УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ
Бр. 311/4-21
21.03. 2023 год.
Београд, Студентски трг 16
тел. 20 27 801, факс: 26 30 151

Наставно-научном већу
Математичког факултета
Универзитета у Београду

На седници наставног већа Математичког факултета одржаној 30. 06. 2017. године, одређени смо у комисију за преглед и оцену докторске дисертације *"Пребројавање класа еквиваленције Булових функција"* кандидата Марка Царића. На основу увида у садржај дисертације подносимо следећи

ИЗВЕШТАЈ

1 Биографија кандидата

Марко Царић је рођен 22. маја 1973. године у Београду. Завршио је Математичку гимназију у Београду 1991. године. Основне студије на Математичком факултету у Београду, на смеру Вероватноћа и статистика, завршио је 2002. године са просеком 8.36. Постдипломске студије на Математичком факултету у Београду, смер Рачунарство, завршио је 2010. године одбраном магистарског рада под насловом *Проналажење колизија код криптографских хеш функција* под менторством професора др Миодрага Живковића. Докторске студије на Математичком факултету у Београду, смер Информатика, уписао је 2015. године. Положио је све испите предвиђене планом и програмом докторских студија са просечном оценом 9.83.

Као програмер радио је у компанији Univerzal Holding од 2002. до 2004. године. На Високој школи за електротехнику и рачунарство у Београду радио је као стручни сарадник, асистент и предавач од 2002. до 2016. године. Као предавач радио је на Високој школи за IT технологије од 2016. до 2017. године. У Народној банци Србије од 2017. године ради као администратор база података.

2 Кратак приказ докторске дисертације и преглед резултата

У овој дисертацији разматран је проблем израчунавања броја класа еквиваленције Булових функција. Тежина одређивања броја класа еквиваленције нагло расте са бројем променљивих n. Мотивација за избор ове теме лежи у чињеници да су конкретни бројеви до сада били познати само за релативно мале вредности n, иако је сам проблем теоријски одавно решен.

Нека је G група пермутација скупа $B_n = \{0,1\}^n$. Разматра се дејство групе G на скаларне, $B_n \mapsto B_1$, односно векторске инвертибилне Булове функције, $B_n \mapsto B_n$. Две скаларне Булове функције $f(x)$ и $g(x)$, дефинисане на B_n, сматрају се еквивалентним у односу на групу G, тј. $f \sim g$, ако је за неко $\sigma \in G$ за свако $x \in B_n$ важи $f(x) = g(\sigma(x))$. Две векторске инвертибилне Булове функције $f(x)$ и $g(x)$, сматрају се еквивалентним у односу на групу G, тј. $f \sim g$, ако за неки пар $(\sigma, \rho) \in G \times G$ за свако $x \in B_n$ важи $g(x) = \rho(f(\sigma(x)))$. Релација еквиваленције $\sim$ разлаже скуп свих Булових функција у класе еквиваленције. Еквиваленција Булових функција има значајну примену у логичкој синтези комбинаторних кола и у криптографији, посебно у вези са пројектовањем табела S (енг. S-box). Нека $U_n(G)$, односно $V_n(G)$ означава број класа еквиваленције скаларних, односно векторских инвертибилних Булових функција од n променљивих у односу на групу G. Бројеви $U_n(G)$ и $V_n(G)$ могу се релативно једноставно израчунати ако се зна циклусни индекс групе G. У дисертацији се разматрају четири групе G пермутација скупа B_n:

- група S'_n индукована групом S_n пермутација координата елемената $x = (x_1, x_2, \ldots, x_n) \in B_n$,
- група G_n, индукована пермутацијама и комплементирањима координата,
- група GL_n линеарних инвертибилних трансформација елемената векторског простора B_n, и
- група AGL_n афиних инвертибилних трансформација елемената B_n.

Ако пермутација $\sigma \in G$ има i_k циклуса дужине $k \geq 1$, њена циклусна структура је $i(\sigma) = (i_1, i_2, \ldots)$. Циклусни индекс групе G је генератриса

$$Z_G(f_1, f_2, \ldots) = \frac{1}{|G|} \sum_{\sigma \in G} \prod_{k \geq 1} f_k^{i_k}$$

циклусних структура свих пермутација $\sigma \in G$. Познати су изрази за циклусне индексе четири разматране групе, али је на основу ових израза

израчунавање практично изводљиво само за релативно мале вредности, за нпр. $n \leq 10$.

Дисертација приказује оригиналне резултате из области пребројавања класа еквиваленције Булових функција у односу на ове четири групе трансформација. Иако су познати изрази за циклусне индексе одговарајућих група трансформација, сами циклусни индекси, односно бројеви $U_n(G)$ и $V_n(G)$, експлицитно су израчунати само за релативно мале вредности n. За све четири групе трансформација изведен је сличан израз за циклусни индекс у облику суме по партицијама броја n. На основу тог израза и претходно израчунатих табела се циклусни индекс израчунава много ефикасније. Преглед познатих резултата за релативно мале n и нових резултата у тези за веће n приказан је у наредној табели:

Број\ G	S'_n	G_n	GL_n	AGL_n
$U_n(G)$	$11 \to 33$	$10 \to 32$	$8 \to 31$	$10 \to 31$
$V_n(G)$	$6 \to 30$	$7 \to 27$	$6 \to 26$	$6 \to 26$

Специјално, у случају групе пермутација S'_n, приказан је ефикасан директни поступак рачунања броја класа еквиваленције, који не користи циклусни индекс.

