УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Марко М. Царић

ПРЕБРОЈАВАЊЕ КЛАСА ЕКВИВАЛЕНЦИЈЕ БУЛОВИХ ФУНКЦИЈА

докторска дисертација

Београд, 2023.

UNIVERSITY OF BELGRADE
FACULTY OF MATHEMATICS

Marko M. Carić

COUNTING EQUIVALENCE CLASSES OF BOOLEAN FUNCTIONS

Doctoral Dissertation

Belgrade, 2023.

Ментор:

др Миодраг Живковић, редовни професор
Универзитет у Београду, Математички факултет

Чланови комисије:

др Филип Марић, ванредни професор
Универзитет у Београду, Математички факултет

др Весна Маринковић, доцент
Универзитет у Београду, Математички факултет

др Раде Живаљевић, научни саветник
Математички институт у Београду

Датум одбране: 15. септембар 2023.

Катарини, Марији и Зоји

Наслов дисертације: Пребројавање класа еквиваленције Булових функција

Резиме: 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 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 $k \geqslant 1$, њена циклусна струк-

тура је $i(\sigma) = (i_1, i_2, \ldots)$. Циклусни индекс групе G је генератриса

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

циклусних структура свих пермутација $\sigma \in G$. Општи изрази за циклусне индексе четири разматране групе су познати, али су сами циклусни индекси, односно бројеви $U_n(G)$ и $V_n(G)$, практично израчунати само за релативно мале вредности, за нпр. $n \leqslant 10$.

Дисертација приказује оригиналне резултате из области пребројавања класа еквиваленције Булових функција у односу на ове четири групе трансформација. 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 циклусни индекс се 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, а описан је трећем раду из уводног поглавља.

Други део дисертације односи се на мононотоне Булове функције — скаларне Булове функције које задовољавају услов монотоности (из $x \leqslant y$ следи $f(x) \leqslant f(y)$). 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.

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 уводном поглављу.

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 $n \leqslant 8$. Приказан је поступак на основу кога је израчунат број r_8, што такође представља оригинални допринос ове дисертације - видети први рад са списка из уводног поглавља. Применивши сличан поступак, Павелски (Pawelski, [31]) је израчунао r_8 практично у исто време када је добијен резултат описан у дисертацији.

Кључне речи: Булове функције, монотоне Булове функције, партиције, циклусни индекс, Фробенијусова теорема, Дедекиндови бројеви

Научна област: Рачунарство

Ужа научна област: Дискретна математика

УДК број: 004.415.5(043.3)

Dissertation title: Counting equivalence classes of Boolean functions

Abstract: In this dissertation, the problem of calculating the number of equivalence classes of Boolean functions is discussed. The difficulty of determining the number of equivalence classes increases sharply with the number of variables n. The motivation for choosing this topic lies in the fact that concrete numbers have been known so far only for relatively small values of n, although the problem itself was theoretically solved a long time ago.

Let G be the group of permutations of the set $B_n = \{0,1\}^n$. The effect of the group G on scalar, $B_n \mapsto B_1$, that is, vectorial invertible Boolean functions, $B_n \mapsto B_n$. Two scalar Boolean functions $f(x)$ and $g(x)$, defined on B_n, are considered equivalent with respect to the group G, i.e. $f \sim g$, if for some $\sigma \in G$ for every $x \in B_n$ $f(x) = g(\sigma(x))$ holds. Two vector invertible Boolean functions $f(x)$ and $g(x)$, are considered equivalent with respect to the group G, i.e. $f \sim g$, if for some pair $(\sigma, \rho) \in G \times G$ for each $x \in B_n$ holds $g(x) = \rho(f(\sigma(x)))$. The equivalence relation $\sim$ decomposes the set of all Boolean functions into equivalence classes. Equivalence of Boolean functions has significant applications in the logical synthesis of combinatorial circuits and in cryptography, especially in connection with the design of S-boxes.

Let $U_n(G)$ and $V_n(G)$ denote number of equivalence classes of scalar, i.e. vector invertible Boolean functions of n variables in relation to the group G. The numbers $U_n(G)$ and $V_n(G)$ can be calculated relatively simply if the cycle index of the group G is known. The dissertation considers four groups G of permutations of the set B_n:

- group S'_n induced by group S_n permutations of coordinates elements $x = (x_1, x_2, \ldots, x_n) \in B_n$,
- group G_n, induced by permutations and complementations of coordinates,
- group of GL_n linear invertible transformations elements of the vector space B_n, i
- group of AGL_n affine invertible transformations elements B_n.

If the permutation $\sigma \in G$ has i_k cycles of length $k \geqslant 1$, its cycle structure is

$i(\sigma) = (i_1, i_2, \ldots)$. The cyclic index of the group G is the generatrix

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

of cycle structures of all permutations $\sigma \in G$. General expressions for cycle indices the four considered groups are known, but the cycle indices themselves, i.e. the numbers $U_n(G)$ and $V_n(G)$, are practically calculated only for relatively small values, for e.g. $n \leqslant 10$.

The dissertation presents original results in the field of enumeration of equivalence classes of Boolean functions in relation to these four groups of transformations. A similar expression was derived for all four groups of transformations for the cycle index in the form of sum over partitions of the number n. Based on that expression and previously calculated tables, the cycle index is calculated much more efficiently. An overview of known results for relatively small n and new results in the thesis for larger n is shown in the following table:

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

Specially, in the case of the permutation group S'_n, an effective direct procedure for calculating the number of equivalence classes that does not use a cycle index is shown, and is described in the third paper from the introductory chapter.

The second part of the dissertation concerns monotone Boolean functions — scalar Boolean functions which satisfy the monotonicity condition (from $x \leqslant y$ follows $f(x) \leqslant f(y)$). Let r_n, i.e. d_n (the n-th Dedekind number), denote the number of equivalence classes of monotone Boolean functions in relation to the group S'_n, that is, the total number of monotone Boolean functions of n variables. The difficulty of calculating the number r_n increases rapidly with n, so that until recently the last calculated member of the sequence was r_7. The procedure described in the dissertation is based on the Frobenius theorem, by which it was determined number r_8. In doing so, the known value of the number d_8 is used.

The dissertation consists of the first - introductory chapter and the following three chapters. In the second chapter, theoretical terms related to the material from chapters 3 and 4 are introduced, and they refer to discrete mathematics, combinatorics and cycle indices of the considered four groups of transformations.

Chapter 3 describes the procedure for calculating the cycle indices for the four considered groups of permutations, as well as numbers $U_n(G)$ and $V_n(G)$ equivalence classes of Boolean functions in relation to these groups. First, common improvements for all four groups are considered, and then specific accelerations related to individual groups. These results are published in the second paper listed in the introductory chapter.

In chapter 4, the problem of finding the number of equivalence classes of monotone Boolean functions is solved. First, a general expression for calculating the number r_n is given based on the Frobenius theorem in the form of the sum (by partitions of the number n) of the number of fixed points of the permutation corresponding to the partition. After that, depending on the graphs corresponding to different partitions, different ways of calculating the number of fixed points for $n \leqslant 8$ are shown. The procedure based on which the number r_8 was calculated, which also represents the original contribution of this dissertation is presented - see the first paper from the list from the introductory chapter. Applying a similar procedure, Pawelski [31] calculated r_8 practically at the same time as the obtained result described in the dissertation.

Keywords: Boolean functions, monotone Boolean functions, partitions, cyclic index, Frobenius theorem, Dedekind numbers

Research area: Computer science

Research sub-area: Discrete mathematics

UDC number: 004.415.5(043.3)

Захвалница

Желео бих да се захвалим ментору професору др Миодрагу Живковићу на свему што сам од њега научио. Захвалан сам члановима комисије, професорима, др Филипу Марићу, др Весни Маринковић и др Радету Живаљевићу на корисним сугестијама које су допринеле унапређењу овог рукописа. Дугујем велику захвалност мојим родитељима Зоји и Мирку, који су ме увек подржавали у жељи за стицањем нових сазнања. Захвалио бих се такође свима који су ме охрабривали да завршим рад на овој дисертацији, а посебно мојој супрузи Катарини и ћеркама Марији и Зоји.

Садржај

Глава 1

Увод

Многи проблеми пребројавања, а нарочито они код којих међу посматраним објектима има „сличних", тешко би се могли замислити без примене теорије група [10]. Нека је X произвољан коначан скуп, а $G = S_X$ група узајамно једнозначних трансформација $X \to X$ (пермутација) које на њега делују. Група S_X зове се симетрична група скупа X; ако је $|X| = n$, онда се уместо S_X користи ознака S_n, а група се зове симетрична група *степена* n. Елементи $x, y \in X$ су слични (еквивалентни) ако постоји транформација $\sigma \in G$ таква да је $\sigma(x) = y$. Пошто је сличност релација еквиваленције, дејство групе G разлаже скуп X на класе еквиваленције, *орбите*.

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

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

циклусних структура свих пермутација $\sigma \in G$.

У овом раду разматрају се четири групе G пермутација скупа $B_n = \{0, 1\}^n$:

- 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 инвертибилних трансформација елемената векторског простора B_n, и

- група AGL_n инвертибилних трансформација елемената B_n и комплементирања координата.

Разматрају се три врсте Булових функција дефинисаних на скупу B_n:

- скаларне, $B_n \mapsto B_1$,
- векторске инвертибилне, $B_n \mapsto B_n$, и
- мононотоне — скаларне функције које задовољавају услов монотоности: $x \leqslant y \Rightarrow f(x) \leqslant f(y)$.

У следећој табели приказан је пример векторске инвертибилне функције $f : B_3 \mapsto B_3$,

$$y = (y_1, y_2, y_3) = f(x) = f(x_1, x_2, x_3)$$

и њене инверзне функције $x = f^{-1}(y)$.

x_1	x_2	x_3	y_1	y_2	y_3	y_1	y_2	y_3	x_1	x_2	x_3
0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	1	0	1	1
0	1	0	0	1	0	0	1	0	0	1	0
0	1	1	0	0	1	0	1	1	0	0	1
1	0	0	1	0	0	1	0	0	1	0	0
1	0	1	1	1	0	1	0	1	1	1	1
1	1	0	1	1	1	1	1	0	1	0	1
1	1	1	1	0	1	1	1	1	1	1	0

Скаларна функција $y_1 = f_1(x)$ је монотона, а скаларна функција $y_2 = f_2(x)$ није монотона, јер је на пример $(1,1,0) \leqslant (1,1,1)$ и $f_2(1,1,0) = 1 > 0 = f_2(1,1,1)$.

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 векторски инвертибилне Булове функције $f(x)$ и $g(x)$, дефинисане на B_n, 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 (сва три типа) у класе еквиваленције. Нека $U_n(G)$, односно $V_n(G)$ означава број класа еквиваленције скаларних, односно векторских инвертибилних Булових функција од n променљивих. Бројеви $U_n(G)$ и $V_n(G)$ могу

се релативно једноставно израчунати ако се зна циклусни индекс групе G. Инспирисан претходним радовима [2, 5, 32, 34, 36], Харисон (Harrison) је у радовима [22, 23] извео опште изразе за циклусне индексе за S'_n, G_n, GL_n и AGL_n и експлицитно их израчунао за $n \leqslant 6$. Лоренс (Lorens)[20, 21] је израчунао број класа еквиваленције инвертибилних Булових функција за ове четири групе трансформација за $n \leqslant 5$. Полазећи од изоморфизма између AGL_n и групе пермутација, Чанг (Zhang) и остали [41] израчунали су $U_n(\mathrm{AGL}_n)$ за $n \leqslant 10$. Већина до сада израчунатих бројева $U_n(G)$ и $V_n(G)$ могу се пронаћи у Енциклопедији целобројних низова (OEIS [30]). Горње границе за индексе израчунатих бројева, кодови одговарајућих низова у OEIS и референце на евентуалне радове у оквиру којих је израчунато више чланова низа него у OEIS приказане су у табели 1.1.

Табела 1.1: Горње границе за индексе израчунатих бројева $U_n(G)$ и $V_n(G)$ и њихови кодови у Енциклопедији целобројних низова (OEIS [30]).

Низ \ G	S'_n	G_n	GL_n	AGL_n
$U_n(G)$	11 ([19], A003180)	10 ([19], A000616)	8 (A000585)	10 ([41], A000214)
$V_n(G)$	6 (A000653)	7 (A000654)	6 (A001038)	6 (A001537)

Треба напоменути да је Фрипертингер (Fripertinger) ([15]) имплементирао рачунање циклусног индекса за GL_n и AGL_n у оквиру програмског пакета SYMMETRICA, уз приказ времена израчунавања за $n \leqslant 17$. Наша верзија Фрипертингеровог програма рачуна циклусни индекс за $n \leqslant 21$. Користећи овај резултат није тешко израчунати $U_n(G)$ и $V_n(G)$ за GL_n и AGL_n за веће n од приказаних у табели 1.1.

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. Дедекиндове бројеве d_7 и d_8 израчунали су Берман (Berman) и Келер (Köhler) [3] и Видеман (Wiedemann) [40], користећи сличан приступ. Чучанг (Chuchang) и Шобен (Shoben) [28, 29] израчунали су r_7 користећи Фробенијусову теорему. Стивен (Stephen) и Јусун (Yusun) [37] потврдили су резултат за r_7 користећи други приступ. Познато је да је Булова функција $f \in \mathcal{B}_n$ монотона ако и само ако се у запису њене дисјунктивне нормалне форме не појављују негације. Профил монотоне Булове функције $f \in \mathcal{B}_n$ је вектор $(p_1, \ldots, p_n)$, где је p_k број

конјукција од k променљивих у оквиру DNF функције f. Стивен и Јусун су израчунали r_7, разлагањем скупа $\mathcal{D}_7$ према профилима монотоних Булових функција. Применивши Фробенијусову теорему Павелски (Pawelski) [31] је израчунао r_8, практично у исто време када је добијен и наш резултат.

