2}. Zrejme $M_{n,k}^\alpha(f)=\sum_K \xi_K$, kde suma ide cez všetky *k*-rozmerné intervaly *K* obsahujúce vrchol α.

Tvrdenie 4

$$\left[\binom{2^n-2^k}{m-2^k}-(n-k)\binom{2^n-2^{k+1}}{m-2^{k+1}}\right]\binom{2^n}{m}^{-1}\binom{n}{k}\left(\frac{m}{2^n}\right)^{2^k-2}\leqslant EM_{n,k}^\alpha \text{ a}$$

$$EM_{n,k}^\alpha\leqslant\binom{2^n-2^k}{m-2^k}\binom{2^n}{m}^{-1}\binom{n}{k}\left(\frac{m}{2^n}\right)^{2^k-2}.$$

Dôkaz:

$$EM_{n,k}^\alpha=\sum_{f\in C_n^\alpha}P_3(\{f\})M_{n,k}^\alpha(f)=\sum_{f\in C_n^\alpha}P_3(\{f\})\sum_K\xi_K(f)=\sum_K\sum_{f\in C_n^\alpha}P_3(\{f\})\xi_K(f).$$

Je zrejmé, že hodnota výrazu nezáleží na voľbe vrchola α, preto bez ujmy na všeobecnosti, nech $\alpha=(1, ..., 1)$. Rovnako môžeme bez ujmy na všeobecnosti

vybrať jeden konkrétny *k*-rozmerný interval, nech teda $K' = N_{x_1 \wedge x_2 \wedge \ldots x_{n-k}}$. Keďže existuje práve $\binom{n}{n-k} = \binom{n}{k}$ *k*-rozmerných intervalov dostávame, že

$EM^{\alpha}_{n,k} = \binom{n}{k} \sum_{f \in C^{\alpha}_n} P_3(\{f\}) \xi_{K'}(f) = \binom{n}{k} P_3\left(\{f; f \in C^{\alpha}_{n,k} \wedge \xi_{K'}(f) = 1\}\right)$. Nech

$A_n = \{f; f \in C^{\alpha}_n \wedge \xi_{K'}(f) = 1\}$, nech a_i je počet párov $(f_1, f_2) \in A_n$, takých, že $|N_{f_2}| = i$. Stačí vypočítať $P_1(A_n)$, keďže $P_3(A_n) = P_1(A_n) \cdot P_1^{-1}(C^{\alpha}_n)$ Pritom

$$P_1(A_n) = \sum_{i=0}^{m} a_i \cdot \binom{2^n}{m}^{-1} \left(\frac{m}{2^n}\right)^i \left(\frac{2^n - m}{2^n}\right)^{2^n - i}. \qquad (4.1)$$

Potrebujeme zistiť hodnotu a_i. Nech φ je počet všetkých párov $(f_1, f_2) \in C^{\alpha}_n$ takých, že $K' \subseteq N_{f_1}$, $K' - \{\alpha\} \subseteq N_{f_2}$ a $|N_{f_2}| = i$. Maximalitu zabezpečíme pomocou princípu zapojenia a vypojenia. Nech γ_i je vlastnosť, že interval $N_{x_1 \wedge .. \wedge x_{i-1} \wedge x_{i+1} \wedge .. \wedge x_{n-k}}$ je obsiahnutý v N_{f_1}. Nech γ_i' je negácia γ_i. Potom chceme vypočítať hodnotu $\varphi(\gamma_1', .., \gamma_{n-k}')$. Teda počet párov, ktoré obsahujú v N_{f_1} interval *K'*, ale neobsahujú v N_{f_1} žiadny interval rádu o 1 menšieho (teda rádu *n-k-1*). Pomocou princípu zapojenia a vypojenia dostávame

$$\varphi(\gamma_1', \ldots, \gamma_{n-k}') = \sum_{j=0}^{n-k} (-1)^j \left(\sum_{i_1 < .. < i_j} \varphi(\gamma_{i_1}, .., \gamma_{i_j}) \right) = \sum_{j=0}^{n-k} (-1)^j \binom{n-k}{j} \varphi(\gamma_{1,}, .., \gamma_j).$$

Využívame fakt, že rozhoduje len počet vlastností γ_i vo φ a tak môžeme bez ujmy

na všeobecnosti vybrať prvých *j*. Naviac platí

$\varphi(\gamma_1, ..., \gamma_j) = \binom{2^n-(j+1)2^k}{m-(j+1)2^k}\binom{m-(2^k-1)}{i-(2^k-1)}$. Poslednú rovnosť získame z toho, že

$\varphi(\gamma_1, ..., \gamma_j)$ je počet párov $(f_1, f_2) \in C_n^\alpha$, ktoré v N_{f_1} obsahujú *K′*. Teda majú definovaných 2^k vrcholov. Takisto obsahujú *j* (*k+1*)-rozmerných intervalov, avšak príspevok každého takéhoto intervalu je len 2^k, pretože 2^k vrcholov majú spoločných s *K′*. Taktiež si treba uvedomiť fakt, že množiny týchto 2^k prispievajúcich vrcholov sú po dvoch disjunktné. Aplikovaním Bonferroniho nerovností dostávame

$$\left[\binom{2^n-2^k}{m-2^k}-(n-k)\binom{2^n-2^{k+1}}{m-2^{k+1}}\right]\binom{m-(2^k-1)}{i-(2^k-1)} \leqslant a_i \leqslant \binom{2^n-2^k}{m-2^k}\binom{m-(2^k-1)}{i-(2^k-1)} \qquad (4.2)$$

Upravujme najprv horný odhad $EM_{n,k}^\alpha$, zo (4.1) máme

$P_1(A_n) = \sum_{i=0}^{m} a_i \cdot \binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^i\left(\frac{2^n-m}{2^n}\right)^{2^n-i}$ a pomocou (4.2) dostávame

$$\leqslant \sum_{i=0}^{m}\binom{2^n-2^k}{m-2^k}\binom{m-(2^k-1)}{i-(2^k-1)}\cdot\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^i\left(\frac{2^n-m}{2^n}\right)^{2^n-i} =$$

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

$$= \binom{2^n-2^k}{m-2^k}\binom{2^n}{m}^{-1}\left(\frac{2^n-m}{2^n}\right)^{2^n}\left(\frac{m}{2^n}\right)^{2^k-1}\left(\frac{2^n}{2^n-m}\right)^m =$$

$$= \binom{2^n-2^k}{m-2^k}\binom{2^n}{m}^{-1}\left(\frac{2^n-m}{2^n}\right)^{2^n-m}\left(\frac{m}{2^n}\right)^{2^k-1} \leqslant \left(\frac{2^n-m}{2^n}\right)^{2^n-m}\left(\frac{m}{2^n}\right)^{2^{k+1}-1}.$$

Podobne pre dolný odhad $EM_{n,k}^\alpha$ dostaneme

$P_1(A_n) \geqslant \left[\binom{2^n - 2^k}{m - 2^k} - (n-k)\binom{2^n - 2^{k+1}}{m - 2^{k+1}} \right] \binom{2^n}{m}^{-1} \left(\frac{2^n - m}{2^n} \right)^{2^n - m} \left(\frac{m}{2^n} \right)^{2^k - 1}$. Využitím $EM_{n,k}^{\alpha} = \binom{n}{k} P_3(A_n) = \binom{n}{k} \frac{P_1(A_n)}{P_1(C_n^{\alpha})}$ v oboch odhadoch dostávame požadované tvrdenie.