Други део дисертације односи се на мононотоне Булове функције — скаларне Булове функције које задовољавају услов монотоности (из $x \leq y$ следи $f(x) \leq f(y)$). Нека r_n, односно d_n (n-ти Дедекиндов број), означава број класа еквиваленције монотоних Булових функција у односу на групу S'_n, односно укупан број монотоних Булових функција од n променљивих. Тежина израчунавања броја r_n нагло расте са n, тако да је донедавно последњи израчунати члан низа био r_7. У дисертацији се описује поступак заснован на Фробенијусовој теореми, којим је одређен број r_8. При томе се користи позната вредност броја d_8.

Рукопис има 156 страница, од чега су прилози 21 страница, а основни текст 135 страница. Списак литературе састији се од 43 референци. Дисертација се састоји од првог - уводног поглавља и од наредна три поглавља.

У другом поглављу уводе се теоријски појмови у вези са материјалом из поглавља 3 и 4, а односе се на дискретну математику, комбинаторику и циклусне индексе разматране четири групе трансформација.

У поглављу 3 описује се поступак израчунавања цикусних индекса за четири разматране групе пермутација, као и бројева $U_n(G)$ и $V_n(G)$ класа еквиваленција Булових функција у односу на ове групе. Најпре се разматрају заједничка побољшања за све четири групе, а затим и специфична убрзања везана за појединачне групе. Ови резултати објављени су у другом раду са списка у одељку 3.1.

У поглављу 4 решава се проблем проналажења броја класа еквиваленције монотоних Булових функција. Најпре се даје општи израз за

рачунање броја r_n на основу Фробенијусове теореме — у облику суме (по партицијама броја n) броја фиксних тачака пермутације која одговара партицији. Након тога, у зависности од графова који одговарају различитим партицијама, приказују се различити начини рачунања броја фиксних тачака за $n \leq 8$. Приказан је поступак на основу кога је израчунат број r_8, што такође представља оригинални допринос ове дисертације, видети први рад са списка у одељку 3.1. Применивши сличан поступак Павелски (Pawelski, препринт https://arxiv.org/abs/2108.13997) је израчунао r_8, практично у исто време када је добијен резултат описан у дисертацији.

3 Објављени радови

3.1 Радови из области дисертације објављени су у часописима

1. M. Carić, M. Živković, *The number of nonequivalent monotone Boolean functions of 8 variables*, i IEEE Transactions on Information Theory, 2022, doi: 10.1109/TIT.2022.3214973. **M21**

2. M. Živković, M. Carić, *On the Number of Equivalence Classes of Boolean and Invertible Boolean Functions*, in IEEE Transactions on Information Theory, vol. 67, no. 1, pp. 391-407, Jan. 2021, doi: 10.1109/TIT.2020.3025767. **M21**

3. M. Carić, M. Živković, M. *On the number of equivalence classes of invertible Boolean functions under action of permutation of variables on domain and range*, Publications de l'Institut Mathématique. 100(114) 95–99 (2016). **M23**

3.2 Остали објављени радови

1. M. Carić, *Finding Collision for MD4 Hash Algorithm Using Hybrid Algorithm*, IPSI Transactions on Internet Research, January 2015, Vol. 11, No. 1, pp. 13-18. **M53**

2. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *Security of Computer Systems and Networks, Book Preview*, ComSIS – The international journal published by ComSIS Consortium, Volume 4, Number 1, June 2007. **M23**

3.3 Објављене књиге и збирке задатака

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007, ISBN 978-86-7555-305-2.

2. B. Đorđević, M. Carić, D. Pleskonjić, N. Maček, *GNU/Linux sistemsko programiranje – priručnik za laboratorijske vežbe*, Visoka škola elektrotehnike i računarstva, Beograd, 2007, ISBN 978-86-7982-009-9.

3. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić, *Sigurnost računarskih mreža – zbirka rešenih zadataka*, Viša elektrotehnička škola, Beograd, 2006, ISBN 86-85081-55-6.

4 Закључак и предлог комисије

Разматрани рукопис садржи важан допринос и значајне оригиналне резултате у вези са проблемима из дискретне математике. Кандидат је до сада као коаутор објавио три научна рада која се односе на садржај дисертације. На основу свега горе наведеног, и како су испуњени сви формални услови, предлажемо да се рукопис *Пребројавање класа еквиваленције Булових функција*, кандидата Марка Царића, прихвати као докторска дисертација, и да се одреди комисија за њену одбрану.

Комисија:

М Живковић

(др Миодраг Живковић, редовни професор, ментор)

Филип Марић

(др Филип Марић, ванредни професор)

В Маринковић

(др Весна Маринковић, доцент)

Раде Живаљевић

(др Раде Живаљевић, научни саветник у МИ САНУ)

Београд, 20. марта 2023. године