Дисертација је састављена из три дела. У поглављу 2 дат је преглед теорије потребан за разумевање идеја из којих су проистекли новодобијени резултати. У поглављу 3 приказан је начин добијања броја класа еквиваленције Булових и инвертибилних Булових функција за битно веће вредности од постојећих. У поглављу 4 приказан је нови начин рачунања броја класа еквиваленције монотоних Булових функција.

Резултати из области дисертације објављени су у радовима:

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.

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.

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).

Глава 2

Основни појмови и теореме

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

2.1 Дискретна математика

У овом одељку уводе се теоријски појмови везани за партиције, групе и Булове функције. Додатно, као основа за поглавље 3, уводе се појмови везани за коначна поља, полиноме, матрице и векторске просторе. Као основа за поглавље 4, уводе се појмови везани за графове.

2.1.1 Партиције

У теорији бројева и комбинаторици, *партиција* позитивног целог броја n, је начин записа броја n као збира позитивних целих бројева. Два збира која се разликују само по редоследу својих сабирака сматрају се истом партицијом; ако је редослед сабирака битан, збир постаје *композиција*. На пример, 4 се може поделити на пет различитих начина:
4
$3 + 1$
$2 + 2$
$2 + 1 + 1$
$1 + 1 + 1 + 1$
При томе, две различите композиције $1 + 2 + 1$ и $1 + 1 + 2$ представљају исту

партицију $2+1+1$. Нека је P_n скуп партиција броја n, $n = a_1 + a_2 + \ldots + a_k$, $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_k > 0$.

Нека $P(n,k)$ и $\overline{P}(n,k)$ означавају редом скуп партиција броја n од највише k сабирака и од тачно k сабирака: специјално, $P(n,n) = P_n$. Партиције броја n од највише k сабирака могу се разложити на два скупа: скуп партиција од тачно k сабирака и скуп партиција од највише $k-1$ сабирака, па важи следеће разлагање у дисјунктну унију

$$P(n,k) = \overline{P}(n,k) \cup P(n,k-1),\ 1 \leqslant k \leqslant n.$$

Нека је $p(n,k) = |P(n,k)|$ и $\overline{p}(n,k) = |\overline{P}(n,k)|$. Ови бројеви задовољавају рекурентну релацију

$$p(n,k) = \overline{p}(n,k) + p(n,k-1),\ 1 \leqslant k \leqslant n \tag{2.1}$$

уз почетне услове $p(n,1) = \overline{p}(n,1) = 1$. У табелама 2.1 и 2.2 приказане су вредности $\overline{p}(n,k)$ и $p(n,k)$ за $n \leqslant 9$.

Табела 2.1: Број партиција броја $n \leqslant 9$ од тачно k сабирака.

k \ n	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1
2		1	1	2	2	3	3	4	4
3			1	1	2	3	4	5	7
4				1	1	2	3	5	6
5					1	1	2	3	5
6						1	1	2	3
7							1	1	2
8								1	1
9									1

Табела 2.2: Број партиција броја $n \leqslant 9$ од највише k сабирака.

k \ n	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1
2		2	2	3	3	4	4	5	5
3			3	4	5	7	8	10	12
4				5	6	9	11	15	19
5					7	10	13	18	24
6						11	14	20	27
7							15	21	28
8								22	29
9									30

На пример, партиције броја 3 од највише 2 сабирка су: 3 и $2+1$; партиција броја 3 од тачно 2 сабирка је само $2+1$. Одузимањем броја 1 од сваког сабирка из партиција скупа $\overline{P}(n,k)$ добија се скуп $P(n-k,k)$. Обрнуто, додавањем броја 1 сваком сабирку из скупа $P(n-k,k)$ добија се скуп $\overline{P}(n,k)$. На пример, партиције скупа $\overline{P}(5,3)$ су $3+1+1$ и $2+2+1$. Одузимањем броја 1 од сваког сабирка добијају се партиције скупа $P(2,3)$: 2 и $1+1$. Комбиновањем са изразом (2.1) долази се до рекурентне релације:

$$p(n,k) = p(n-k,k) + p(n,k-1),\ 1 \leqslant k \leqslant n. \tag{2.2}$$

Даљим рекурзивним разлагањем другог сабирка добија се:

$$p(n,k) = \sum_{i=1}^{k} p(n-i,i),\ 1 \leqslant k \leqslant n.$$

Скуп $\overline{P}(n,k)$ се може поделити на два скупа: скуп партиција међу којима се налази сабирак 1 и скуп партиција без сабирка 1. Елиминацијом једног сабирка 1 из партиција првог скупа добија се скуп $\overline{P}(n-1,k-1)$. Одузимањем броја 1 од сваког сабирка из партиција другог скупа добија се скуп $\overline{P}(n-k,k)$, при чему важи и обрнуто тврђење. Дакле, важи:

$$\overline{p}(n,k) = \overline{p}(n-k,k) + \overline{p}(n-1,k-1),\ 1 \leqslant k \leqslant n.$$

Произвољна партиција $n = a_1 + a_2 + \ldots + a_k$ једнозначно је представљена вектором $p = (p_1, p_2, \ldots, p_n) \in P_n$, где је $p_i = |\{j \mid a_j = i|\}$. На пример, за

$n = 4$, вектор $(2, 1, 0, 0)$ придружен је партицији $2 + 1 + 1$. У даљем тексту ће

$$P_n = \{(p_1, p_2, \ldots, p_n) \mid \sum_{i=1}^{n} ip_i = n\} \tag{2.3}$$

истовремено означавати и скуп придружен партицијама броја $n \geqslant 1$; погодности ради, нека је $P_0 = \{(0)\}$.

2.1.2 Групе

Алгебарска структура је непразан скуп у коме су дефинисане извесне операције које задовољавају задата својства. Алгебарска структура са једном бинарном операцијом назива се *групоид*. Ако скуп означимо са X, а бинарну операцију са $\cdot$, одговарајући групоид означава се као уређен пар $G = (X, \cdot)$.

Дефиниција 2.1.1. *Групоид $G = (X, \cdot)$ назива се група ако су испуњени следећи услови:*

- $(\forall a, b, c \in X),\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$, *(асоцијативност)*
- $(\exists e \in X)(\forall a \in X),\ e \cdot a = a \cdot e = a$, *(постојање неутралног елемента)*
- $(\forall a \in X)(\exists a^{-1} \in X),\ a \cdot a^{-1} = a^{-1} \cdot a = e$. *(постојање инверзног елемента)*

Пример 2.1.1. *Нека је $Z_m = \{0, 1, ..., m - 1\}$ и нека је операција $+$ сабирање по модулу m. Тада је $(Z, +)$ група.*

Дефиниција 2.1.2. *Ред $|G|$ групе G је број њених елемената.*

Пример 2.1.2. *Нека су темена квадрата из скупа $\{1, 2, 3, 4\}$. Ротације и рефлексије квадрата, заједно са операцијом композиције чине диедарску групу D_4, $|D_4| = 8$.*

Табела 2.3: Елементи диедарске групе D_4.

идентичка трансформација (ротација за 0°)	R_0
ротација за 90°	R_{90}
ротација за 180°	R_{180}
ротација за 270°	R_{270}
рефлексија око дијагонале 13	D
рефлексија око дијагонале 24	D'
рефлексија око средина страница 12 и 34	H
рефлексија око средина страница 14 и 23	V

Дефиниција 2.1.3. *Ако за групе* $(G, \cdot)$ *и* $(H, \cdot)$ *важи* $H \subseteq G$*, онда је* H *подгрупа групе* G*.*

Дефиниција 2.1.4. *За подгрупу* H *групе* G *и било које* $a \in G$*,* $a \circ H = \{x | x = a \circ h$ *за неко* h *из* $H\}$ *је леви разред (косет) подгрупе* H *у* G*. Аналогно се дефинише десни разред.*

Пример 2.1.3. *Нека је* G *група са операцијом сабирања над скупом целих бројева,* $\mathbb{Z} = (\{\ldots, -2, -1, 0, 1, 2, \ldots\}, +)$ *и нека је* H *њена подгрупа* $(3\mathbb{Z}, +) = (\ldots, -6, -3, 0, 3, 6, \ldots, +)$*. Тада су разреди подгрупе* H *групе* G *скупови* $3\mathbb{Z}, 3\mathbb{Z}+1$ *и* $3\mathbb{Z}+2$*, где је* $3\mathbb{Z}+a = \ldots, -6+a, -3+a, a, 3+a, 6+a, \ldots$*. Ова три скупа разлажу скуп* $\mathbb{Z}$*, па покривају све десне разреде подгрупе* H*. Због комутативности сабирања важи* $H+1 = 1+H$ *и* $H+2 = 2+H$*. Дакле, у овом случају, сваки десни разред истовремено је и леви разред подгрупе* H*.*

Скуп свих разреда подгрупе H групе G чини *количничку групу* $G : H$.

Дефиниција 2.1.5. *Број левих (десних) разреда подгрупе* H *групе* G *назива се индекс подгрупе* H *групе* G*, у ознаци* $[G : H]$*.*

Теорема 2.1.1. *(Лагранж, Lagrange) Ако је* G *коначна група и ако је* H *подгрупа групе* G*, тада* $|H||G|$ *и важи* $[G : H] = |G|/|H|$*.*

Дефиниција 2.1.6. *Пресликавање* $f : G \mapsto H$ *назива се хомоморфизам групе* $(G, \cdot)$ *на групу* $(H, \times)$ *ако важи*

$$(\forall x, y \in G)\ f(x \cdot y) = f(x) \times f(y).$$

Мономорфизам, епиморфизам и *изоморфизам*, представљају редом инјективни, сурјективни и бијективни хомоморфизам. Изоморфизам групе на саму себе назива се *аутоморфизам*. Хомоморфизам групе на неки њен део назива се *ендоморфизам*.

Дефиниција 2.1.7. *Централизатор елемента* x *групе* G *дефинише се изразом*

$$C_G(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}.$$

Централизатор C_G је подгрупа групе G.

Пример 2.1.4. *Постоје четири централизатора - подгрупе групе* D_4*:*

$C(R_0) = D_4 = C(R_{180})$
$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270})$
$C(H) = \{R_0, H, R_{180}, V\} = C(V)$
$C(D) = \{R_0, D, R_{180}, D'\} = C(D')$

Бијективно пресликавање скупа X на себе, назива се *пермутација* скупа X. *Композиција* две пермутације $\sigma \circ \rho$ је пермутација која елементе $x \in X$ пресликава у елементе $\sigma(\rho(x))$. Композиција је асоцијативна операција, па се у запису композиције пермутација могу изоставити заграде. У општем случају, композиција две пермутације није комутативна операција.

Скуп свих пермутација коначног скупа X са операцијом композиције пресликавања је група S_X, *симетрична група* скупа X. Уколико је $|X| = n$, уместо S_X користи се и ознака S_n за симетричну групу *степена* n. Свака подгрупа групе S_X назива се *група пермутација*.

Пермутација скупа величине n може се представити матрицом $2 \times n$, чија се прва врста састоји од оригинала, а друга од одговарајућих слика. Тако на пример, пермутација

$$\begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \end{pmatrix} \tag{2.4}$$

одговара бијекцији скупа $X = \{a, b, c, d, e\}$ на себе самог и пресликава елементе $a \to b,\ b \to c,\ c \to d,\ d \to e,\ e \to a$. Пермутација облика

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ a_2 & a_3 & \cdots & a_k & a_1 \end{pmatrix}, \tag{2.5}$$

чини *циклус* дужине k и представља се изразом $(a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$. Пермутација из претходног примера управо је овог облика; чини циклус $(a\ b\ c\ d\ e)$ дужине 5, односно представља *цикличну* пермутацију. Циклус дужине k има k еквивалентних записа. На пример, циклус $(a\ b\ c\ d\ e)$ може се написати и у облику $(b\ c\ d\ e\ a)$. Произвољна пермутација скупа X разлаже се у производ (композицију) дисјунктних циклуса. Елементи скупа које пермутација пресликава у себе саме су *фиксне тачке* пермутације и припадају циклусима дужине један.

Пример 2.1.5. *Пермутација*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = (1\ 2)(3)(4\ 5\ 6)$$

је производ три циклуса: једног дужине два, једног дужине три и једне фиксне тачке. Елементи у овим циклусима су дисјунктни подскупови скупа X и чине једно разлагање скупа X. Уобичајено је да се приликом записа пермутације циклуси дужине 1 *изостављају.*

Две композиције пермутација $a = (1\ 3\ 5\ 2)$ и $b = (1\ 6\ 3\ 4)$ су различите

$$a \circ b = (1\ 6\ 5\ 2)(3\ 4),$$

$$b \circ a = (1\ 4)(2\ 6\ 3\ 5).$$

Дефиниција 2.1.8. *Нека је G група пермутација скупа X. За сваки елемент $i \in X$, стабилизатор елемента i групе G је*

$$\mathrm{stab}_G(i) = \{g \in G \mid g(i) = i\}$$

Стабилизатор stab_G је подгрупа групе G.

Ако се $\sigma \in S_n$ састоји од p_i циклуса дужине i, $1 \leqslant i \leqslant n$, кажемо да је тип пермутације σ једнак $p = \mathrm{type}(\sigma) = (p_1, p_2, \ldots, p_n) \in P_n$. Партиција $p \in P_n$ може се представити полиномом $f^p = \prod_{i=1}^{M} f_i^{p_i}$, где су f_1, f_2, $\ldots$ f_M независне променљиве, а M горња граница дужина циклуса пермутације σ. У складу са (2.3), у наставку се користе ова три еквивалентна формата партиција (нерастући низ сабирака $(a_1, a_2, \ldots, a_k)$, p и f^p).