Tvrdenie 5

Nech $\left\lceil 1 + lg\, lg\, n - lg\, lg \frac{2^n}{m} \right\rceil \leqslant k$, potom $(n-k)\binom{2^n - 2^{k+1}}{m - 2^{k+1}}\binom{2^n - 2^k}{m - 2^k}^{-1} \leqslant \frac{1}{n}$ a

$$\binom{2^n - 2^k}{m - 2^k}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^k - 2}\binom{n}{k}\left(1 - \frac{1}{n}\right) \leqslant EM_{n,k}^{\alpha}.$$

Dôkaz:

Aplikovaním Formuly 1 a z následných úprav dostávame

$$(n-k)\binom{2^n - 2^{k+1}}{m - 2^{k+1}}\binom{2^n - 2^k}{m - 2^k}^{-1} = (n-k)\binom{2^n - 2^k - 2^k}{m - 2^k - 2^k}\binom{2^n - 2^k}{m - 2^k}^{-1} \leqslant (n-k)\frac{\left(m - 2^k\right)^{2^k}}{\left(2^n - 2^k\right)^{2^k}}$$

$$= (n-k)\left(\frac{m - 2^k}{2^n - 2^k}\right)^{2^k} \leqslant n \cdot \left(\frac{m}{2^n}\right)^{2^k}.$$

Nech $k \geqslant 1 + lg\, lg\, n - lg\, lg \frac{2^n}{m}$. Keďže k je prirodzené číslo, je táto podmienka ekvivalentná s podmienkou $k \geqslant \left\lceil 1 + lg\, lg\, n - lg\, lg \frac{2^n}{m} \right\rceil$. Využitím predpokladu

dostávame $n\cdot\left(\frac{m}{2^n}\right)^{2^k}\leqslant n\cdot\left(\frac{m}{2^n}\right)^{2^{1+lg\,lg\,n-lg\,lg\frac{2^n}{m}}}=n\cdot\left(\frac{m}{2^n}\right)^{2\cdot\frac{lg\,n}{lg\frac{2^n}{m}}}=n\cdot\left(\frac{m}{2^n}\right)^{lg_{\frac{m}{2^n}}n^{-2}}=n^{-1}$,

priamym dôsledkom čoho je $\frac{\binom{2^n-2^k}{m-2^k}}{\binom{2^n}{m}}\left(\frac{2^n}{m}\right)^{2^k-2}\binom{n}{k}\left(1-\frac{1}{n}\right)\leqslant EM^{\alpha}_{n,k}$.

Označme $\kappa=\left\lceil\, 1+lg\,lg\,n-lg\,lg\,\frac{2^n}{m}\,\right\rceil$.

Teraz zhora odhadneme $E\left(M^{\alpha}_{n,\kappa}\right)^2$.

Tvrdenie 6

$$E\left(M^{\alpha}_{n,\kappa}\right)^2\leqslant\frac{\binom{2^n-2^\kappa}{m-2^\kappa}^2}{\binom{2^n}{m}^2}\left(\frac{m}{2^n}\right)^{2\cdot\left(2^\kappa-2\right)}\binom{n}{\kappa}^2\left[1+O\left(\frac{2^{2n}}{m^2}\frac{\kappa^3}{n}\right)\right].$$

<u>Dôkaz:</u>

$$E\left(M^{\alpha}_{n,\kappa}\right)^2=\sum_{f\in C^{\alpha}_n}P_3\left(\{f\}\right)\left(M^{\alpha}_{n,\kappa}(f)\right)^2=\sum_{f\in C^{\alpha}_n}P_3\left(\{f\}\right)\left(\sum_I\xi_I(f)\right)^2=$$

$$=\sum_{f\in C^{\alpha}_n}P_3\left(\{f\}\right)\left(\sum_{I,J}\xi_I(f)\xi_J(f)\right).$$ Definujme indikátor

$\xi'_I(f)=\begin{cases}1 & I\ je\ interval\ f_1\ a\ I-\{\alpha\}\subseteq N_{f_2}\\ 0 & inak\end{cases}$. Potom platí, že

$$E\left(M^{\alpha}_{n,\kappa}\right)^2\leqslant\sum_{f\in C^{\alpha}_n}P_3\left(\{f\}\right)\left(\sum_{(I,J)}\xi'_I(f)\xi'_J(f)\right)=\sum_{(I,J)}\sum_{f\in C^{\alpha}_n}P_3\left(\{f\}\right)\xi'_I(f)\xi'_J(f).\qquad(6.1)$$

Prienik intervalov *I* a *J* je podkocka kocky D^n, ktorá obsahuje práve $2^{\kappa+1}-2^j$ vrcholov, kde *j* je dimenzia priestoru $I \cap J$. Intervaly *I* a *J* nie sú disjunktné, kedže oba obsahujú vrchol α. Je zrejmé, že hodnota výrazu nie je ovplyvnená konkrétnou voľbou intervalov *I* a *J*, závisí len od dimenzie priestoru $I \cap J$. Pritom počet dvojíc intervalov (*I*, *J*) takých, že $dim(I \cap J) = j$ je presne $\binom{n}{j}\binom{n-j}{n-\kappa}\binom{n-\kappa}{\kappa-j}$. A tak zo (6.1) dostávame $E\left(M_{n,\kappa}^{\alpha}\right)^2 \leqslant \sum_{j=0}^{\kappa}\binom{n}{j}\binom{n-j}{n-\kappa}\binom{n-\kappa}{\kappa-j}\sum_{f\in C_n^{\alpha}} P_3(\{f\})\xi'_{I_j}(f)\cdot\xi'_{J_j}(f)$,

kde pre fixovanú dvojicu intervalov (I_j, J_j) platí $dim(I_j \cap J_j) = j$. Definujme množiny

$G_j = \left\{f; f\in C_n^{\alpha} \wedge \xi'_{I_j}(f)\cdot\xi'_{J_j}(f) = 1\right\}$ pre $0 \leqslant j \leqslant \kappa$. Potom

$$E\left(M_{n,\kappa}^{\alpha}\right)^2 \leqslant \sum_{j=0}^{\kappa}\binom{n}{j}\binom{n-j}{n-\kappa}\binom{n-\kappa}{\kappa-j}P_3(G_j) = \binom{n}{\kappa}\sum_{j=0}^{\kappa}\binom{\kappa}{j}\binom{n-\kappa}{\kappa-j}P_3(G_j). \qquad (6.2)$$

Podobne ako pri strednej hodnote, stačí nám vypočítať $P_1(G_j)$.

Nech $b_{j,t}$ je počet párov $(f_1, f_2)\in C_n^{\alpha}$ takých, že

$I_j \subseteq N_{f_1}$, $J_j \subseteq N_{f_1}$, $I_j - \alpha \subseteq N_{f_2}$, $J_j - \alpha \subseteq N_{f_2}$, $|N_{f_2}| = t$. Potom zrejme

$$b_{j,t} = \binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{m-2^{\kappa+1}+2^j+1}{t-2^{\kappa+1}+2^j+1} \qquad (6.3)$$

Keďže $P_1(G_j) = \sum_{t=0}^{m} b_{j,t}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^t\left(\frac{2^n-m}{2^n}\right)^{2^n-t}$, pomocou (6.3) dostávame

$$P_1(G_j) = \sum_{t=0}^{m}\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{m-2^{\kappa+1}+2^j+1}{t-2^{\kappa+1}+2^j+1}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^t\left(\frac{2^n-m}{2^n}\right)^{2^n-t} =$$

$$\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n}{m}^{-1}\left(\frac{2^n-m}{2^n}\right)^{2^n}\sum_{t=0}^{m}\binom{m-2^{\kappa+1}+2^j+1}{t-2^{\kappa+1}+2^j+1}\left(\frac{m}{2^n-m}\right)^t=$$

$$\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n}{m}^{-1}\left(\frac{2^n-m}{2^n}\right)^{2^n-m}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-2^j-1}.$$ Odtiaľ

$$P_3\left(G_j\right)=\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-2^j-2},$$ z čoho dostávame, že

$$E\left(M_{n,\kappa}^{\alpha}\right)^2\leqslant\binom{n}{\kappa}\sum_{j=0}^{\kappa}\binom{\kappa}{j}\binom{n-\kappa}{\kappa-j}\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-2^j-2}. \qquad (6.4)$$

Pozornému čitateľovi určite neuniklo, že sme doteraz nijako nevyužili hodnotu premennej κ, mohli sme preto v predchádzajúcich vzťahoch písať namiesto κ ľubovoľné $0\leqslant k\leqslant n$. V tejto chvíli však upozorňujeme na fakt, že

$$\kappa=\left\lceil 1+lg\,lg\,n-lg\,lg\,\frac{2^n}{m}\right\rceil.$$

Nech c_j je rovné j-tému prvku sumy zo vzťahu (6.4), teda pre $j\in\{0,1,\ldots,\kappa\}$

$$c_j=\binom{\kappa}{j}\binom{n-\kappa}{\kappa-j}\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-2^j-2}. \qquad (6.5)$$

Ukážeme, že pre $j>1$ platí $c_1\geqslant c_j$, teda že $\lim_{n\to\infty}\frac{c_j}{c_1}=0.$ (6.6)

Nech $\upsilon=\dfrac{lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^\kappa}{m-2^\kappa}\right)}{lg\,\frac{2^n}{m}}$. Náš výpočet rozdelíme do dvoch vetiev.