Нека је $B_n = \{0,1\}^n$ и $N = 2^n$ за $n \geqslant 1$. Нека $[a..b]$ означава скуп $\{a, a+1, \ldots, b\}$. Пермутација $\sigma \in S_n$ која пермутује n симбола $x_1, x_2, ..., x_n$, једнозначно одређује (индукује) пермутацију σ' која n-торку $x = (x_1, ..., x_n) \in B_n$ пресликава у n-торку $\sigma'(x) = (x_{\sigma(1)}, ..., x_{\sigma(n)}) \in B_n$. Ако се n-торке $x = (x_1, x_2, \ldots, x_n) \in B_n$ кодирају бројевима $X = \sum_{i=1}^{n} x_i 2^{n-i}$, онда важи $\sigma'(X) = Y = \sum_{i=1}^{n} y_i 2^{n-i}$, где је $y = \sigma(x)$. Нека је S'_n група коју чине све пермутације σ' које одговарају пермутацијама $\sigma \in S_n$. Нека $w(x) = \sum_{i=1}^{n} x_i$ означава *Хемингову* (Hamming) *тежину* низа $x \in B_n$. Пошто пермутација $\sigma' \in S'_n$ само пермутује компоненте n-торке x на коју делује, увек важи $w(\sigma'(x)) = w(x)$.

Пример 2.1.6. *За $n = 3$ и $\sigma = (1\ 2)$, пермутација σ' замењује прве две компоненте бинарне тројке, па је*

$$\sigma' = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 & 7 \end{pmatrix} = (0)(1)(2\ 4)(3\ 5)(6)(7).$$

Пермутација σ' пресликава $5 = (1,0,1)$ у $3 = (0,1,1)$, па је $w(5) = w(3)$.

Пример 2.1.7. *Настављајући претходни пример, за* $n = 3$ *и* $\sigma = (1\ 2)$*, је* $\mathrm{type}(\sigma) = (1, 1, 0)$ *(пермутација* σ *састоји се од једног циклуса* (3) *дужине* 1*, једног циклуса* $(1\ 2)$ *дужине* 2 *и без циклуса дужине* 3*). Пермутација* σ' *има четири циклуса дужине* 1 *и два циклуса дужине* 2*, што одговара разлагању* $3 = 2 + 1$*. Због тога је* $\mathrm{type}(\sigma') = (4, 2, 0, 0, 0, 0, 0, 0)$*, што се може представити циклусном структуром* $f^{\mathrm{type}(\sigma')} = f_1^4 f_2^2$*.*

Дефиниција 2.1.9. *Нека је* G *група пермутација над скупом* X*. За сваки елемент* $x \in X$*, нека је* $\mathrm{orb}_G(x) = \{\sigma(x) | \sigma \in G\}$*. Скуп* $\mathrm{orb}_G(x) \subseteq X$ *назива се орбита елемента* x *у односу на групу* G*.*

У претходној дефиницији, индекс G може се изоставити када је јасно о којој групи се ради.

Група G делује на себе *конјугацијом* ако се сваком $g \in G$ придружи пресликавање $\alpha_g : G \to G$, $\alpha_g(x) = gxg^{-1}$. За $x \in G$ *конјугациона класа* елемента x дефинише се изразом

$$x^G = \{y \in G \mid y = gxg^{-1} \text{ за неко } g \in G\}.$$

Приметимо да овде важи $x^G = \mathrm{orb}(x)$ и $\mathrm{stab}_G(x) = C_G(x)$. Све пермутације (дејства) које припадају истој конјугационој класи имају исту циклусну структуру.

Теорема 2.1.2. *Нека је* G *група пермутација скупа* X*. Тада, за свако* $i \in X$ *важи*

$$|G| = |\mathrm{orb}_G(i)||\mathrm{stab}_G(i)|.$$

Доказ. На основу Лагранжове теореме, $|G|/|\mathrm{stab}_G(i)|$ је број различитих левих разреда подгрупе $\mathrm{stab}_G(i)$ групе G. Зато је довољно успоставити бијекцију између левих разреда подгрупе $\mathrm{stab}_G(i)$ и елемената орбите $\mathrm{orb}_G(i)$. Нека је T пресликавање које за произвољно $\phi \in G$ разреду $\phi\,\mathrm{stab}_G(i)$ придружује елеменат орбите $\phi(i)$. Пресликавање T је добро дефинисано, пошто из $\alpha\,\mathrm{stab}_G(i) = \beta\,\mathrm{stab}_G(i)$ следи $\alpha^{-1}\beta \in \mathrm{stab}_G(i)$, $(\alpha^{-1}\beta)(i) = i$ и према томе $\alpha(i) = \beta(i)$. Претходни низ корака у обрнутом редоследу показује да је T 1-1 пресликавање. Нека је $j \in \mathrm{orb}_G(i)$. Тада је $\alpha(i) = j$ за неко $\alpha \in G$ и важи $T(\alpha\,\mathrm{stab}_G(i)) = \alpha(i) = j$ па је T такође и „на" пресликавање. □

Последица 2.1.1. *За свако* $x \in G$ *важи једнакост*

$$|x^G| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

Доказ. Доказ следи из Лагранжове теореме (теорема 2.1.1) и из једнакости $x^G = \mathrm{orb}(x)$ и $\mathrm{stab}_G(x) = C_G(x)$. □

Лема 2.1.1. *Ако је (векторска инвертибилна функција од n променљивих) F фиксна тачка трансформације одређене паром пермутација (σ, ρ), и ако је $(X_1 \cdots X_k)$ циклус пермутације σ (тј. $\sigma(X_i) = X_{i+1}, i = 1, 2, ..., k-1, \sigma(X_k) = X_1$), онда сви елементи $F(X_i)$ у бинарном запису имају исти број јединица.*

Доказ. $F(X_i) = \rho(F(\sigma(X_i)) = \rho(F(X_{i+1})$, па $F(X_i)$ и $F(X_{i+1})$ имају исти број јединица. □

2.1.3 Декартов производ пермутација

У овој тачки дефинише се Декартов производ две или више пермутација, и оператор $\times$ који циклусну структуру Декартовог производа пермутација изражава преко циклусних структура аргумената.

Дефиниција 2.1.10. *Нека је α_i пермутација скупа Z_i, $1 \leqslant i \leqslant n$. Декартов производ $(\alpha_1, \ldots, \alpha_n)$ пермутација $\alpha_1, \ldots, \alpha_n$ је пермутација скупа $Z_1 \times Z_2 \times \cdots \times Z_n$ дефинисана једнакошћу:*

$$(\alpha_1, \ldots, \alpha_n)(z_1, \ldots, z_n) = (\alpha_1(z_1), \ldots, \alpha_n(z_n))$$

Нека $\langle p, q\rangle$ и (p, q) редом означавају најмањи заједнички садржалац и највећи заједнички делилац бројева p и q.

Теорема 2.1.3. *Нека су пермутације $\alpha = (a_1, \ldots, a_p)$ и $\beta = (b_1, \ldots, b_q)$ редом циклуси дужине p и q. Тада је циклусна структура пермутације (α, β) дата изразом*

$$f^{(p,q)}_{\langle p,q\rangle}.$$

Доказ. За $p = q$ тврђење следи директно из дефиниције. Циклусна структура пермутације (α, β) је $f^p_p = f^{(p,p)}_{\langle p,p\rangle}$, пошто елемент x из X може бити у пару са било којим елементом y из Y, следбеник x у пару са следбеником y, ... Резултат је циклус дужине p и то важи за све могуће парове (x, y) за фиксирано x. Без смањења општости претпоставимо да је $p < q$. Ако произвољно изаберемо елемент (a_1, b_1), резултат је циклус

$$(a_1, b_1) \to (a_2, b_2) \to \cdots (a_p, b_p) \to (a_1, b_{p+1}) \to \cdots \to (a_p, b_q)$$

дужине $\langle p,q\rangle(p,q)$. Пошто се пермутује pq елемената и пошто важи

$$pq = \langle p,q\rangle(p,q)$$

из чињенице да у једном циклусу постоји $\langle p,q\rangle$ елемената следи да постоји (p,q) таквих циклуса. □

Пример 2.1.8. *Декартов производ два циклуса* $(a\ b)\times(c\ d\ e)$ *је пермутација - циклус дужине* 6*:*

$$(a\ b)\times(c\ d\ e) = \big\{\{a,c\},\{b,d\},\{a,e\},\{b,c\},\{a,d\},\{b,e\}\big\}.$$

Циклусна структура Декартовог производа $(a\ b)\times(c\ d\ e)$ *је дакле* f_6*.*

Нека $\langle z_1,z_2,\ldots,z_n\rangle$ и $(z_1,z_2,\ldots,z_n)$ редом означавају најмањи заједнички садржалац и највећи заједнички делилац бројева $z_1,z_2,\ldots,z_n$.

Теорема 2.1.4. *Нека је* α_i *пермутација скупа* Z_i*, са циклусном структуром* $f_{x_i}^{y_i}$*,* $i=1,\ldots,n$*. Декартов производ* $(\alpha_1,\ldots,\alpha_n)$ *има циклусну структуру*

$$f^{\prod_{i=1}^{n}(x_iy_i)/\langle x_1,x_2,\ldots,x_n\rangle}_{\langle x_1,x_2,\ldots,x_n\rangle}$$

Доказ. Доказ се изводи индукцијом по n. За $n=2$ Декартов производ (α_1,α_2) на основу теореме 2.1.3 има циклусну структуру $f^{y_1y_2(x_1,x_2)}_{\langle x_1,x_2\rangle}$. Претпоставимо да је тврђење тачно за неко $n=k>1$ тј. пермутација $(\alpha_1,\ldots,\alpha_n)$ има циклусну структуру

$$f^{\prod_{i=1}^{k}(x_iy_i)/\langle x_1,x_2,\ldots,x_k\rangle}_{\langle x_1,x_2,\ldots,x_k\rangle}.$$

Тада је циклусна структура Декартовог производа $(\alpha_1,\ldots,\alpha_n,\alpha_{n+1})$ једнака циклусној структури Декартовог производа две пермутације са циклусним структурама $f^{\prod_{i=1}^{k}(x_iy_i)/\langle x_1,x_2,\ldots,x_k\rangle}_{\langle x_1,x_2,\ldots,x_k\rangle}$ и $f^{y_{k+1}}_{x_{k+1}}$, па је једнака

$$\begin{aligned}
& f^{(\langle x_1,x_2,\ldots,x_k\rangle,x_{k+1})y_{k+1}\prod_{i=1}^{k}(x_iy_i)/\langle x_1,x_2,\ldots,x_k\rangle}_{\langle\langle x_1,x_2,\ldots,x_k\rangle,x_{k+1}\rangle} = \\
= \ & f^{[\langle x_1,x_2,\ldots,x_k\rangle x_{k+1}/\langle\langle x_1,x_2,\ldots,x_k\rangle,x_{k+1}\rangle]y_{k+1}\prod_{i=1}^{k}(x_iy_i)/\langle x_1,x_2,\ldots,x_k\rangle}_{\langle x_1,x_2,\ldots,x_{k+1}\rangle} = \\
= \ & f^{[\langle x_1,x_2,\ldots,x_k\rangle/\langle x_1,x_2,\ldots,x_{k+1}\rangle]x_{k+1}y_{k+1}\prod_{i=1}^{k}(x_iy_i)/\langle x_1,x_2,\ldots,x_k\rangle}_{\langle x_1,x_2,\ldots,x_{k+1}\rangle} = \\
= \ & f^{\prod_{i=1}^{k+1}(x_iy_i)/\langle x_1,x_2,\ldots,x_{k+1}\rangle}_{\langle x_1,x_2,\ldots,x_{k+1}\rangle}
\end{aligned}$$

□

Теорема 2.1.5. *Нека је α пермутација скупа X, $|X| = a$, са циклусном структуром $f_1^{j_1} \cdots f_a^{j_a}$ и нека је β пермутација скупа Y, $|Y| = b$, са циклусном структуром $f_1^{k_1} \cdots f_b^{k_b}$. Пермутација (α, β) има циклусну структуру*

$$\prod_{p=1}^{a} \prod_{q=1}^{b} f_{\langle p,q \rangle}^{j_p k_q (p,q)} \tag{2.6}$$

Доказ. Доказ следи из особине Декартовог производа и теореме 2.1.3. □

Теорема 2.1.5 може се уопштити:

Теорема 2.1.6. *Нека је α_i пермутација скупа Z_i, $|Z_i| = k_i, i = 1, \ldots, n$ са циклусном структуром $f_1^{y_{z_1}} \cdots f_{k_i}^{y_{z_{k_i}}}$. Пермутација $(\alpha_1, \ldots, \alpha_n)$ има циклусну структуру*

$$\prod_{z_1=1}^{k_1} \prod_{z_2=1}^{k_2} \cdots \prod_{z_n=1}^{k_n} f_{<z_1,z_2,\ldots,z_n>}^{\prod_{i=1}^{n}(z_i y_{i,z_i})/<z_1,z_2,\ldots,z_n>}$$

Доказ. Доказ се изводи индукцијом на основу теорема 2.1.4 и 2.1.5. □

Дефиниција 2.1.11. *Нека је α_i пермутација скупа Z_i са циклусном структуром F_i, $i = 1, \ldots, n$. Операција $\times$ (крст) над циклусним структурама дефинисана је условом да је циклусна структура пермутације $(\alpha_1, \ldots, \alpha_n)$ једнака $\times_{i=1}^{n} F_i$.*

Циклусна структура пермутације $(\alpha_1, \ldots, \alpha_n)$ једнозначно је одређена циклусним структурама пермутација $\alpha_1, \ldots, \alpha_n$, па је ова дефиниција исправна. Следећа последица теореме 2.1.6 прецизира начин рачунања са оператором $\times$.

Последица 2.1.2.

$$\prod_{z_1=1}^{k_1} \prod_{z_2=1}^{k_2} \cdots \prod_{z_n=1}^{k_n} \bigtimes_{i=1}^{n} f_{z_i}^{y_{i,z_i}} = \prod_{z_1=1}^{k_1} \prod_{z_2=1}^{k_2} \cdots \prod_{z_n=1}^{k_n} f_{<z_1,z_2,\ldots,z_n>}^{\prod_{i=1}^{n}(z_i y_{i,z_i})/<z_1,z_2,\ldots,z_n>}$$

Специјално важи:

$$f_p^j \times f_q^k = f_{\langle p,q \rangle}^{jk(p,q)}. \tag{2.7}$$

2.1.4 Коначна поља и полиноми

Дефиниција 2.1.12. *Алгебарска структура $(S, +, \cdot)$, где су $+$ и $\cdot$ бинарне операције скупа S, назива се поље, ако су испуњени следећи услови:*

- *$(S, +)$ је група,*
- *бинарне операције $+$ и $\cdot$ су комутативне,*
- *операција $\cdot$ је дистрибутивна према операцији $+$,*
- *структура $(S\backslash\{0\}, \cdot)$, где је 0 неутрални елемент групе $(S, +)$, је комутативна група.*

Поље са коначним бројем елемената назива се *коначно поље*. Уколико у претходним условима $(S\backslash\{0\}, \cdot)$ није група (из услова који чине групу изузето је постојање инверзног елемента), алгебарска структура постаје *комутативни прстен* (или само *прстен* уколико услов комутативности није задовољен). Неутрални елемент за $(S\backslash\{0\}, \cdot)$ означаваћемо са 1.

Пример 2.1.9. *Нека је дат скуп $Z_m = \{0, 1, ..., m-1\}$ и нека су операције $+$ и $\cdot$ редом сабирање и множење по модулу m. Алгебарска структура $(Z, +, \cdot)$ је поље ако и само ако је m прост број.*

Дефиниција 2.1.13. *Нека је x апстрактни симбол. Скуп свих полинома*

$$p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + c_nx^n$$

са коефицијентима $c_i \in \mathbb{F}$ означава се са $\mathbb{F}[x]$. Уколико је $c_n = 1$, полином је моничан.

У пољу $\mathbb{F}_2[x] = Z_2[x]$, сви ненула полиноми су монични.

Дефиниција 2.1.14. *Нека је p прост број. Нека је $Z_p[x]$ скуп полинома са коефицијентима из Z_p и нека су операције $+$ и $\cdot$ сабирање и множење по модулу p. За $f, g \in Z_p[x]$, каже се да f дели g, односно $f|g$, ако постоји $q \in Z_p[x]$ тако да важи $g = qf$. Степен полинома $f(x)$, у ознаци $\deg(f)$, је највећи степен променљиве x. Ако $f, g, h \in Z_p[x]$ и $\deg(f) = n \geqslant 1$, тада су полиноми g и h конгруентни по модулу f, у ознаци $g(x) \equiv h(x) \pmod{f(x)}$, ако $f(x)|(g(x) - h(x))$.*

У наставку се разматрају полиноми над пољем $Z_p[x]$, при чему је p прост број, и посебно случај $p = 2$.

Теорема 2.1.7 (Дељење полинома са остатком.)**.** *Нека је* $\deg(f) = n$*. За произвољни полином* g *постоје јединствени полиноми* q *и* r*, такви да је* $g = qf + r$ *и* $\deg(r) < n$*.*

Доказ. Постоји бар један полином q такав да је $g = qf + r$ и $\deg(r) < n$. Заиста,

- Ако је $\deg(g) < n$, тада је $q = 0$ важи $r = g$ и $\deg(r) < n$.
- У противном, ако је $\deg(g) \geqslant n$, претпоставимо да не постоје полиноми q и r, такви да је $g = qf + r$ и $\deg(r) < n$. Нека су q и r таква два полинома да је $g = qf + r$ и $\deg(r) \geqslant n$, при чему степен остатка $\deg(r)$ има најмању могућу вредност. Ако су a и b најстарији коефицијенти полинома g и f, онда два полинома $q' = q - ag/(bf)$ и $r' = g - q'f$ такође задовољавају услов $g = q'f + r'$, при чему је, супротно претпоставци, $\deg(r') < \deg(r)$.

Полиноми q, r чије је постојање доказано, су јединствени који задовољавају услове $g = qf + r$ и $\deg(r) < n$. Заиста, из претпоставке да постоје друга два полинома q', r' који задовољавају исте услове следи $r' - r = f(q - q')$; ако је $q \neq q'$, онда је $\deg(f(q - q')) \geqslant n$ $\deg(r - r') < n$, супротно претпоставци. □

Аналогно конструкцији Z_m у оквиру Z (елементи су остаци, а операције сабирање и множење по модулу f), из $Z_p[x]$ се издвајају остаци по модулу f, у ознаци $Z_p[x]/(f)$, који могу бити степена највише $n - 1$.

Дефиниција 2.1.15. *Полином* $f \in Z_p[x]$ *је несводљив ако не постоје полиноми* $f_1, f_2 \in Z_p[x]$*, такви да важи* $f = f_1 f_2$*, уз* $\deg(f_1) > 0$ *и* $\deg(f_2) > 0$*.*

Теорема 2.1.8. *$Z_p[x]/(f)$ је поље ако и само ако је полином f несводљив.*

Елементе поља $Z_p[x]/(f)$ чини p^n полинома из $Z_p[x]$ степена највише $n-1$. На пример, за $p = 2$ и $n = 3$ постоји 8 полинома степена највише 2.

Пример 2.1.10. *За конструкцију поља од* $2^3 = 8$ *елемената, потребно је у прстену* $Z_2[x]$ *пронаћи несводљив полином степена* 3*. При томе је довољно посматрати полиноме који имају слободан члан 1, јер су полиноми са слободним чланом* 0 *дељиви полиномом* x*. То су полиноми:*

$f_1(x) = x^3 + 1,\ f_2(x) = x^3 + x + 1,\ f_3(x) = x^3 + x^2 + 1,\ f_4(x) = x^3 + x^2 + x + 1.$

Полиноми f_1 и f_4 нису несводљиви јер је

$$f_1(x) = (x+1)(x^2+x+1),\ f_4(x) = (x+1)(x^2+1).$$

Преостала два полинома f_2 и f_3 су несводљиви, пошто нису дељиви ни са x ни са $x+1$. Поље $Z_2[x]/(x^3+x+1)$ има 8 елемената: $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$. *Сабирање и множење полинома обавља се по модулу x^3+x+1. На пример,*

$$(x^2+1)(x^2+x+1) = x^4+x^3+x+1 = (x+1)(x^3+x+1)+x^2+x = x^2+x.$$

Нека је p прост број и $n \geqslant 1$. У скупу $Z_p[x]$ постоји барем један несводљив полином степена n [16], па постоји коначно поље од p^n елемената. Нека је $\phi(n)$ Ојлерова (Euler) функција дефинисана као број позитивних целих бројева мањих или једнаких од n, који су узајамно прости са n. У скупу $Z_p[x]$ постоји $\phi(p^n-1)/n$ несводљивих полинома степена n. Међутим, коначна поља конструисана од било која два несводљива полинома међусобно су изоморфна [16]. Дакле, постоји јединствено коначно поље од p^n елемената које означавамо са $\mathrm{GF}(p^n)$. Специјално за $n = 1$, $\mathrm{GF}(p)$ је исто што и Z_p.

Следећа лема наводи се без доказа.

Лема 2.1.2. *За сваки полином $f(x) \in \mathbb{F}[x],\ f(0) \neq 0$ постоји $e > 0$ тако да важи $f(x)|x^e - 1$.*

Дефиниција 2.1.16. *Ред* $\mathrm{ord}(p)$ *полинома $p(x)$ је најмањи број e такав да важи*

$$p(x)|x^e - 1.$$

2.1.5 Матрице

У наставку, ако се не нагласи другачије, разматрају се матрице над пољем $\mathbb{F}$.

Дефиниција 2.1.17. *Квадратна матрица A је инвертибилна, ако постоји матрица B тако да важи $AB = BA = I$, где је I јединична матрица исте димензије као A. Инвертибилну матрицу често називамо регуларном матрицом.*

Дефиниција 2.1.18. *Две матрице A и B су еквивалентне ако важи $B = PAQ$ где су P и Q инвертибилне матрице.*

Дефиниција 2.1.19. *Дијагонална матрица* $\mathrm{diag}(d_1, \ldots, d_n)$ *је квадратна матрица са елементима* $d_1, \ldots, d_n$ *на главној дијагонали, док су сви остали елементи нуле.*

Јединична матрица је специјалан случај дијагоналне матрице $\mathrm{diag}(1, 1, ..., 1)$.

Дефиниција 2.1.20. *Директни производ произвољне две матрице* A *и* B *дефинише се изразом:*

$$A \oplus B = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right],$$

где су 0 0*-матрице одговарајуће димензије.*

Линеарна група степена n $\mathrm{GL}(n, \mathbb{F})$ над пољем $\mathbb{F}$ је скуп свих $n \times n$ инвертибилних матрица над пољем $\mathbb{F}$ са операцијом множења матрица. Матрица A из групе пресликава елемент $x \in B_n$ у елемент Ax. *Афина* група степена n над пољем $\mathbb{F}$ је скуп парова (A, b), $A \in \mathrm{GL}(n, \mathbb{F})$, $b \in M_{n,1}(\mathbb{F})$ са операцијом множења $(A', b') \circ (A'', b'') = (A'A'', b'A'' + b'')$. Пар (A, b) из групе пресликава елемент $x \in B_n$ у елемент $Ax + b$.

Дефиниција 2.1.21. *Две матрице* $A, B \in M_n(\mathbb{F})$ *су сличне ако је* $B = P^{-1}AP$ *за неку инвертибилну матрицу* $P \in M_n(\mathbb{F})$. *Трансформација* $P^{-1}AP$ *је трансформација сличности матрице* A.

Квадратној инвертибилној матрици $A \in M_n(\mathbb{F})$ одговара линеарно пресликавање векторског простора $\mathbb{F}^n \mapsto \mathbb{F}^n$, које произвољан вектор $x \in \mathbb{F}^n$ пресликава у вектор Ax. Колоне матрице A су слике базних вектора $e_1, e_2, \ldots, e_n$, колона јединичне матрице реда n. У општем случају се колоне матрице линеарног пресликавања $L : \mathbb{F}^n \mapsto \mathbb{F}^n$ у бази $b_1, \ldots, b_n$ састоје се од координата слика базних вектора. Матрице линеарне трансформације у различитим базама су међусобно сличне. Група $\mathrm{GL}(n, q)$ може се посматрати и као група $n \times n$ несингуларних матрица чији су елементи из поља $\mathrm{GF}(q)$. У групи матрица $\mathrm{GL}(n, q)$ сличност је исто што и конјугованост у смислу група, па сличне матрице такође зовемо *конјугатима*.

За матрицу $A \in M_n(\mathbb{F}_q)$ нека је

$$[A]_{\mathrm{GL}(n,q)} = \{P^{-1}AP : P \in \mathrm{GL}(n, q)\}$$

скуп матрица конјугованих матрици A и нека су

$$C_{M_n(\mathbb{F}_q)}(A) = \{X \in M_n(\mathbb{F}_q) : AX = XA\}$$
$$C_{\mathrm{GL}(n,q)}(A) = \{P \in \mathrm{GL}(n,q) : AP = PA\} = C_{(M_n(\mathbb{F}_q))}(A) \cap \mathrm{GL}(n,q)$$

редом централизатори матрице A у $M_n(\mathbb{F}_q)$ и $\mathrm{GL}(n,q)$. За $A \in \mathrm{GL}(n,q)$, $[A]_{\mathrm{GL}(n,q)}$ је класа конјугованости матрице A у $\mathrm{GL}(n,q)$ и важи

$$|[A]_{\mathrm{GL}(n,q)}| = \frac{|\mathrm{GL}(n,q)|}{|C_{\mathrm{GL}(n,q)}(A)|}.$$

Нека је x симболичка променљива. Матрица $xI - A$ је *карактеристична* матрица квадратне матрице A. *Карактеристични* полином квадратне матрице A дефинише се изразом $\chi_A(x) = \det(xI - A)$ и важи $\chi_A(A) = 0$. Карактеристични полином је инваријантан у односу на сличност матрица.

Ако за $f \in \mathbb{F}[x]$ важи $f(A) = 0 \cdot I$, каже се да f *поништава* A. Међу свим моничним полиномима који поништавају A, монични полином $m_A(x)$ најмањег степена назива се *минимални* полином квадратне матрице A. Из дефиниције минималног полинома следи $m_A(x)|\chi_A(x)$.

Нека је матрица $xI - A$ (на основу познатог поступка дијагонализације) слична дијагоналној матрици $\mathrm{diag}(f_1, ..., f_n)$ над прстеном $\mathbb{F}[x]$, при чему су $f_1, ..., f_n$ јединствени монични полиноми такви да $f_1|f_2|...|f_n$. Елементи скупа $\{f_1, ..., f_n\}$ називају се *инваријантни фактори* матрице A. Неконстантни инваријантни фактори такође се зову *нетривијални* инваријантни фактори.

Дефиниција 2.1.22. *Нека су $f_1, ..., f_n$ инваријантни фактори матрице A и нека је*

$$f_j(x) = p_1(x)^{c_{j1}} \cdots p_m(x)^{c_{jm}},\ j = 1, ..., n,$$

где су $c_{ji} \geqslant 0$ цели бројеви и $p_1(x), ..., p_m(x)$ различити монични несводљиви полиноми. Све изразе у скупу

$$\{d_i = p_i(x)^{c_{ji}},\ c_{ji} \geqslant 1,\ j = 1, ..., n\}$$

рачунајући и дупликате, називамо елементарним делитељима матрице A.

Инваријантни фактори и елементарни делитељи могу се добити једни из других и важи:

$$f_1(x) \cdots f_n(x) = \det(xI - A) = d_1(x) \cdots d_m(x).$$

Пример 2.1.11. *Нека матрица A реда 12 над прстеном Q има следеће инваријантне факторе: $f_1(x) = \cdots = f_9(x) = 1$, $f_{10}(x) = x^2 + 1$, $f_{11}(x) =$*

$(x^2+1)(x^2-2)$, $f_{12}(x) = (x^2+1)(x^2-2)^2$. *Тада су елементарни делитељи:* $x^2+1,\ x^2+1,\ x^2+1,\ x^2-2,\ (x^2-2)^2$.