1. prípad: $4\upsilon+2 \leqslant j$.

Nech $j \in \{0, 1, \ldots, \kappa-1\}$ Pre podiel $\frac{c_j}{c_1}$ potom platí

$$\frac{c_j}{c_1} = \frac{\kappa^j (n-\kappa)^{\kappa-j} (\kappa-1)!}{j!(\kappa-j)!\,\kappa (n-\kappa)^{\kappa-1}} \left(\frac{2^n}{m}\right)^{2^j-2} \binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j} \binom{2^n-2^{\kappa+1}+2}{m-2^{\kappa+1}+2}^{-1} \leqslant$$

$$\leqslant \frac{1}{\kappa-j}\binom{\kappa-1}{j} \frac{(\kappa-1)^{j-1}}{(n-2\kappa+j)^{j-1}} \left(\frac{2^n}{m}\right)^{2^j-2} \binom{2^n-2^{\kappa}}{m-2^{\kappa}} \binom{2^n-2^{\kappa+1}+2}{m-2^{\kappa+1}+2}^{-1} =$$

$$= \frac{1}{\kappa-j}\binom{\kappa-1}{j} \frac{(\kappa-1)^{j-1}}{(n-2\kappa+j)^{j-1}} \left(\frac{2^n}{m}\right)^{2^j-2} \frac{(2^n-2^{\kappa})^{2^{\kappa}-2}}{(m-2^{\kappa})^{2^{\kappa}-2}} \leqslant$$

$$\leqslant \frac{(\kappa-1)^{2j}}{(n-2\kappa+j)^{j-1}} \left(\frac{2^n}{m}\right)^{2^{\kappa}-2} \left(\frac{2^n-2^{\kappa}}{m-2^{\kappa}}\right)^{2^{\kappa}-2} \leqslant \frac{(\kappa-1)^{2j}}{(n-2\kappa+j)^{j-1}} \left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa}}{m-2^{\kappa}}\right)^{2^{\kappa}} =$$

$$= 2^{2\cdot j\cdot lg(\kappa-1)+2^{\kappa}\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa}}{m-2^{\kappa}}\right)-(j-1)\cdot lg(n-2\kappa+j)} \leqslant 2^{2\cdot\kappa\cdot lg\,\kappa+2^{\kappa}\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa}}{m-2^{\kappa}}\right)-(j-1)\cdot lg\left(n\cdot\left(1-\frac{2\kappa}{n}\right)\right)} \leqslant$$

Využijeme, že $\kappa \leqslant 2+lg\,lg\,n-lg\,lg\,\frac{2^n}{m}$. Potom dostávame

$$\leqslant 2^{2\cdot\kappa\cdot lg\,\kappa+2^{\kappa}\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa}}{m-2^{\kappa}}\right)-(j-1)\cdot\left(lg\,n+lg\left(1-\frac{2\kappa}{n}\right)\right)} \leqslant 2^{2\cdot\kappa\cdot lg\,\kappa+4(lg\,n)\,lg^{-1}\frac{2^n}{m}\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa}}{m-2^{\kappa}}\right)-(j-1)\cdot\left(lg\,n+lg\left(1-\frac{2\kappa}{n}\right)\right)}$$

$$\leqslant 2^{2\cdot\kappa\cdot lg\,\kappa+(4\upsilon-j+1)\cdot lg\,n-(j-1)\cdot lg\left(1-\frac{2\kappa}{n}\right)} \leqslant 2^{2\cdot\kappa\cdot lg\,\kappa-lg\,n-\kappa\cdot lg\left(1-\frac{2\kappa}{n}\right)} \to 0.$$

Pre podiel $\frac{c_k}{c_1}$ to platí tiež, podobným postupom dostávame

$$\frac{c_k}{c_1} \leqslant \frac{(\kappa-1)!}{\kappa(n-\kappa)^{\kappa-1}} \left(\frac{2^n}{m}\cdot\frac{2^n-2^k}{m-2^k}\right)^{2^{\kappa}-2} \leqslant 2^{\kappa lg\,\kappa+2^k lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^k}{m-2^k}\right)-(\kappa-1)\left(lg\,n+lg\left(1-\frac{\kappa}{n}\right)\right)} \leqslant$$

$$\leqslant 2^{2\cdot\kappa\cdot lg\,\kappa-lg\,n-(\kappa-1)\cdot lg\left(1-\frac{\kappa}{n}\right)} \to 0.$$

2. prípad $4\upsilon+2 > j > 1$.

Zo (6.5) dostávame

$$\frac{c_j}{c_1}=\frac{\kappa^j\left(n-\kappa\right)^{\underline{\kappa-j}}\left(\kappa-1\right)!}{j!\left(\kappa-j\right)!\,\kappa\left(n-\kappa\right)^{\underline{\kappa-1}}}\left(\frac{2^n}{m}\right)^{2^j-2}\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n-2^{\kappa+1}+2}{m-2^{\kappa+1}+2}^{-1}\leqslant$$

$$\leqslant\frac{1}{\kappa-j}\binom{\kappa-1}{j}\frac{\left(\kappa-1\right)^{\underline{j-1}}}{\left(n-2\kappa+j\right)^{\underline{j-1}}}\left(\frac{2^n}{m}\right)^{2^j-2}\frac{\left(2^n-2^{\kappa+1}+2^j\right)^{\underline{2^j-2}}}{\left(m-2^{\kappa+1}+2^j\right)^{\underline{2^j-2}}}\leqslant$$

$$\leqslant\frac{\left(\kappa-1\right)^{2\mathrm{j}}}{\left(n-2\kappa+j\right)^{j-1}}\left(\frac{2^n}{m}\right)^{2^j-2}\left(\frac{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\right)^{2^j-2}\leqslant$$

$$\leqslant\frac{\left(\kappa-1\right)^{2\mathrm{j}}}{\left(n-2\kappa+j\right)^{j-1}}\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\right)^{2^j-2}\leqslant$$

$$=2^{2\cdot j\cdot lg\left(\kappa-1\right)+\left(2^j-2\right)\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\right)-\left(j-1\right)\cdot lg\left(n-2\kappa+j\right)}\leqslant\quad\text{pritom}$$

$$\leqslant 2^{\left(8\upsilon+4\right)\cdot lg\,\kappa+2^{4\upsilon+2}\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\right)-lg\,n-lg\left(1-\frac{2\kappa}{n}\right)}\to 0.$$

Vráťme sa späť ku vzťahu (6.4)

$$E\left(M_{n,\kappa}^{\alpha}\right)^2\leqslant\binom{n}{\kappa}\sum_{j=0}^{\kappa}\binom{\kappa}{j}\binom{n-\kappa}{\kappa-j}\binom{2^n-2^{\kappa+1}+2^j}{m-2^{\kappa+1}+2^j}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-2^j-2}=\binom{n}{\kappa}\sum_{j=0}^{\kappa}c_j.$$