Теорема 2.1.9. *Ако су $f_1, ..., f_n$ инваријантни фактори матрице A над простеном $\mathbb{F}[x]$ такви да $f_1|f_2|...|f_n$, тада је f_n минимални полином матрице $A \in M_n(\mathbb{F})$.*

Доказ. Доказ директно следи из израза $\chi_A(x) = f_1(x) \cdots f_n(x)$. □

Пример 2.1.12. *Нека је у пољу $GF(2)$ дефинисана матрица*

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Карактеристични и минимални полиноми матрице A су редом x^4+1 и $(x+1)^3 = x^3+x^2+x+1$. Нетривијални инваријантни фактори и елементарни делитељи су $(x+1)$ и $(x+1)^3$.

Дефиниција 2.1.23. *За $n \geqslant 1$ нека је дат монични полином облика:*

$$q(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} + x^n.$$

За $n \geqslant 2$, придружена (companion) матрица овог полинома дефинисана је изразом:

$$C(q) := \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{bmatrix}.$$

За $n = 1$ је $q(x) = x + c_0$ и $C(q) = [-c_0]$.

Теореме 2.1.10 и 2.1.11 наводе се без доказа.

Теорема 2.1.10. *Свака матрица је слична матрици придруженој свом карактеристичном полиному.*

Теорема 2.1.11. *Карактеристични и минимални полином придружене матрице су једнаки.*

Дефиниција 2.1.24. *Ред е матрице A је најмањи природан број такав да важи $A^e = I$.*

Егзистенција реда матрице e следи на основу леме 2.1.2 и теореме 2.1.12.

Теорема 2.1.12. *Нека је*

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + c_nx^n \in \mathbb{F}[x]$$

где је $n \geqslant 1$ и $c_0 \neq 0$. Ред полинома f једнак је реду његове придружене матрице A из $\mathrm{GL}(n, \mathbb{F})$.

Доказ. Пошто је A придружена матрица полинома $f(x)$, полином $f(x)$ је истовремено и карактеристични и минимални полином матрице A. Ако $f(x)|x^e - 1$ за неко e, следи $f(A)|A^e - I$ тј. $A^e - I = 0$. Ако $f(x) \nmid x^e - 1$ за неко e, следи $f(A) \nmid A^e - I$ тј. $A^e - I \neq 0$. Дакле, $A^e = I$ ако и само ако $f(x)|x^e - 1$. Специјално, претходно разматрање важи и за најмање могуће e које задовољава наведене услове. □

Пример 2.1.13. *Нека је*

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

придружена матрица полинома $x^3 + x + 1$ над пољем $GF(2)$. Непосредно се проверава да је $A[0\ 0\ 0]^T = [0\ 0\ 0]^T$ и $A^7v = v,\ x \neq 0$. Карактеристични и минимални полином матрице A је $f(x) = x^3+x+1$ и непосредно се проверава да је ред полинома $f(x)$ једнак 7 тј. $x^3 + x + 1|x^7 - 1$.

Придружена матрица је специјалан случај *хипер-придружене* матрице:

Дефиниција 2.1.25. *За $n \geqslant 1$ нека је $q(x)$ моничны полином облика:*

$$q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + x^n.$$

За $n \geqslant 2$, хипер-придружена (hyper-companion) матрица полинома q^k дефинисана је изразом:

$$H(q(x)^k) = C_k(q) \coloneqq \begin{bmatrix} C(q) & 0 & \cdots & 0 & 0 \\ N & C(q) & \cdots & 0 & 0 \\ 0 & N & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & N & C(q) \end{bmatrix}_{(kn)\times(kn)}$$

где је N $n \times n$-матрица састављена од свих нула осим елемента у горњем десном углу са вредношћу 1. *За $k = 1$, $H(q) = C_1(q) = C(q)$.*

Пример 2.1.14.

$$H((x^2+1)^3) = \begin{bmatrix} C(x^2+1) & 0 & 0 \\ N & C(x^2+1) & 0 \\ 0 & N & C(x^2+1) \end{bmatrix} = \left[\begin{array}{cc|cc|cc} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right].$$

$$H(x^3 + 5x^2 - 6) = C(x^3 + 5x^2 - 6) = \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{bmatrix}.$$

$$H((x-3)^4) = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 3 \end{bmatrix}.$$

Лема 2.1.3. *Нека је $q \in \mathbb{F}[x]$ моничан полином степена $n \geqslant 1$. Тада је:*

- *карактеристични и минимални полином придружене матрице $C(q)$ једнак $q(x)$.*
- *карактеристични и минимални полином хипер-придружене матрице $C_k(q)$ једнак $q^k(x)$.*

Дакле, за $k \geqslant 1$, инваријантни фактори матрице $C_k(q)$ су $\{1, ..., 1, q^k(x)\}$ и $C_k(q)$ има један елементарни делитељ $q^k(x)$.

Скуп *канонских* матрица треба да садржи све „представнике" класа еквиваленције. Другим речима, свака матрица треба да буде еквивалентна тачно једној из скупа канонских матрица. Канонске форме матрица дефинишу се тако да „што је могуће више" имају дијагонални облик. Нека је:

$$B = \operatorname{diag}(B_1, ..., B_r),\ C = \operatorname{diag}(C_1, ..., C_r),\ P = \operatorname{diag}(P_1, ..., P_r)$$

где су за свако $i = 1, ..., r$, B_i, C_i, P_i квадратне матрице истих димензија, а матрице P_i су инвертибилне. Матрица B је директни производ матрица $B_1, ..., B_r$. Матрица P је инвертибилна и важи:

$$BC = \mathrm{diag}(B_1C_1, ..., B_rC_r)$$
$$P^{-1} = \mathrm{diag}(P_1^{-1}, ..., P_r^{-1})$$
$$P^{-1}BP = \mathrm{diag}(P_1^{-1}B_1P_1, ..., P_r^{-1}B_rP_r)$$

Лема 2.1.4. *[25, 26] За матрице над прстеном $\mathbb{F}[x]$ важе следећа тврђења:*

- ***Сличност директних производа:***
  Ако је матрица B_i слична са C_i за $i = 1, ..., r$, тада је $\mathrm{diag}(B_1, ..., B_r)$ слична са $\mathrm{diag}(C_1, ..., C_r)$.

- ***Еквиваленткост директних производа:***
  Ако је матрица B_i еквивалентна са C_i за $i = 1, ..., r$, тада је $\mathrm{diag}(B_1, ..., B_r)$ еквивалентна са $\mathrm{diag}(C_1, ..., C_r)$.

- ***Пермутација директних производа:***
  Нека су за $i = 1, ..., r$ B_i квадратне матрице. Тада је за сваку пермутацију p индекса $(1, ..., r)$, $\mathrm{diag}(B_1, ..., B_r)$ еквивалентна са $\mathrm{diag}(B_{p(1)}, ..., B_{p(r)})$.

- ***Разлагање директних производа:***
  Нека су полиноми $f(x)$ и $g(x)$ узајамно прости. Тада је $\mathrm{diag}(1, fg)$ над пољем $\mathbb{F}[x]$ еквивалентна са $\mathrm{diag}(f, g)$. Општије, ако су $q_1, ..., q_k$ узајамно прости полиноми, тада је матрица $\mathrm{diag}(q_1, ..., q_k)$ еквивалентна са матрицом $\mathrm{diag}(I_{k-1}, \prod_{i=1}^{k} q_i)$.

Теорема 2.1.13. *Свака квадратна матрица над пољем $\mathbb{F}$ слична је:*

- *директном производу придружених матрица нетривијалних инваријантних фактора,*

- *директном производу придружених матрица елементарних делитеља над пољем $\mathbb{F}$ и*

- *директном производу хипер-придружених матрица елементарних делитеља над пољем $\mathbb{F}$.*

Другим речима, нека су за $A \in M_n(\mathbb{F})$, $f_1, ..., f_n$ инваријантни фактори и нека су над прстеном $\mathbb{F}[x]$, $d_1 = q_1^{k_1}, ..., d_m = q_m^{k_m}$ елементарни делитељи, где су $q_1, ..., q_m$ несводљиви полиноми. Тада је матрица A слична са следећим матрицама:

$$\mathrm{diag}(C(f_1), ..., C(f_n))$$
$$\mathrm{diag}(C(d_1), ..., C(d_m))$$
$$\mathrm{diag}(C_{k_1}(q_1), ..., C_{k_m}(q_m))$$

Пошто је сличност релација еквиваленције, матрице $C_k(q)$ и $C(q^k)$ су сличне.

Дефиниција 2.1.26. *Матрица A је у Јакобсоновој канонској форми (у даљем тексту - у канонској форми), ако је директни производ хипер-придружених матрица елементарних делитеља над прстеном $\mathbb{F}[x]$*

$$A = \begin{bmatrix} H_1 & 0 & 0 & 0 & 0 \\ 0 & H_2 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & H_{n-1} & 0 \\ 0 & 0 & 0 & 0 & H_n \end{bmatrix}$$

где је H_i матрица придружена i-том елементарном делитељу.

Пример 2.1.15. *Нека је као у примеру 2.1.12, у пољу $GF(2)$*

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Карактеристични и минимални полиноми матрице A редом су $x^4 + 1$ и $(x+1)^3 = x^3+x^2+x+1$. Придружена матрица елементарног делитеља $x+1$ је $\begin{bmatrix} 1 \end{bmatrix}$. Придружена матрица елементарног делитеља $(x+1)^3 = x^3+x^2+x+1$ (односно минималном полиному) је

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

па је канонска форма матрице A

$$\left[\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] = \mathrm{diag}(\begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}).$$

Пример 2.1.16. *Нека су дати инваријантни фактори над пољем* Q: $f_1(x) = (x_2+4)(x_2-3)$ *и* $f_2(x) = (x_2+4)^2(x_2-3)^2$. *Елементарни делитељи су* (x_2+4), (x_2-3), $(x_2+4)^2$ *и* $(x_2-3)^2$ *па канонска форма матрице има облик:*

$$\operatorname{diag}(\begin{bmatrix} 0 & -4 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -4 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -4 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 \end{bmatrix}).$$

Пример 2.1.17. *Нека је у пољу* $GF(2)$ *дефинисана матрица*

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Матрица A *делује на векторе из* F_2^3 *на следећи начин:*

v	000	001	010	011	100	101	110	111
Av	000	001	110	111	100	101	010	011

Пермутација индукована матрицом A *(дејством* A *матрице на све векторе из* F_2^3*) има циклусну структуру којој одговара моном* $f_1^4 f_2^2$. *Исту структуру има и пермутација индукована канонском формом марtице* A. *Карактеристични и минимални полиноми матрице* A *су редом* x^3+x^2+x+1 *и* $x^2+1=(x+1)^2$. *Канонска форма матрице* A *је*

$$\left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \end{array}\right].$$

Први блок матрице делује на први бит, док други блок делује на последња два бита вектора. Због тога се формирање циклусних структура може посматрати независно по блоковима, при чему се у коначном исходу сва дејства првог блока „упарују" са свим дејствима другог блока. Блокови устварипредстављају хипер-придружене матрице које одговарају факторима $x+1$ *и* $(x+1)^2$ *минималног полинома (елементарним делитељима карактеристичног полинома) матрице* A. *Дејство првог блока је пермутација са циклусном структуром* f_1^2:

$$\begin{bmatrix}1\end{bmatrix}\begin{bmatrix}0\end{bmatrix} = \begin{bmatrix}0\end{bmatrix}, \quad \begin{bmatrix}1\end{bmatrix}\begin{bmatrix}1\end{bmatrix} = \begin{bmatrix}1\end{bmatrix}.$$

Дејство другог блока је пермутација са циклусном структуром $f_1^2 f_2$:

$$\begin{bmatrix}0\\0\end{bmatrix} \to \begin{bmatrix}0\\0\end{bmatrix}, \ \begin{bmatrix}0\\1\end{bmatrix} \to \begin{bmatrix}1\\0\end{bmatrix}, \ \begin{bmatrix}1\\0\end{bmatrix} \to \begin{bmatrix}0\\1\end{bmatrix}, \ \begin{bmatrix}1\\1\end{bmatrix} \to \begin{bmatrix}1\\1\end{bmatrix}.$$

Циклусна структура пермутације која одговара матрици A је Декартов производ блоковима индукованих циклусних структура:

$$f_1^2 \times f_1^2 f_2 = f_1^4 f_2^2.$$

Пример 2.1.18. *Посматрајмо регуларне матрице димензије 2 у пољу $GF(2)$.*

- *Карактеристични и минимални полином матрице $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ редом су $(x-1)^2$ и $(x-1)$. Ред минималног полинома је 1 и елементарни делитељи матрице су $(x-1)$ и $(x-1)$. Канонска форма, састављена од два блока хипер-придружених матрица је $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$. Сваком блоку одговара пермутација са циклусном структуром f_1^2, а пермутација која одговара канонској форми има циклусну структуру $f_1^2 \times f_1^2 = f_1^4$.*
- *Карактеристични и минимални полином матрице $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$ је $(x-1)^2$. Ред минималног полинома је 2 и елементарни делитељ матрице је $(x-1)^2$. Канонска форма, састављена од једног блока хипер-придружене (истовремено и придружене) матрице је $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$ и пермутација која одговара канонској форми има циклусну структуру $f_1^2 f_2$.*
- *Карактеристични и минимални полином матрице $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$ је x^2+x+1. Ред минималног полинома је 3 и елементарни делитељ матрице је x^2+x+1. Канонска форма, састављена од једног блока хипер-придружене (истовремено и придружене) матрице је $\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$ и пермутација која одговара канонској форми има циклусну структуру $f_1 f_3$.*

Ове три матрице можемо узети као представнике конјугованих класа (сличних матрица). Узимајући у обзир свих шест регуларних матрица, непосредно се проверава да је $Z_{\mathrm{GL}(2,2)}(f) = \frac{1}{6}(f_1^4 + 3f_1^2 f_2 + 2f_1 f_3)$.

Напомена 2.1.1. *Изоставимо полином x и посматрајмо несводљиве полиноме $p(x)$ степена мањег или једнаког од 2. Скуп елементарних делитеља полинома облика $p(x)^k$ степена 2, које индукују представници конјугованих класа је скуп $\{\{x-1, x-1\}, \{(x-1)^2\}, \{x^2+x+1\}\}$. Пошто постоји по један несводљиви полином степена 1 и 2, овај скуп се може добити из скупа свих несводљивих полинома $p(x)$ степена $\leqslant 2$, разлагањем на партиције броја k.*

2.1.6 Векторски простори

Нека је S поље и нека је V скуп чије елементе називамо векторима. За векторе $x_1, ..., x_n$ из векторског простора V над пољем S каже се да су *линеарно зависни* ако постоје елементи $\alpha_1, ..., \alpha_n$ поља S, који нису сви једнаки нули, такви да важи једнакост

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = \vec{0} \tag{2.8}$$

где је $\vec{0}$ неутрални елемент у групи $(V, +)$. Израз на левој страни једнакости (2.8) назива се *линеарна комбинација* вектора $x_1, ..., x_n$. Ако вектори нису линеарно зависни, кажемо да су линеарно независни. Другим речима, за независне векторе $x_1, ..., x_n$ из једнакости (2.8) следи $\alpha_1 = 0, ..., \alpha_n = 0$. За коначан скуп вектора каже се да је *линеарно зависан* или *линеарно независан* према томе да ли су вектори који образују скуп линеарно зависни или независни. Нека је $T = \{x_1, ..., x_t\} \subset V$. Скуп свих линерних комбинација вектора из T, тј. скуп

$$U = \{\alpha_1 x_1 + \cdots + \alpha_t x_t \mid \alpha_1, ..., \alpha_t \in S\}$$

назива се *линеал* ($L(T)$) скупа T. Каже се да је U генерисан скупом T. Линеарно независан скуп вектора B назива се *база* векторског простора V ако B генерише V. Број елемената у произвољној бази назива се *димензија* простора V.

Дефиниција 2.1.27. *Сваки непразан подскуп W простора $V(\mathbb{F})$ је потпростор ако заједно са сваким паром вектора које садржи, садржи и све њихове линеарне комбинације. Другим речима, потпростор мора бити затворен за операције дефинисане у простору V.*

Сума потпростора W_1 и W_2 је линеал њихове уније:

$$W_1 + W_2 = L(W_1 \cup W_2).$$

Уколико је пресек два потпростора нула вектор, њихова сума назива се директном (унутрашњом) сумом и означава са $W_1 \oplus W_2$. Потпростори W_1 и W_2 чине разлагање (декомпозицију) простора V уколико важи

$$V = W_1 \oplus W_2.$$

Пример 2.1.19. *Скуп $Z_p[x]$ полинома са коефицијентима из Z_p, где је p прост број, представља векторски простор над пољем Z_p.*

Дефиниција 2.1.28. *Модул је генерализација појма векторског простора у коме је поље скалара замењено прстеном.*

Теорема 2.1.14. *Матрица A је регуларна (несингуларна) ако и само ако су врсте (колоне) матрице линеарно независне.*

Дефиниција 2.1.29. *Нека су V и W векторски простори над пољем F. Линеарно пресликавање из V у W је функција T из V у W тако да је*

$$T(c\alpha + \beta) = c(T\alpha) + T\beta$$

за све векторе $\alpha, \beta \in V$ и за сваки скалар $c \in F$.

Матрицу $A_{m,n}$ можемо посматрати као функцију (линеарну трансформацију) $T : \mathbb{F} \to \mathbb{F}$ дефинисану изразом $T(x) = Ax$ за свако $x \in \mathbb{F}$. $\mathrm{GL}(n, q)$ је група свих инвертибилних линеарних трансформација n-димензионог векторског простора над пољем $\mathrm{GF}(q)$. Сличне матрице представљају исто линеарно пресликавање над двема базама векторског простора.

Теорема 2.1.15. *Ред групе $GL(n, q)$ је $\prod_{i=0}^{n-1}(q^n - q^i)$.*

Доказ. Потребно је избројати све $n \times n$ матрице чије су врсте линеарно независне. При формирању такве матрице, њена прва врста може да буде било који вектор дужине n који за елементе нема све нуле. Таквих вектора има $q^n - 1$. Друга врста мора бити линеарно независна од прве, што значи да не може бити једнака првој врсти помноженој скаларом из скупа $\{0, 1, \ldots, q-1\}$. Дакле, за другу врсту постоји $q^n - q$ могућности. Уопште, i-та врста не сме бити линеарна комбинација претходних $i-1$ врста, односно не сме припадати линеалу првих $i-1$ врста. Пошто постоји q^{i-1} линеарних комбинација првих $i-1$ врста, за i-ту врсту постоји $q^n - q^{i-1}$ могућности. Дакле, $n \times n$ матрицу могуће је формирати на $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i)$ начина. □

Пример 2.1.20. *Размотримо групу $GL(n,2)$ свих инвертибилних линеарних трансформација n-димензионог векторског простора над пољем* $\mathrm{GF}(2)$. *Група $GL(n,2)$ може се посматрати и као група $n \times n$ несингуларних матрица чији су елементи из поља* $\mathrm{GF}(2)$. *Нека је $A = (a_{ij})$ једна таква матрица и нека су дати скуп улазних променљивих $x = \{x_1, x_2, \ldots, x_n\}$ и Булова функција $f : \{0,1\}^n \to \{0,1\}^n$, тако да је $f(x_1, x_2, \ldots, x_n) = \{f_1, f_2, \ldots, f_n\}$. Дејство матрице A на улазне и излазне променљиве означимо респективно са xA и fA (тј. x и f су врсте). Множење матрице и вектора дефинише се на уобичајени начин ($\oplus$ овде означава компонентно сабирање по модулу 2):*

$$xA = \Big(\bigoplus_{k=1}^{n} a_{k1}x_k, \ldots, \bigoplus_{k=1}^{n} a_{kn}x_k \Big)$$

односно

$$fA = \Big(\bigoplus_{k=1}^{n} a_{k1}f_k, \ldots, \bigoplus_{k=1}^{n} a_{kn}f_k \Big).$$

Ред групе $\mathrm{GL}(n,2)$ *је*

$$\prod_{i=0}^{n-1}(2^n - 2^i) = (2^n - 1)2(2^{n-1} - 1)2^2(2^{n-2} - 1)\cdots 2^{n-1}(2^1 - 1)$$

$$= 2^{1+2+\cdots+n-1}\prod_{i=1}^{n}(2^i - 1) = 2^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(2^i - 1) \tag{2.9}$$

Трансформације афине групе $\mathrm{AGL}(n,2)$ *добијају се композицијом трансформација линеарне групе и 2^n трансформација комплементирања излаза, па је*

$$|\mathrm{AGL}(n,2)| = 2^n|\mathrm{GL}(n,2)| = 2^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(2^i - 1).$$

Дефиниција 2.1.30. *Нека је V векторски простор. Инваријантан потпростор линеарног пресликавања $T : V \to V$ је потпростор $W \subseteq V$ затворен за T, тј. потпростор за који важи $T(W) \subseteq W$.*

Напомена 2.1.2. *Базу једнодимензионог векторског простора V чини било који ненула вектор $v \in V$. Било који други вектор из V може се представити као λv, где је λ скалар. Свако линеарно пресликавање T може се представити матрицом A, при чему је $Av = \lambda v$, па је V инваријантан потпростор.*

Дефиниција 2.1.31. *Нека је V векторски простор и нека је $T : V \to V$ линеарно пресликавање. T-циклични потпростор векторског простора V генерисан вектором v је потпростор $W \subseteq V$ генерисан скупом вектора $\{v, T(v), T^2(v), T^3(v), ...\}$. Уколико је димензија T-цикличног потпростора W једнака димензији векторског простора V, v је циклични вектор пресликавања T на простору V.*

Нека је

$$p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + c_nx^n$$

карактеристични полином пресликавања T и нека је v циклични вектор пресликавања T. Нека је $T(v_1) = v_2,\ T(v_2) = v_3,\ T(v_3) = v_4, ..., T(v_{n-1}) = v_n$. Из $p(T) = c_0 + c_1T + c_2T^2 + \cdots + c_{n-1}T^{n-1} + c_nT^n = 0$, тј. $c_0v + c_1Tv + c_2T^2v + \cdots + c_{n-1}T^{n-1}v + c_nT^nv = 0$, следи $T(v_n) = -c_0v_1 - c_1v_2 - \cdots - c_{n-1}v_n$. Дакле, пресликавање T у бази B може се представити матрицом:

$$C(p) \coloneqq \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{bmatrix}.$$

Приметимо да је ова матрица придружена матрица карактеристичног и истовремено минималног полинома $p(x)$.

Пример 2.1.21. *Нека је V дводимензиони векторски простор и нека је пресликавање T представљено матрицом $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ у стандардној бази $\{e_1 = [1\ 0]^T, e_2 = [0\ 1]^T\}$. Пошто је $T(e_1) = e_2$, следи да циклични вектор e_1 разапиње V. С друге стране, $T(e_2) = 0 = 0 \cdot e_2$, па e_2 не разапиње V.*

Следећа теорема је непосредна последица Теореме 2.1.12.

Теорема 2.1.16. *Нека је V векторски простор у коме оператор (матрица) A има минимални полином облика $p(x) = (q(x))^k$ где је $q(x)$ несводљиви полином. Тада за сваки вектор $v \in V$ из $A^sv = v$ следи $s|\operatorname{ord}(p(x))$.*

Теорема 2.1.16 илуструје важну чињеницу да *циклуси* које генерише матрица A морају бити дужине која дели ред минималног полинома матрице A.

Пример 2.1.22. *Нека је дата матрица*

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Карактеристични и минимални полином матрице A над пољем $GF(2)$ је $f(x) = x^3 + x^2 + x + 1 = (x+1)^3$. Ред овог полинома је 4. Пошто је карактеристични полином једнак минималном, одговарајућа придружена матрица има исти ред као и минимални полином. Постоји вектор $v \neq 0$, рецимо $v = [1\ 0\ 0]^T$ такав да важи $A^4 v = v$ и постоји циклус $v_2 = Av,\ v_3 = Av_2,\ v_4 = Av_3,\ v = Av_4$. На овај начин нису „исцрпљени" сви вектори простора, па даље посматрамо скуп „преосталих" вектора. На овом новом потпростору рестрикција линеарног пресликавања има минимални полином $(x-1)^2 = x^2+1$. Ред овог полинома је 2, па за рецимо вектор $v = [0\ 1\ 0]^T$ важи $A^2 v = v$. Пошто још увек нису исцрпљени сви вектори простора, посматра се нови потпростор који има минимални полином $x-1 = x+1$ и састоји се од јединог преосталог ненула вектора $v = [0\ 0\ 1]^T$ за који важи $Av = v$. Имајући у виду да се нула вектор увек пресликава у себе, из претходних закључака следи да дејство матрице A на векторе простора разлаже простор на два циклуса дужине 1, један циклус дужине 2 и један циклус дужине 4 односно циклусну структуру $f_1^2 f_2 f_4$. Дакле, инваријантни простор састављен од свих вектора разложен је на (директну суму) четири циклична потпростора и збир димензија потпростора једнак је димензији простора.

Уопштимо сада претходна разматрања. Нека је A линеарни оператор n-димензионог векторског простора V над пољем $\mathbb{F}$. Нека је

$$\varphi(x) = \prod_{i=1}^{s} P_i(x)^{c_i} \tag{2.10}$$

минимални полином оператора A, где су $P_i(x)$ различити, монични, несводљиви полиноми над пољем $\mathbb{F}$. *Примарна декомпозиција* векторског простора V је директна сума инваријантних потпростора U_i таквих да је $P_i(x)^{c_i}$ минимални полином потпростора U_i. Сваки од инваријантних потпростора U_i је директна сума цикличних потпростора $W_{i,j}$ таквих да је $P_i(x)^{c_i}$ минимални полином потпростора $W_{i,r(i)}$ и минимални полином потпростора $W_{i,j}$ дели минимални

полином потпростора $W_{i,j+1},\ j = 1, ..., r(i) - 1$. Дакле, важе следећи изрази:

$$V = \bigoplus_{i=1}^{s} U_i \qquad \text{и} \qquad U_i = \bigoplus_{j=1}^{r(i)} W_{i,j}.$$

Нека је $P_i(x) = \sum_{j=0}^{d_i} b_j x^j \in F[x],\ b_{d_i} = 1$. Нека је W_i циклични потпростор димензије kd_i са минималним полиномом $P_i(x)^k$. Рестрикција оператора A на W_i представља се хипер-придруженом матрицом $H(P_i^k)$. Дакле, простор са минималним полиномом из израза (2.10) разлаже се на директну суму $\alpha_j^{(i)}$ цикличних потпростора са минималним полиномом $P_i(x)^j$ за $1 \leqslant j \leqslant c_i,\ 1 \leqslant i \leqslant s$. Класична нормална форма матрице A је блок дијагонална матрица

$$\operatorname{diag}\big(D(P_1, \alpha^{(1)}), ..., D(P_s, \alpha^{(s)})\big), \tag{2.11}$$

при чему се матрице $D(P_i(x), \alpha^{(i)})$ даље разлажу на блок дијагоналне матрице (канонску форму) облика

$$D(P_i, \alpha^{(i)}) = \operatorname{diag}\big(\underbrace{H(P_i), ..., H(P_i)}_{\alpha_1^{(i)}}, \underbrace{H(P_i^2), ..., H(P_i^2)}_{\alpha_2^{(i)}}, ...\big). \tag{2.12}$$

Из претходног следи да карактеристични полином матрице A има облик:

$$\chi_A(x) = \prod_{i=1}^{s} P_i(x)^{a_i}$$

где је $a_i = \sum_j j\alpha_j^{(i)}$ и $\sum_{i=1}^{s} a_i d_i = n$. Дакле, дејство матрице A може се представити као директни производ

$$\bigtimes_{i=1}^{s} \bigtimes_{j=1}^{a_i} \bigtimes_{k=1}^{\alpha_j^{(i)}} H(P_i^j) = \bigtimes_{i=1}^{s} \bigtimes_{j=1}^{a_i} H(P_i^j)^{\times \alpha_{ij}}. \tag{2.13}$$

2.1.7 Булове функције

Елемент $x = (x_1, x_2, \ldots, x_n) \in B_n$ одговара целом броју $X = \sum_{i=1}^{n} x_i 2^{n-i}$. Функција $f\colon B_n \mapsto B_1$ која одговара вектору $F = [f_0, f_1, \ldots, f_{N-1}] \in B_N$ ($N = 2^n$), односно таблици истинитости функције f, $f_X = f(x)$, назива се Булова функција. Без опасности од забуне, користићемо ознаке x и f редом за X и F. Скуп $\mathcal{B}_n$ Булових функција $f\colon B_n \mapsto B_1$ у овом контексту одговара скупу вектора B_N. У случају пресликавања $f : B_n \mapsto B_m$, f се назива *векторска* Булова функција. Специјално, за $m = n$, уколико је f бијективно пресликавање, векторска Булова функција је *инвертибилна*. *Хемингова тежина* Булове функције f у ознаци $\operatorname{wt}(f)$ представља број улаза x таквих да је $f(x) = 1$.