Nech $\Psi=\binom{n}{\kappa}^2\binom{2^n-2^\kappa}{m-2^\kappa}^2\binom{2^n}{m}^{-2}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-4}$, potom využitím (6.6) dostávame, že

$$E\left(M_{n,\kappa}^{\alpha}\right)^2\leqslant\binom{n}{\kappa}\left(c_0+\kappa\cdot c_1\right)=\binom{n}{\kappa}\binom{n-\kappa}{\kappa}\binom{2^n-2^{\kappa+1}+1}{m-2^{\kappa+1}+1}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-3}+$$

$$+\kappa^2\cdot\binom{n}{\kappa}\binom{n-\kappa}{\kappa-1}\binom{2^n-2^{\kappa+1}+2}{m-2^{\kappa+1}+2}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^{\kappa+1}-4}=$$

$$= \Psi \cdot \left[\binom{n-\kappa}{\kappa} \binom{n}{\kappa}^{-1} \frac{\binom{2^n - 2^{\kappa+1}+1}{m-2^{\kappa+1}+1}}{\binom{2^n-2^\kappa}{m-2^\kappa}} \binom{2^n}{m} \frac{m}{2^n} + \kappa^2 \cdot \binom{n-\kappa}{\kappa-1} \binom{n}{\kappa}^{-1} \binom{2^n}{m} \frac{\binom{2^n-2^{\kappa+1}+2}{m-2^{\kappa+1}+2}}{\binom{2^n-2^\kappa}{m-2^\kappa}} \right] \leqslant$$

$$\Psi \cdot \left[\frac{(2^n-2^{\kappa+1}+1)!\,(m-2^\kappa)!\,(m-2^\kappa)!\,(2^n-1)!}{(m-2^{\kappa+1}+1)!\,(2^n-2^\kappa)!\,(2^n-2^\kappa)!\,(m-1)!} + \kappa^2 \cdot \binom{n-\kappa}{\kappa-1} \binom{n}{\kappa}^{-1} \binom{2^n}{m} \frac{\binom{2^n-2^{\kappa+1}+2}{m-2^{\kappa+1}+2}}{\binom{2^n-2^\kappa}{m-2^\kappa}} \right]$$

$$= \Psi \cdot \left[\frac{(m-2^\kappa)^{\underline{2^\kappa-1}}\,(2^n-1)^{\underline{2^\kappa-1}}}{(2^n-2^\kappa)^{\underline{2^\kappa-1}}\,(m-1)^{\underline{2^\kappa-1}}} + \kappa^2 \cdot \binom{n-\kappa}{\kappa-1} \binom{n}{\kappa}^{-1} \frac{(m-2^\kappa)^{\underline{2^\kappa-2}}\,(2^n)^{\underline{2^\kappa}}}{(2^n-2^\kappa)^{\underline{2^\kappa-2}}\,(m)^{\underline{2^\kappa}}} \right] \leqslant$$

$$\leqslant \Psi \cdot \left[1 + \frac{(m-2^\kappa)^{\underline{2^\kappa-2}}\,(2^n-2)^{\underline{2^\kappa-2}}}{(2^n-2^\kappa)^{\underline{2^\kappa-2}}\,(m-2)^{\underline{2^\kappa-2}}} O\left(\frac{\kappa^3}{n} \left(\frac{2^n}{m} \right)^2 \right) \right] \leqslant$$

$$\leqslant \Psi \cdot \left[1 + \frac{(m-2^\kappa)^{\underline{2^\kappa-2}}\,(2^n-2^\kappa)^{\underline{2^\kappa-2}}}{(2^n-2^\kappa)^{\underline{2^\kappa-2}}\,(m-2^\kappa)^{\underline{2^\kappa-2}}} O\left(\frac{\kappa^3}{n} \cdot \left(\frac{2^n}{m} \right)^2 \right) \right] = \Psi \left[1 + O\left(\left(\frac{2^n}{m} \right)^2 \cdot \frac{\kappa^3}{n} \right) \right]$$

A to sme chceli dokázať.

Tvrdenie 7

$$P_3\left(\left\{ f\,;\, f \in C_n^\alpha \wedge \left| M^\alpha_{n,\kappa}(f) - EM^\alpha_{n,\kappa} \right| \geqslant \frac{EM^\alpha_{n,\kappa}}{\kappa} \right\} \right) = O\left(\left(\frac{2^n}{m} \right)^2 \cdot \frac{\kappa^5}{n} \right).$$

Dôkaz:

Z Čebyševovej nerovnosti pre $\varepsilon = \frac{EM^\alpha_{n,\kappa}}{\kappa}$ dostávame

$$P_3\left(\left\{f\,;\,f\in C_n^{\alpha}\wedge\left|M_{n,\kappa}^{\alpha}(f)-EM_{n,\kappa}^{\alpha}\right|\geqslant\frac{EM_{n,\kappa}^{\alpha}}{\kappa}\right\}\right)\leqslant\kappa^2\cdot\frac{DM_{n,\kappa}^{\alpha}}{(EM_{n,\kappa}^{\alpha})^2}=$$

$$=\kappa^2\cdot\frac{E(M_{n,\kappa}^{\alpha})^2-(EM_{n,\kappa}^{\alpha})^2}{(EM_{n,\kappa}^{\alpha})^2},\quad\text{následnými úpravami dostávame}$$

$$\leqslant\kappa^2\frac{\binom{2^n-2^\kappa}{m-2^\kappa}^2\binom{2^n}{m}^{-2}\left(\frac{m}{2^n}\right)^{2\cdot(2^\kappa-2)}\binom{n}{\kappa}^2\left[1+O\left(\left(\frac{2^n}{m}\right)^2\cdot\frac{\kappa^3}{n}\right)-\left(1-\frac{1}{n}\right)^2\right]}{\binom{2^n-2^\kappa}{m-2^\kappa}^2\binom{2^n}{m}^{-2}\left(\frac{m}{2^n}\right)^{2(2^\kappa-2)}\binom{n}{\kappa}^2\left(1-\frac{1}{n}\right)^2}=O\left(\left(\frac{2^n}{m}\right)^2\cdot\frac{\kappa^5}{n}\right).$$

Teraz pre každú dvojicu $f=(f_1,f_2)\in C_n$ definujeme podmnožinu vrcholov z N_{f_1} nasledovným spôsobom: $Z_f=\left\{\alpha\,;\,\alpha\in N_{f_1}\wedge\left|M_{n,\kappa}^{\alpha}(f)-EM_{n,\kappa}^{\alpha}\right|\geqslant\kappa^{-1}EM_{n,\kappa}^{\alpha}\right\}$. Vrcholy množiny Z_f budeme nazývať zlé vrcholy páru f.

Tvrdenie 8

Nech $f\in C_n$, nech $\alpha\in N_{f_1}-Z_f$ a nech $\upsilon=lg^{-1}\frac{2^n}{m}\cdot lg\left(\frac{2^n}{m}\cdot\frac{2^n-2^\kappa}{m-2^\kappa}\right)$, potom

$$M_{n,\kappa}^{\alpha}(f)\geqslant 2^{\kappa(lgn)\left(1-\frac{2\upsilon+1}{\kappa}\right)}(1-o(1)).$$

Dôkaz:

Nech je daný pár $f \in C_n$ spĺňajúci predpoklady. Keďže α nie je zlý vrchol páru f vieme, že $EM^{\alpha}_{n,\kappa}\left(1+\frac{1}{\kappa}\right) \geqslant M^{\alpha}_{n,\kappa}(f) \geqslant EM^{\alpha}_{n,\kappa}\left(1-\frac{1}{\kappa}\right)$. Použitím tvrdenia 5 a následných úprav dostávame

$$M^{\alpha}_{n,\kappa}(f) \geqslant \binom{2^n-2^\kappa}{m-2^\kappa}\binom{2^n}{m}^{-1}\left(\frac{m}{2^n}\right)^{2^\kappa-2}\binom{n}{\kappa}\left(1-\frac{1}{n}\right)\left(1-\frac{1}{\kappa}\right) \geqslant$$

$$\geqslant \frac{(m)^{\underline{2^\kappa}}}{\left(2^n\right)^{\underline{2^\kappa}}}\left(\frac{m}{2^n}\right)^{2^\kappa-2}\left(\frac{n}{\kappa}\right)^{\kappa}\left(1-o(1)\right) \geqslant \left(\frac{m-2^\kappa}{2^n-2^\kappa}\right)^{2^\kappa-1}\left(\frac{m}{2^n}\right)^{2^\kappa-1}\left(\frac{n}{\kappa}\right)^{\kappa}\left(1-o(1)\right) =$$

$$= \left(\frac{n}{\kappa}\right)^{\kappa}\left(\frac{m\cdot(m-2^\kappa)}{2^n\cdot(2^n-2^\kappa)}\right)^{2^\kappa-1}\left(1-o(1)\right) = 2^{\kappa lg\frac{n}{\kappa}+(2^\kappa-1)lg\left(\frac{m\cdot(m-2^\kappa)}{2^n\cdot(2^n-2^\kappa)}\right)}\left(1-o(1)\right) \geqslant$$

$$\geqslant 2^{\kappa(lg\,n-lg\,\kappa)+(lg\,n)\left(lg^{-1}\frac{2^n}{m}\right)2lg\left(\frac{m\cdot(m-2^\kappa)}{2^n\cdot(2^n-2^\kappa)}\right)}\left(1-o(1)\right) = 2^{\kappa(lg\,n-lg\,\kappa)-2\cdot(lg\,n)\upsilon}\left(1-o(1)\right) =$$

$$= 2^{\kappa lg(n)\left(1-\frac{lg\,\kappa}{lg\,n}-\frac{2\upsilon}{\kappa}\right)}\left(1-o(1)\right) \geqslant 2^{\kappa lg(n)\left(1-\frac{2\upsilon+1}{\kappa}\right)}\left(1-o(1)\right).$$

Dokázali sme, že keď máme vrchol $\alpha \in N_{f_1}$ páru $(f_1, f_2) \in C_n$, ktorý nepatrí medzi zlé vrcholy tohto páru, t.j. $\alpha \notin Z_{(f_1,f_2)}$, tak (skoro isto) existuje aspoň jeden taký κ rozmerný maximálny interval K_α, že $K_\alpha \subseteq N_{f_1}$ a $K_\alpha - \{\alpha\} \subseteq N_{f_2}$.

Teraz sa pozrieme práve na zlé vrcholy párov z C_n, pričom prejdeme z pravdepodobnostného priestoru $\left(C^{\alpha}_n, P_3\right)$ do priestoru $\left(C_n, P_2\right)$.

Nech $f \in C_n$, definujme $\zeta(f)$ ako náhodnú premennú na $\left(C_n, P_2\right)$, ktorá

označuje počet zlých vrcholov páru *f*. Definujme indikátor $\zeta_\alpha(f) = \begin{cases} 1 & \alpha \in Z_f \\ 0 & inak \end{cases}$.

Tvrdenie 9

$$E\,\zeta = 2^n \cdot O\left(\frac{2^n}{m}\frac{\kappa^5}{n}\right).$$

Dôkaz:

$$E\,\zeta = \sum_{f \in C_n} P_2(\{f\})\zeta(f) = \sum_{f \in C_n} P_2(\{f\}) \sum_{\alpha \in D^n} \zeta_\alpha(f) = \sum_{\alpha \in D^n} \sum_{f \in C_n} P_2(\{f\})\zeta_\alpha(f) =$$

$= 2^n \sum_{f \in C_n} P_2(\{f\})\zeta_{\bar{1}}(f)$, kde $\bar{1}$ označuje vrchol $\bar{1} = (1, 1, \ldots 1)$. Ďalej dostávame, že $2^n \sum_{f \in C_n} P_2(\{f\})\zeta_{\bar{1}}(f) = 2^n \cdot P_2\left(\{f; f \in C_n \wedge \bar{1} \in Z_f\}\right) =$

$$= 2^n \cdot P_3\left(\{f; f \in C_n \wedge \bar{1} \in Z_f\}\right) \cdot P_2\left(C_n^{\bar{1}}\right) = 2^n \cdot O\left(\left(\frac{2^n}{m}\right)^2 \cdot \frac{\kappa^5}{n}\right) \cdot \frac{m}{2^n} = 2^n \cdot O\left(\frac{2^n}{m} \cdot \frac{\kappa^5}{n}\right).$$

Tvrdenie 10

Nech $f \in C_n$, potom (skoro isto) platí $|Z_f| \leqslant \frac{\kappa^6}{n}\frac{2^{2n}}{m}$.

Dôkaz:

Keďže $\zeta(f) = |Z_f|$ z Markovovej nerovnosti pre $\varepsilon = 2^{2n}\frac{\kappa^6}{m \cdot n}$ dostávame požadované tvrdenie.

Tvrdenie 11

Pre každú funkciu $f \in F_m$ existuje (skoro isto) v (F_m, P_0) taký pár

$(f_1, f_2) \in C_n$, že $f_1 = f$, $|N_{f_2}| = 2^{n-\chi}$ a $|Z_f| \leqslant \frac{\kappa^6}{n}\frac{2^{2n}}{m}$, kde

$\chi = 2 + \lfloor lg\, log_{\frac{2^n}{m}} n + lg\, lg\, lg\, n \rfloor$.

Dôkaz:

Definujme množiny $Q_n = \left\{ f ; f \in C_n \wedge |Z_f| \leqslant \frac{\kappa^6}{n}\frac{2^{2n}}{m} \right\}$,

$R_n = \left\{ f ; f \in B_n \wedge |N_f| \leqslant 2^{n-\chi} \right\}$,

$S_n = \left\{ f ; f \in F_m \wedge \left(\exists g \in R_n : (f, g) \in Q_n\right) \right\}$.

Chceme teda dokázať, že náhodná boolovská funkcia má skoro isto vlastnosti funkcií z množiny S_n, teda že $\lim_{n\to\infty} P_0(S_n) = 1$. Nech naviac $T_n = F_m \times R_n$ a $U_n = Q_n \cap T_n$.

Potom $P_1(U_n) = \sum_{(f_1, f_2)\in U_n} P_1\left(\{(f_1, f_2)\}\right) = \sum_{(f_1, f_2)\in U_n} P_0\left(\{f_1\}\right) P_0'\left(\{f_2\}\right)$

Nech $U_n^{(1)}$ je projekcia na prvé prvky párov z U_n. Podobne nech $U_n^{(2)}$ je projekcia na druhé prvky párov z U_n. Potom

$$\sum_{(f_1, f_2)\in U_n} P_0\left(\{f_1\}\right)\cdot P_0'\left(\{f_2\}\right) \leqslant \sum_{f_1 \in U_n^{(1)}} P_0\left(\{f_1\}\right)\cdot P_0'\left(U_n^{(2)}\right) \leqslant$$

$$\leqslant P_0'(R_n)\cdot \sum_{f_1 \in U_n^{(1)}} P_0\left(\{f_1\}\right) \leqslant P_0(S_n)\cdot P_0'(R_n).$$

Preto $P_0(S_n) \geqslant \frac{P_1(U_n)}{P_0'(R_n)}$ a tak

$$\lim_{n\to\infty} P_0(S_n) \geqslant \lim_{n\to\infty} \frac{P_1(U_n)}{P_0'(R_n)} = \lim_{n\to\infty} \frac{P_1(Q_n \cap T_n)}{P_1(F_m \times R_n)} =$$

$$= \lim_{n\to\infty} \frac{1 - P_1(Q_n^K \cup T_n^K)}{P_1(T_n)} \geqslant \lim_{n\to\infty} \frac{1 - P_1(Q_n^K) - P_1(T_n^K)}{P_1(T_n)} = \lim_{n\to\infty} \frac{P_1(T_n) - P_2(Q_n^K)\cdot P_1(C_n)}{P_1(T_n)},$$

kde Q_n^K označuje komplement (doplnok) množiny Q_n, podobne T_n^K komplement množiny T_n. Z tvrdenia 10 vieme, že $P_2(Q_n) \to 1$, čo nám dáva požadované tvrdenie.