Пример 2.1.23. *У случају векторских Булових функција $f\colon B_n \mapsto B_m$ сваком од 2^n улаза може се придружити било који од 2^m излаза. Другим речима, број векторских Булових функција одговара броју варијација са понављањем 2^n-те класе од 2^m елемената, тј. $(2^m)^{2^n} = 2^{m2^n}$. Специјално, за $m = 1$ број Булових функција је 2^{2^n}. Број инвертибилних Булових функција од n променљивих једнак је $2^n!$.*

Дефиниција 2.1.32. *Нека је G пермутациона група која делује на B_n. Две Булове функције $f, g\colon B_n \to B_1$ пермутационо су еквивалентне у односу на G, ако постоји пермутација $\sigma \in G$ таква да је $f(x) = g(\sigma(x))$ за свако $x \in B_n$.*

Релација пермутационе еквиваленције разлаже $\mathcal{B}_n$ на класе еквиваленције. Нека је представник класе еквиваленције лексикографски најмања N-торка у класи. Нека $U_n(G)$ означава број класа еквиваленције Булових функција у односу на G; специјално, за четири групе које се разматрају у раду (S'_n, G_n, GL_n и AGL_n), то су низови A003180, A000616, A000585, A000214 у енциклопедији [30].

Пример 2.1.24. *Свих* 16 *Булових функција $f\colon B_2 \mapsto B_1$ приказане су у табели 2.4 својим таблицама истинитости. Нека на аргумент (x_1, x_2) делује симетрична група S_2, коју чине две пермутације:* (1)(2) *и* (1 2). *Пермутација* (1)(2) *сваку функцију пресликава у њу саму. Пермутација* (1 2) *индукује замену друге и треће врсте (замена колона x_1 и x_2 у табели 2.4), па парови функција (f_3,f_5),(f_4,f_6),(f_{11},f_{13}) и (f_{12},f_{14}) чине класе еквиваленције. Све остале функције припадају једночланим класама еквиваленције. Дакле,* 16 *Булових функција од две променљиве разлажу се на $U_2(S_2) = 12$ класа еквиваленције (једночлане класе у табели нису обојене).*

Табела 2.4: Класе еквиваленције Булових функција $f\colon B_2 \mapsto B_1$ у односу на групу S_2

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Две инвертибилне функције $f, g : B_n \to B_n$ еквивалентне су у односу на групу G ако постоје две пермутације $\sigma, \rho \in G$ такве да је $f(x) = \rho(g(\sigma(x)))$

за све $x \in B_n$. Нека $V_n(G)$ означава број класа еквиваленције инвертибилних Булових функција од n променљивих под дејством исте групе G на домен и кодомен. Првих неколико чланова овог низа за четири групе које се разматрају у раду (S'_n, G_n, GL_n и AGL_n) могу се наћи у енциклопедији [30] (низови A000653, A000654, A001038, A001537).

Пример 2.1.25. *За $n = 2$ постоји $2^2! = 24$ инвертибилних Булових функција f_i, $1 \leqslant i \leqslant 24$. Булове функције $f\colon B_2 \mapsto B_2$ приказане су својим таблицама истинитости (видети табелу 2.5):*

Табела 2.5: Класе еквиваленције инвертибилних Булових функција $f\colon B_2 \mapsto B_2$ у односу на групу S_2

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}
0	0	00	00	00	00	00	00	01	01	01	01	01	01
0	1	01	01	10	10	11	11	00	00	10	10	11	11
1	0	10	11	01	11	01	10	10	11	00	11	00	10
1	1	11	10	11	01	10	01	11	10	11	00	10	00

x_1	x_2	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{24}
0	0	10	10	10	10	10	10	11	11	11	11	11	11
0	1	00	00	01	01	11	11	00	00	01	01	10	10
1	0	01	11	00	11	00	01	01	10	00	10	00	01
1	1	11	01	11	00	01	00	10	01	10	00	01	00

Ако S_2 делује и на улазне променљиве (x_1, x_2) и на излазне променљиве f_{x_1}, f_{x_2}, онда четири трансформације из $S_2 \times S_2$ разлажу 24 функције на $V_2 = 7$ класа еквиваленције: (f_1,f_3),(f_2,f_4,f_5,f_6),(f_7,f_9,f_{13},f_{15}),$(f_8,f_{11},f_{14},f_{17})$, $(f_{10},f_{12},f_{16},f_{18})$,$(f_{19},f_{20},f_{21},f_{23})$ *и* (f_{22},f_{24}). *Представници ових класа еквиваленције су редом* $f_1, f_2, f_7, f_8, f_{10}, f_{19}$ *и* f_{22}.

Ако је $x, y \in B_n$, $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$, тада неједнакост $x \leqslant y$ означава скуп неједнакости $x_i \leqslant y_i$, $1 \leqslant i \leqslant n$. Булова функција $f\colon B_n \mapsto B_1$ је *монотона* ако за сваки пар $x, y \in B_n$ услов $x \leqslant y$ имплицира $f(x) \leqslant f(y)$. Означимо са $\mathcal{D}_n$ скуп монотоних Булових функција од n променљивих и нека је $d_n = |\mathcal{D}_n|$ (Дедекиндови бројеви, видети [12]).

Пример 2.1.26. *Из скупа од* 16 *Булових функција, само њих* 6 *су монотоне, тј. $d_2 = 6$ (видети табелу 2.6).*

Табела 2.6: Скуп $\mathcal{D}_2$

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6
0	0	0	0	0	0	0	1
0	1	0	0	0	1	1	1
1	0	0	0	1	0	1	1
1	1	0	1	1	1	1	1

За две монотоне Булове функције f_1 и f_2 важи:

$$x \leqslant y \Rightarrow (f_1(x) \wedge f_2(x) \leqslant f_1(y) \wedge f_2(y))$$

$$x \leqslant y \Rightarrow (f_1(x) \vee f_2(x) \leqslant f_1(y) \vee f_2(y))$$

Дакле, конјукција и дисјункција две монотоне Булове функције такође су монотоне Булове функције. Ако је функција $f : B_n \mapsto B_1$ монотона, онда су све функције еквивалентне (у односу на групу пермутација променљивих) са f такође монотоне. Заиста, ако је $\pi \in S_n$ и $g(x) = f(\pi(x))$ за све $x \in B_n$, онда из $x \leqslant y$ следи $\pi(x) \leqslant \pi(y)$ и $g(x) = f(\pi(x)) \leqslant f(\pi(y)) = g(y)$. Према томе, пермутациона релација еквиваленције разлаже $\mathcal{D}_n$ на класе еквиваленције. Означимо са $\mathcal{R}_n$ скуп представника класа еквиваленције монотоних Булових функција од n променљивих и нека је $r_n = |\mathcal{R}_n|$.

Пример 2.1.27. *Неекивалентне монотоне Булове функције од две променљиве су (видети табелу 2.6):* $f_1 = 0,\ f_2 = x_1 \wedge x_2,\ f_3 = x_1,\ f_5 = x_1 \vee x_2,\ f_6 = 1$. *Функција* $f_3 = x_1$ *еквивалентна је са* $f_4 = x_2$. *Примећује се да изрази за монотоне Булове функције не садрже негацију, што важи и у општем случају.*

2.1.8 Графови

Дефиниција 2.1.33. *Нека је* X *непразан скуп и* ρ *бинарна релација над* X. *Уређен пар* $G = (X, \rho)$ *се назива граф. Елементи скупа* X *су чворови графа, а елементи скупа* ρ *гране графа.*

Дефиниција 2.1.34. *Граф* $G = (X, \rho)$ *је симетричан или неусмерен ако и само ако је* ρ *симетрична релација.*

Граф $G = (X, \rho)$ је асиметричан или усмерен ако и само ако је ρ асиметрична релација.

За произвољан граф, уместо $G = (X, \rho)$ често се пише $G = (X, U)$, при чему се заобилази појам бинарне релације и U тумачи као скуп уређених

парова елемената скупа X, тј. као скуп грана. Дакле, граф је задат ако је задат скуп чворова и скуп грана.

Нека је дат граф $G = (X, U)$. Граф облика $H = (Y, T)$, при чему је $Y \subseteq X$ и $T = U \cap (Y \times Y)$ (T је подскуп скупа U који садржи све оне парове из U који су индуковани од елемената скупа Y), назива се подграф графа G, индукован скупом чворова Y. Дакле, индуковани подграф из датог графа добија се тако што се уочи неки подскуп Y скупа чворова и удаље из графа сви остали чворови заједно са гранама које су суседне удаљеним чворовима. У подграфу остају само гране које повезују чворове из Y.

Два графа су *изоморфна* ако постоји узајамно једнозначно пресликавање скупа њихових чворова (из једног на други) које одржава особину суседности чворова.

Дефиниција 2.1.35. *За произвољне графове $G_1 = (X_1, U_1)$ и $G_2 = (X_2, U_2)$ каже се да су изоморфни ако и само ако постоји бијекција φ скупа X_1 на X_2 за коју важи:*

$$(\forall a, b \in X_1)(a, b) \in U_1 \Leftrightarrow (\varphi(a), \varphi(b)) \in U_2.$$

Изоморфизам графа са самим собом назива се *аутоморфизам*. Скуп свих аутоморфизама једног графа са операцијом композиције је група.

2.2 Комбинаторика

У овом одељку, као основа за поглавље 3, уводе се теоријски појмови везани за Фробенијусову теорему. Специјално, као основа за поглавље 3, уводе се појмови везани за циклусни индекс, Појину и де Бројнову теорему.

2.2.1 Фробенијусова теорема

Фробенијусова (Frobenius) теорема даје израз за број орбита скупа под дејством пермутационе групе. У литератури се Фробенијусова теорема често среће под називом Бернсајдова (Burnside) лема. У оквиру доказа теореме користи се неколико лема.

Лема 2.2.1. *Непразан скуп H групе $(G, \cdot)$ је подгрупа ако и само ако за свако $h_1, h_2 \in H$ важи $h_1 \cdot h_2^{-1} \in H$.*

Доказ. Нека је H група и нека $h_1, h_2 \in H$. Из $h_2^{-1} \in H$ следи $h_1 \cdot h_2^{-1} \in H$. Обрнуто, нека за свако $h_1, h_2 \in H$ важи $h_1 \cdot h_2^{-1} \in H$. Специјално, за $h_1 = h_2$ добија се $h_1 \cdot h_1^{-1} \in H$ односно $e \in H$. За $h_1 = e$ добија се $e \cdot h_2^{-1} \in H$ односно $h_2^{-1} \in H$. Коначно, за $h_1, h_2 \in H$ из $h_1 \cdot h_2^{-1} \in H$ и $h_2^{-1} \in H$ следи $h_1 \cdot (h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$, па је H група. □

Следећа теорема даје кардиналност орбите $\mathrm{orb}(x)$.

Лема 2.2.2. *Нека је $G_x = \{g | g \in G,\ g(x) = x\}$. За свако $x \in X$, скуп G_x је подгрупа групе G. Кардиналност орбите $orb(x)$ елемената групе G који фиксирају елемент $x \in X$ једнака је индексу количничке подгрупе $G : G_x$, тј. важи:*

$$|orb(x)| = [G : G_x]$$

Доказ. Нека је $g \in G_x$. Специјално, за идентичку трансформацију g важи $g(x) = x$, тј. $x \in G_x$. Из $x = g^{-1}(g(x)) = g^{-1}(x)$ следи $g^{-1} \in G_x$. За $g_1, g_2 \in G_x$ из $g_1 \cdot g_2^{-1}(x) = g_1(g_2^{-1}(x)) = g_1(x) = x$ следи $g_1 \cdot g_2^{-1} \in G_x$, па на основу леме 2.2.1 следи да је G_x подгрупа групе G.

Посматрајмо било који (рецимо леви) разред $g_1 G_x$ подгрупе G_x и нека је $g_2 \in g_1 G_x$. Пошто је $g_1 G_x$ леви разред, постоји $g \in G_x$ такво да је $g_2 = g_1 \cdot g$. Како је $g_2(x) = g_1 \cdot g(x) = g_1(g(x)) = g_1(x)$, то елементи истог разреда пресликавају x у исти елемент. С друге стране, ако g_1 и g_2 пресликавају x у исти елемент, тј. ако је $g_1(x) = g_2(x)$, тада је $g_2^{-1} g_1(x) = x$. Одавде је $g_2^{-1} \cdot g_1 \in G_x$, тј. g_1 и g_2 припадају истом разреду. Дакле, g_1 и g_2 припадају истом разреду ако и само ако пресликавају x у исти елемент. Према томе, произвољни разред $g_1 G_x$ може се придружити елементу $y = g_1(x) = g_2(x)$ који је у истој орбити са x. Обрнуто, нека је елемент y у истој орбити са x. Тада постоји $g \in G$ такво да је $y = g(x)$, па је y придружен разреду који садржи g. Дакле, постоји бијективно пресликавање између елемената орбите елемента x и разреда групе G у односу на подгрупу G_x. □

Теорема 2.2.1. (Фробенијус) *Број орбита скупа X индукованих дејством пермутационе групе G дат је изразом:*

$$\frac{1}{|G|} \sum_{g \in G} I(g). \tag{2.14}$$

где је $I(g)$ број елемената скупа X које пермутација g фиксира, тј. број циклуса дужине један у пермутацији g.