Zavedieme novú premennú, nech pre $f \in F_m$ symbol $h_{n,k}(f)$ označuje počet vrcholov v N_f, ktoré sú pokryté nejakým *k*-rozmerným intervalom funkcie *f*.

Tvrdenie 12

Nech je daná ľubovoľná funkcia $f \in F_m$. Potom (skoro isto) platí nerovnosť

$$h_{n,k}(f) \leqslant \varphi(n)\cdot\binom{n}{k}\cdot 2^n \cdot \left(\frac{m}{2^n}\right)^{2^k}, \quad \text{kde} \quad \frac{1}{\varphi(n)} = o(1).$$

Dôkaz

Nech je daná ľubovoľná funkcia $f \in F_m$. Nech $i_{n,k}(f)$ označuje počet *k*-rozmerných intervalov funkcie *f*. Potom zrejme platí $h_{n,k}(f) \leqslant 2^k \cdot i_{n,k}$.

Z tvrdenia 0 i) vieme, že $E\, i_{n,k} = \binom{n}{k}\cdot 2^{n-k}\cdot\binom{2^n - 2^k}{m - 2^k}\cdot\binom{2^n}{m}^{-1}$. Počítajme

$$P_0\left(\left\{f\,;\, h_{n,k}(f) \geqslant \varphi(n)\cdot\binom{n}{k}\cdot 2^n\cdot\left(\frac{m}{2^n}\right)^{2^k}\right\}\right) \leqslant \qquad (12.1)$$

pomocou formuly 1 dostávame

$$P_0\left(\left\{f\,;h_{n,k}(f)\geqslant\varphi(n)\cdot\binom{n}{k}\cdot 2^n\cdot\binom{2^n-2^k}{m-2^k}\cdot\binom{2^n}{m}^{-1}\right\}\right)\leqslant$$

$$\leqslant P_0\left(\left\{f\,;i_{n,k}(f)\cdot 2^k\geqslant\varphi(n)\cdot\binom{n}{k}\cdot 2^n\cdot\binom{2^n-2^k}{m-2^k}\cdot\binom{2^n}{m}^{-1}\right\}\right)=$$

$$=P_0\left(\left\{f\,;i_{n,k}(f)\geqslant\varphi(n)\cdot\binom{n}{k}\cdot 2^{n-k}\cdot\binom{2^n-2^k}{m-2^k}\cdot\binom{2^n}{m}^{-1}\right\}\right)=$$

$$=P_0\left(\left\{f\,;i_{n,k}(f)\geqslant\varphi(n)\cdot E\,i_{n,k}\right\}\right).$$

Pomocou Markovovej nerovnosti z (12.1) dostávame

$$P_0\left(\left\{f\,;h_{n,k}(f)\geqslant\varphi(n)\cdot\binom{n}{k}\cdot 2^n\cdot\left(\frac{m}{2^n}\right)^{2^k}\right\}\right)\leqslant\frac{1}{\varphi(n)}$$

Kapitola 5

Hlavný dôkaz

Tvrdenie 1

Nech $l(f)$ označuje maximálnu dĺžku (počet implikantov) iredundantnej DNF. Potom s pravdepodobnosťou idúcou k 1 (pre $n \to \infty$) platí, že

$m(n)\cdot\left(1-\varepsilon_3(n)\right) \leqslant l(f) \leqslant m(n)$, kde $\varepsilon_3(n) \to 0$. Teda $l(f) \sim m(n)$. Naviac keď

$\lim_{n\to\infty}\left(\frac{m}{2^n}\right) = p \in (0,1)$, tak $\varepsilon_3(n) = O\left(\frac{1}{lg(n)\cdot lg\, lg(n)}\right)$.

Dôkaz, horný odhad

Chceme dokázať, že $l(f) \leqslant m$. Nech je daná ľubovoľná funkcia $f \in F_m$, nech U je jej iredundantné pokrytie maximálnymi intervalmi (je zrejmé, že idedundantná DNF je zložená len z prostých implikantov a teda iredundantné pokrytie pozostáva len z maximálnych intervalov). Každý maximálny interval I_k v pokrytí U musí obsahovať aspoň jeden taký vrchol α_k, ktorý nie je pokrytý žiadnym iným intervalom v U, presnejšie $(\alpha_k \in I_k) \wedge \left(\alpha_k \notin \bigcup_{j \neq k} I_j\right)$. Inak by bolo možné daný interval vynechať a pokrytie by nebolo iredundantné. Keďže graf indukovaný funkciou f obsahuje práve m vrcholov, dĺžka iredundantnej DNF prislúchajúcej pokrytiu U nemôže prekročiť m. A to sme chceli dokázať.

dolný odhad

Z tvrdenia 11 vieme, že

$$P_0(S_n) = \lim_{n\to\infty} P_0\left(\left\{f\,;\, f \in F_m \wedge \left(\exists g : (f,g) \in C_n \wedge Z_{(f,g)} \leqslant \frac{\kappa^6}{n}\frac{2^{2n}}{m}\right)\right\}\right) = 1.$$ Nech

$$V_n = \left\{f\,;\, f \in F_m \wedge h_{n,k} \leqslant \varphi(n)\binom{n}{k}2^n\left(\frac{m}{2^n}\right)^{2^k}\right\},$$ kde $\varphi(n) \to \infty$. Pomocou tvrdenia 12 dostávame, že $\lim_{n\to\infty} P_0(V_n) = 1$ a tak $\lim_{n\to\infty} P_0(S_n \cap V_n) = 1.$ Chceme dokázať, že ľubovoľná funkcia $f \in (S_n \cap V_n)$ má (skoro isto) iredundantné pokrytie dĺžky aspoň

$m\cdot\left(1-\varepsilon_3(n)\right)$, kde $\varepsilon_3(n)\to 0$.

Nech teda *f* je ľubovoľná funkcia z množiny $\left(S_n\cap V_n\right)$. Nech *g* je funkcia taká, že $(f,g)\in C_n$, $|N_g|=2^{n-\chi}$ a $\left|Z_{(f,g)}\right|\leqslant\frac{\kappa^6}{n}\frac{2^{2n}}{m}$, kde

$\chi=2+\lfloor lg\,log_{\frac{2^n}{m}}n+lg\,lg\,lg\,n\rfloor$.

Z tvrdenia 8 vieme, že pre $\alpha\in N_f-Z_{(f,g)}$ platí $M^{\alpha}_{n,\kappa}(f,g)\geqslant 1$. Inými slovami, každý vrchol $\alpha\in N_f-Z_{(f,g)}$ je obsiahnutý v nejakom κ rozmernom maximálnom intervale *K* funkcie f takom, že $K-\{\alpha\}\subseteq N_g$. Iredundantné pokrytie množiny N_f skonštruujeme nasledovným spôsobom:

Najprv nech U_1 je iredundantné pokrytie množiny $Z_{(f,g)}$ maximálnymi intervalmi *I* funkcie *f*. Nevyžadujeme $I\subseteq Z_{(f,g)}$.

Každý vrchol $\alpha\in\left(N_g-\cup U_1\right)$ je obsiahnutý aspoň v jednom κ rozmernom maximálnom intervale K_α funkcie f takom, že $K_\alpha-\{\alpha\}\subseteq N_g$. Nech U_2 je ľubovoľné iredundantné pokrytie množiny $\left(N_g-\cup U_1\right)$ takýmito maximálnymi intervalmi. Znakom $\cup U$ pritom myslíme zjednotenie vrcholov obsiahnutých v jednotlivých intervaloch pokrytia *U*.

Podobne každý vrchol $\alpha\in\left(N_f-\cup\left(U_1\cup U_2\right)\right)$ je obsiahnutý v nejakom κ rozmernom maximálnom intervale K_α takom, že $K_\alpha-\{\alpha\}\subseteq N_g$. Máme práve $M^{\alpha}_{n,\kappa}(f,g)$ možností ako zvoliť maximálny interval K_α. Voľbou práve jedného

takéhoto maximálneho intervalu pre každý vrchol α dostávame iredundantné pokrytie U_3 množiny $\left(N_f - \cup(U_1 \cup U_2)\right)$. Treba si uvedomiť fakt, že každý interval K_α pokrýva práve jeden vrchol množiny $\left(N_f - \cup(U_1 \cup U_2)\right)$. Dôvod je zrejmý. Keďže $K_\alpha - \{\alpha\} \subseteq N_g$, tak všetky vrcholy intervalu K_α okrem vrcholu α sú už pokryté intervalmi z $\cup(U_1 \cup U_2)$.

Nakoniec nech U je iredundantné pokrytie získané z $U_1 \cup U_2 \cup U_3$. Zjavne dĺžka iredundantnej DNF identifikovanej pokrytím U nebude menšia ako U_3. Pritom

$$|U_3| = |N_f - \cup(U_1 \cup U_2)| \geqslant |N_f| - |\cup U_1| - |\cup U_2|, \qquad (1.1)$$

V tejto chvíli upozorňujeme na fakt, že (prvá) rovnosť vo vzťahu (1.1) nie je úplne triviálna, využíva fakt spomínaný v predošlom odstavci, že každý interval v U_3 pokrýva práve jeden vrchol množiny $N_f - \cup(U_1 \cup U_2)$ a preto $|U_3| = |\cup U_3 - \cup(U_1 \cup U_2)|$. Neplatí však (vo všeobecnosti) $N_f = U_3$ na čo by predošlá rovnosť spolu so vzťahom (1.1) mohli zvádzať.

Nech U_1' je podmnožina množiny U_1 pozostávajúca iba z intervalov dimenzie menšej ako χ. Nech $U_1'' = U_1 - U_1'$. Zrejme $|\cup U_1'| \leqslant 2^\chi |U_1'| \leqslant 2^\chi |Z_{(f,g)}|$. Každý vrchol $\alpha \in \cup U_1''$ je obsiahnutý v maximálnom intervale $I \in U_1''$ dimenzie aspoň χ. Z toho vyplýva, že vrchol α je obsiahnutý v intervale (nie nutne maximálnom) $J \subseteq I$ s dimenziou práve χ. Teda $|\cup U_1''| \leqslant h_{n,\chi}(f)$.

U_2 je iredundantné pokrytie množiny $N_g - \cup U_1$ takými intervalmi K_α, že $K_\alpha - \{\alpha\} \subseteq N_g$. Z iredundantnosti vyplýva fakt $|U_2| \leqslant |N_g|$ a keďže každý interval pokrytia U_3 pokrýva najviac 1 vrchol nepatriaci do N_g dostávame $|\cup U_2| \leqslant 2|N_g|$.

Z doterajších úvah vyplýva, že

$$|U| \geqslant |U_3| \geqslant |N_f| - |\cup U_1'| - |\cup U_1''| - |\cup U_2| \geqslant |N_f| - 2^\chi |Z_{(f,g)}| - h_{n,\chi}(f) - 2|N_g| \geqslant$$

$$\geqslant m - 2^\chi \frac{\kappa^6}{n} \frac{2^{2n}}{m} - \varphi(n) \binom{n}{\chi} 2^n \left(\frac{m}{2^n}\right)^{2^\chi} - 2^{n-\chi+1} \geqslant$$

$$\geqslant m \left(1 - \left(\frac{2^n}{m}\right)^2 2^\chi \frac{\kappa^6}{n} - \varphi(n) \left(\frac{3n}{\chi}\right)^\chi \left(\frac{m}{2^n}\right)^{2^\chi - 1} - \frac{2^{n-\chi+1}}{m}\right) \geqslant$$

$$\geqslant m \left(1 - \left(\frac{2^n}{m}\right)^2 2^\chi \frac{\kappa^6}{n} - \varphi(n) 2^{\chi \cdot lg \frac{3n}{\chi}} \cdot 2^{lg\, n \cdot lg^{-1} \frac{2^n}{m} \cdot lg\, lg\, n \cdot lg \frac{m}{2^n}} - \frac{2^{n-\chi+1}}{m}\right) \geqslant$$

$$\geqslant m \left(1 - O\left(\frac{2^{2n}}{m^2} \frac{lg^2(n)}{n}\right) - \varphi(n) 2^{-lg(n) lg\, lg(n)(1+o(1))} - O\left(\frac{2^n}{m} \frac{lg\left(2^n \cdot m^{-1}\right)}{lg(n)\, lg\, lg(n)}\right)\right)$$ a dostávame,

že $$|U| \geqslant |U_3| \geqslant m \left(1 - O\left(\frac{2^n}{m} \frac{lg\left(2^n \cdot m^{-1}\right)}{lg(n)\, lg\, lg(n)}\right)\right) \qquad (1.2)$$

a to sme chceli dokázať.

Tvrdenie 2

S pravdepodobnosťou idúcou k 1 (pre $n \to \infty$) počet iredundantných DNF $\tau(f)$ náhodnej boolovskej funkcie $f \in F_m$ spĺňa nerovnosť

$2^{m \cdot lg\, n \cdot lg\, log_{\frac{2^n}{m}} n \cdot (1 - \varepsilon_4(n))} \leqslant \tau(f) \leqslant 2^{m \cdot lg\, n \cdot lg\, log_{\frac{2^n}{m}} n \cdot (1 + \varepsilon_5(n))}$, kde $\varepsilon_4(n), \varepsilon_5(n) \to 0$. Teda

$lg\,\tau(f) \sim m \cdot lg(n) \cdot lg\, log_{\frac{2^n}{m}} n$. Ak naviac $\lim_{n\to\infty}\left(\frac{m}{2^n}\right) = p \in (0,\,1)$, tak

$\varepsilon_4(n),\, \varepsilon_5(n) = O\left(lg^{-1}\, log_{\frac{2^m}{n}} n\right)$.

Dôkaz, horný odhad

Z tvrdenia 0 iii) vieme, že pre dĺžku skrátenej DNF platí vzťah

$$s(f) \leqslant n^{(1+\varepsilon_2(n))\, lg\, log_{\frac{2^n}{m}} n} \cdot 2^n. \qquad (2.1)$$

Nech W_n je množina všetkých funkcií z F_m, ktoré spĺňajú túto nerovnosť. Nech X_n je množina všetkých funkcií, ktoré spĺňajú tvrdenie 1. Potom zrejme

$\lim_{n\to\infty} P_0(W_n \cap X_n) = 1$. Naviac je jasné, že počet iredundantných DNF možno zhora ohraničiť hodnotou $\sum_{i=1}^{l(f)} \binom{s(f)}{i}$. Označme i-tý prvok tejto sumy d_i. Pre funkciu $f \in (R_n \cap S_n)$ zjavne platí $\lim_{n\to\infty} \frac{s(f)}{l(f)} = \infty$ a prvok $d_{l(f)}$ je najväčší.

Odtiaľ dostávame

$$\tau(f) \leqslant \sum_{i=1}^{l(f)} d_i \leqslant d_{l(f)} + \sum_{i=1}^{l(f)-1} d_i \leqslant d_{l(f)}\left(1 + l(f) \cdot \frac{d_{l(f)-1}}{d_{l(f)}}\right) \leqslant$$

$$\leqslant \binom{s(f)}{l(f)}\left(1 + l(f) \cdot \binom{s(f)}{l(f)-1}\binom{s(f)}{l(f)}^{-1}\right) \leqslant \left(\frac{3 \cdot s(f)}{l(f)}\right)^{l(f)} \cdot \left(1 + l(f) \cdot \frac{l(f)}{s(f) - l(f) + 1}\right).$$

Využitím tvrdenia 0 iii) tvrdenia 1 dostávame

$$\tau(f) \leqslant \left(\frac{3 \cdot n^{(1+\varepsilon_2(n)) lg\, log_{\frac{2^n}{m}} n} 2^n}{m(1-\varepsilon_3(n))} \right)^m (1+o(1)) = \left(\frac{3 \cdot 2^{n+(lg\, n)(1+\varepsilon_2(n)) lg\, log_{\frac{2^n}{m}} n}}{2^{lg\left(m\frac{2^n}{2^n}\right)+lg(1-\varepsilon_3(n))}} \right)^m (1+o(1)) =$$

$$= \left(\frac{3 \cdot 2^{n+(lg\, n)(1+\varepsilon_2(n)) lg\, log_{\frac{2^n}{m}} n}}{2^{n-lg\frac{2^n}{m}+lg(1-\varepsilon_3(n))}} \right)^m (1+o(1)) \leqslant$$

$$\leqslant 2^{(lg\, n)(1+\varepsilon_2(n)) lg\, log_{\frac{2^n}{m}} n \cdot \left(1+O\left(lg\frac{2^n}{m} \cdot \left(\frac{1}{lg\, n \cdot lg\, log_{\frac{2^n}{m}} n}\right)\right)\right) \cdot m} (1+o(1)) \leqslant$$

$$\leqslant 2^{m \cdot (lg\, n) \cdot lg\, log_{\frac{2^n}{m}} n \cdot (1+\varepsilon_2(n)) \cdot \left(1+O\left(lg\frac{2^n}{m} \cdot \left(\frac{1}{lg\, n \cdot lg\, log_{\frac{2^n}{m}} n}\right)\right)\right)} = 2^{m \cdot lg\, n \cdot lg\, log_{\frac{2^n}{m}} n \cdot (1+\varepsilon_5(n))}$$ A to sme chceli dokázať.

Dôkaz, horný odhad

V tvdrení 1 sme konštruovali iredundantné pokrytie U_3 funkcie $f \in (S_n \cap V_n)$ a pripomenuli sme, že pre každý vrchol $\alpha \in (N_f - \cup(U_1 \cup U_2))$ máme $M^{\alpha}_{n,\kappa}(f, g)$ možností ako vybrať maximálny interval K_{α}. Každý takýto interval K_{α} pokrýva práve jeden vrchol množiny $(N_f - \cup(U_1 \cup U_2))$, preto existuje $\prod_{\alpha \in (N_f - \cup(U_1 \cup U_2))} M^{\alpha}_{n,\kappa}(f, g)$ možností, ako skonštruovať iredundantné pokrytie U_3.

Potom pomocou tvrdenia 8 dostávame

$$\tau(f) \geqslant \prod_{\alpha \in (N_f - \cup(U_1 \cup U_2))} M^{\alpha}_{n,\kappa}(f, g) \geqslant \left(2^{\kappa(lg\, n)\left(1-\frac{2\upsilon+1}{\kappa}\right)} (1-o(1)) \right)^{|U_3|} \geqslant$$ z (1.2) máme

$$\geqslant 2^{\kappa(lg\,n)\left(1-\frac{2\upsilon+1}{\kappa}-\frac{1}{\kappa\,lg\,n}\right)m\cdot(1-\varepsilon_3(n))}=2^{m\,lg\,n\left(\kappa-(2\cdot\upsilon+1)-lg^{-1}n\right)(1-\varepsilon_3(n))}\geqslant$$

$$\geqslant 2^{m\,lg\,n\left(lg\,lg\,n-lg\,lg\,\frac{2^n}{m}-2\upsilon-lg^{-1}n\right)(1-\varepsilon_3(n))}\geqslant 2^{m\cdot lg\,n\cdot lg\,lg_{\frac{2^n}{m}}n\cdot(1-\varepsilon_4(n))}.$$

Pripomíname, že $\upsilon=lg^{-1}\frac{2^n}{m}\cdot lg\left(\frac{2^n}{m}.\frac{2^n-2^\kappa}{m-2^\kappa}\right)$.

Naviac zrejme ak $\left(\frac{m}{2^n}\right)\to p\in(0\,,\,1)$, potom $\varepsilon_4(n)=\left(\frac{1}{lg\,lg_{\frac{2^n}{m}}n}\right)$.

A to sme chceli dokázať.

Kapitola 6

Záver

V tejto kapitole by sme chceli zhrnúť dosiahnuté výsledky. V práci sme sa zaoberali maximálnou dĺžkou a počtom iredundantných disjunktívnych normálnych foriem náhodnej boolovskej funkcie. Dokázali sme, že pre maximálnu dĺžku $l(f)$ iredundantnej DNF náhodnej boolovskej funkcie f platí vzťah

$m(n)\cdot\left(1-\varepsilon_3(n)\right) \leqslant l(f) \leqslant m(n)$. Ďalej sme zhora aj zdola odhadli počet iredundantných DNF $\tau(f)$ náhodnej boolovskej funkcie vzťahom

$$m\cdot lg\, n\cdot lg\, log_{\frac{2^n}{m}} n\cdot(1-\varepsilon_4(n)) \leqslant lg\,\tau(f) \leqslant m\cdot lg\, n\cdot lg\, log_{\frac{2^n}{m}} n\cdot(1+\varepsilon_5(n)).$$

Problematika náhodných boolovských funkcií a minimalizácie DNF však stále

ostáva nevyčerpaná. Ukazuje sa, že vhodným parametrom na skúmanie je počet minimálnych a najkratších DNF, prípadne porovnanie ich počtu. Každá najkratšia DNF je iredundantná, možno takisto skúmať, aký je pomer najkratších DNF oproti všetkým iredundantným DNF náhodnej boolovskej funkcie.

Literatúra

[1] J. C. Bioch: Modular Decomposition of Boolean Functions, ERIM Report Series, Rotterdam 2002.

[2] B. Bollobas: Random Graphs, Academic press, London 1985.

[3] W. Feller: An Introduction to Probability Theory and Its Applications. Vol. 1, 3rd Ed., J. Wiley and Sons, New York 1970.

[4] M. Kovalíková: Metrické vlastnosti boolovských funkcií s daným počtom jednotiek, diplomová práca, FMFI UK, Katedra informatiky, Bratislava 2006.

[5] F. Mileto, G. Putzolu: Average values of quantities appearing in Boolean function minimalization, IEE EC-13, 2, 1964.

[6] E. M. Palmer: Graphical Evolution: Appendixes, New York 1985.

[7] A. A. Sapozhenko: On the maximum length of an irredundant disjunctive normal form of almost every Boolean function. Mat. Zametki, Vol. 4, 1968.

[8] M. Škoviera: O dĺžke a štruktúre skrátenej DNF náhodných boolovských funkcií, diplomová práca, Matematicko-fyzikálna fakulta UK, Katedra matematickej analýzy, Bratislava 1981.

[9] M. Škoviera: On the Minimalization of Random boolean Functions, Part 1, Computers and Artificial Intelligence, Bratislava 1986.

[10] M. Škoviera: On the Minimalization of Random boolean Functions, Part 2, Computers and Artificial Intelligence, Bratislava 1986.

[11] S. V. Yablonskii, O. B. (Eds.) Lupanov: Discrete Mathematics and Mathematical Problems of Cybernetics, Nauka, Moscow 1974.