Доказ. Нека је Кронекеров симбол дефинисан изразом

$$\delta_{i,j} = \begin{cases} 1, & \text{ако је } i = j, \\ 0, & \text{ако је } i \neq j. \end{cases}$$

Број орбита скупа X једнак је

$$\sum_{\mathrm{orb}(x)\subseteq X} 1 = \frac{1}{|G|} \sum_{\mathrm{orb}(x)\subseteq X} |G_x||G : G_x| = \frac{1}{|G|} \sum_{\mathrm{orb}(x)\subseteq X} |G_x||\,\mathrm{orb}(x)| =$$

$$\frac{1}{|G|} \sum_{x\in X} |G_x| = \frac{1}{|G|} \sum_{x\in X} \sum_{g\in G} \delta_{g(x),x} = \frac{1}{|G|} \sum_{g\in G} \sum_{x\in X} \delta_{g(x),x} = \frac{1}{|G|} \sum_{g\in G} I(g)$$

где је $I(g) = \sum_{x\in X} \delta_{g(x),x}$. □

Пример 2.2.1. *Број нееквивалентиних Булових функција из примера 2.1.24 може се израчунати на основу Фробенијусове теореме. Посматра се дејство групе S_2 на бинарне улазе Булових функција $f : B_2 \to B_1$. Под дејством пермутације* (1)(2) *свака од* 16 *Булових функција остаје непромењена. Под дејством пермутације* (1 2)*, мењају се друга и трећа компонента Булових функција, па Булове функције остају непромењене када су им те компоненте исте. Постоји* 8 *таквих функција. Дакле, дејство пермутација из S_2 на два бинарна улаза, производи укупно $16 + 8 = 24$ фиксних тачака. На основу Фробенијусове теореме број орбита индукованих дејством групе S_2 износи $U_2(S_2) = 24/2 = 12$.*

Нека за $x, y \in B_n$, $x \oplus y$ означава компонентно сабирање по модулу 2. Следећи пример илуструје израчунавање броја фиксних тачака за линеарну трансформацију примењену на улазе и излазе.

Пример 2.2.2. *Нека је задат пар инвертибилних матрица*

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

које трансформишу излаз, односно улаз векторске инвертибилне функције $f(x_1, x_2) = (f_1, f_2)(x_1, x_2)$. Услов (A, B) $(fA)(xB) = f(x)$ да функција f буде фиксна тачка трансформације еквивалентан је услову $(fA)(x) = f(xB)$, тј. услову

$$\Big((f_1, f_2) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\Big)(x_1, x_2) = (f_2, f_1)(x_1, x_2) = f\Big((x_1, x_2) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\Big) = f(x_1 \oplus x_2, x_2).$$

Другим речима, функција f је фиксна тачка пара ако за пар функција f_1, f_2 за сваки пар (x_1, x_2) важи идентитет

$$(f_2(x_1, x_2), f_1(x_1, x_2)) = (f_1(x_1 \oplus x_2, x_2), f_2(x_1 \oplus x_2, x_2)).$$

За $x_2 = 0$ добијају се два идентична услова: $f_1(x_1, 0) = f_2(x_1, 0)$. За $x_2 = 1$ добијају се услови: $f_2(x_1, 1) = f_1(\overline{x}_1, 1)$ и $f_1(x_1, 1) = f_2(\overline{x}_1, 1)$. Ове услове задовољавају следеће четири инвертибилне функције:

x_1	x_2	f_1	f_2	f_1	f_2	f_1	f_2	f_1	f_2
0	0	0	0	0	0	1	1	1	1
0	1	0	1	1	0	0	1	1	0
1	0	1	1	1	1	0	0	0	0
1	1	1	0	0	1	1	0	0	1

Дакле, трансформација (A, B) има четири фиксне тачке.

Пример 2.2.3. *За $n = 2$ на основу (2.9) постоји $2 \cdot 1 \cdot 3 = 6$ несингуларних матрица, односно $6^2 = 36$ парова матрица које се могу применити истовремено на улазе и на излазе. Несингуларне матрице реда 2 су следеће матрице:*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Према Фробенијусовој теореми, број класа еквиваленције једнак је количнику броја фиксних тачака и броја примењених трансформација. Непосредним пребројавањем добија се да постоје укупно 72 фиксне тачке.

A	B	*Циклусна структура матрица A и B*	*Број фиксних тачака*
$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	x_1^4	*24*
$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$	x_1x_3	*3*
$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$	x_1x_3	*3*
$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$	$x_1^2x_2$	*4*
$\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$	x_1x_3	*3*
$\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$	$\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$	x_1x_3	*3*

Трансформација (A,B) има фиксне тачке ако и само ако пермутације које реализују матрице A и B имају исту циклусну структуру; то смањује број парова матрица које треба разматрати. За сваки разматрани пар број фиксних тачака може се одредити као у претходном примеру за пар

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

четврти у табели. Поред тога, сви парови са истом структуром циклуса имају исти број фиксних тачака; посао олакшава чињеница да различитих циклусних структура има само три: x_1^4, $x_1^2 x_2$ *и* $x_1 x_3$. *Пошто је број трансформација* $6^2 = 36$, *број класа еквиваленције у односу на линеарну групу је* 2.

Примена Фробенијусове теореме у општем случају није тривијална. Наиме, за групу великог реда потребно је за сваку њену пермутацију одредити број фиксних тачака. Са порастом реда групе, рачунање постаје захтевно. Једно мало упрошћење представља чињеница да конјуговане пермутације имају исту структуру циклуса, па самим тим и исти број фиксних тачака. Стога се у изразу (2.14) може сумирати не по свим пермутацијама већ по класама конјугације.

2.2.2 Израчунавање $U_n(G)$ на основу Појине теореме

Нека је D коначан скуп и нека је G група пермутација скупа D. Нека је R коначан скуп и нека је R^D скуп функција $D \mapsto R$. Група G тада пермутује и функције из R^D.

Функције $f_i, f_j \in R^D$ су еквивалентне ($f_i \sim f_j$) ако постоји $g \in G$ тако да за свако $x \in D$ важи $f_i(x) = f_j(g(x))$. За произвољну функцију $f \in R^D$, нека је $o(f) = \{f' \in R^D,\ f' \sim f\}$. Нека је $F = \{o(f) \mid f \in R^D\}$ скуп свих орбита (класа еквиваленције функција). Појина теорема омогућује израчунавање $|F|$, броја класа еквиваленције функција.

Теорема 2.2.2 (Појина теорема)**.** *Број класа еквиваленције у скупу функција* R^D *једнак је*

$$\left|R^D/G\right| = \frac{1}{|G|} \sum_{g \in G} m^{c(g)},$$

где је $m = |R|$ *и* $c(g)$ *је број циклуса елемента* $g \in G$ *када се он посматра као пермутација скупа* D.

Доказ. Функција $f \in R^D$ је фиксна тачка пермутације $g \in G$ ако и само ако на свим орбитама (циклусима) има константну вредност. Према томе, број фиксних тачака пермутације g добија се степеновањем m на број циклуса пермутације g. На основу Фробенијусове теореме број класа еквиваленције функција $f \in R^D$ је

$$\left|R^D/G\right| = \frac{1}{|G|}\sum_{g\in G} m^{c(g)}.$$

□

Ако је G група пермутација степена m, и ако је циклусни индекс групе G када делује на D једнак

$$Z_G(x_1,\ldots,x_m) = \frac{1}{|G|}\sum_{g\in G} x_1^{k_1(g)}\cdots x_m^{k_m(g)},$$

где је $k_i(g)$ број циклуса дужине i у пермутацији g, $1 \leqslant i \leqslant m$, онда је број класа еквиваленције функција $f \in R^D$ једнак

$$\frac{1}{|G|}\sum_{g\in G} m^{k_1(g)+\cdots+k_m(g)} = Z_G(m,m,\ldots,m).$$

Последица 2.2.1. *Специјално, ако је*

$$\begin{aligned} Z_G(f) &= \frac{1}{|G|}\sum_{g\in G} f^{\mathrm{type}(g)} = \frac{1}{|G|}\sum_{p\in P_n} g(p) f_1^{p_1} f_2^{p_2}\cdots f_n^{p_n} \\ &= \frac{1}{|G|}\sum_{p\in P_n} g(p) f^p. \end{aligned}$$

циклусни индекс групе G, једне од четири типа разматраних група, тада је

$$U_n(G) = Z_G(2,2,\ldots,2) = \frac{1}{|G|}\sum_{p\in P_N} g(p) 2^{\sum_{i=1}^{N} p_i}. \tag{2.15}$$

Пример 2.2.4. *Матрица* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *из групе* $\mathrm{GL}(2,2)$*, (видети пример 2.2.3) реализује следећу пермутацију скупа вектора B_2:*

$$\begin{bmatrix}0\\0\end{bmatrix} \to \begin{bmatrix}0\\0\end{bmatrix},\ \begin{bmatrix}0\\1\end{bmatrix} \to \begin{bmatrix}1\\1\end{bmatrix},\ \begin{bmatrix}1\\0\end{bmatrix} \to \begin{bmatrix}1\\0\end{bmatrix},\ \begin{bmatrix}1\\1\end{bmatrix} \to \begin{bmatrix}0\\1\end{bmatrix}.$$

Два бинарна вектора сликају се у себе саме, а преостала два чине циклус дужине 2, па је моном који одговара циклусној структури пермутације индуковане овом матрицом $x_1^2x_2$. Узимајући у обзир и остале матрице из групе

$\mathrm{GL}(2,2)$, *добија се циклусни индекс*

$$Z_{\mathrm{GL}(2,2)}(x_1,x_2,x_3)=\frac{1}{6}\left(x_1^4+3x_1^2x_2+2x_1x_3\right).$$

На основу Појине теореме број класа еквиваленције Булових функција од две променљиве у односу на групу $\mathrm{GL}(2,2)$ *једнак је*

$$U_2(\mathrm{GL}(2,2))=Z_{\mathrm{GL}(2,2)}(2,2,2)=\frac{1}{6}\left(2^4+3\cdot 2^2\cdot 2+2\cdot 2\cdot 2\right)=8.$$

Пример 2.2.5. *Нека је* C_2^n *група трансформација Булових функција од* n *променљивих коју чине комплементирања* g_a, $a=(a_1,\ldots,a_n)\in B_n$, *подскупова променљивих* $\{x_i \mid a_i=1,\ 1\leqslant i\leqslant n\}$. *Ред групе* C_2^n *је* 2^n. *Комплементирање променљиве означава се надвлачењем те променљиве. На пример,* $g_{(1,0,0)}(f(x_1,x_2,x_3))=f(\bar{x_1},x_2,x_3)$. *Функције* f_1 *и* f_2 *су еквивалентне ако за неко* $g\in C_2^n$ *важи* $f_1(x)=f_2(g(x))$. *За сваку од* 2^n *трансформација групе* G *могу се одредити циклусне структуре. Идентичка трансформација* $g_{(0,0,\ldots,0)}$ *има* 2^n *једночланих циклуса. Све остале трансформације имају по* 2^{n-1} *циклуса дужине* 2 *(транспозиција) одакле се добија циклусни индекс*

$$Z_{C_2^n}(x_1,x_2)=\frac{1}{2^n}\left(x_1^{2^n}+(2^n-1)x_2^{2^{n-1}}\right).$$

На основу Појине теореме број класа еквиваленције Булових функција од две променљиве у односу на групу C_2^n *једнак је*

$$U_n(C_2^n)=Z_{C_2^n}(2,2)=\frac{1}{2^n}(2^{2^n}+(2^n-1)2^{2^{n-1}}).$$

2.2.3 Израчунавање $V_n(G)$ на основу Де Бројнове теореме

Де Бројн (De Bruijn) [5, 6] је разматрао генерализацију Појине (Pólya) [32] теореме на случај када не само на скуп D, већ и на скуп R делује пермутациона група. Другим речима, разматрају се две пермутационе групе G и H, од којих прва делује на скуп D, друга на скуп R [5, 6]. Две функције f_1, f_2 из R^D су еквивалентне, $f_1\sim f_2$, ако постоје пермутације $g\in G$ и $h\in H$, такве да за свако $d\in D$ важи $f_1(g(d))=h(f_2(d))$. Релација $\sim$ је релација еквиваленције, па се скуп R^D може поделити на класе еквиваленције - шаблоне. Свакој функцији $f\in R^D$ додељује се тежина $W(f)$, уз услов да еквивалентне функције имају исту тежину, тј. из $f_1\sim f_2$ следи $W(f_1)=W(f_2)$. Шаблону

F додељује се тежина $W(f)$ која је једнака тежини било које функције $f \in F$ из шаблона. Потребно је одредити инвентар шаблона, односно суму тежина свих шаблона.

За функцију $f = f(x_1, \ldots, x_n)$ од више промењљивих, као што је уобичајено, $\frac{\partial f}{\partial x_i}$ означава парцијални извод по промењљивој x_i, $1 \leqslant i \leqslant n$.

Теорема 2.2.3. *Инвентар шаблона за функције $f \in R^D$ уз претходно дефинисану класу еквиваленције износи:*

$$\sum_{F \in \mathcal{F}} W(F) = \frac{1}{|G||H|} \sum_{g \in G} \sum_{h \in H} \sum_{fg = hf} W(f)$$

где је $\mathcal{F}$ скуп свих шаблона, а $\sum_{f}^{(g,h)} W(f)$ означава суму свих тежина $W(f)$ функција f таквих да важи $fg = hf$.

Доказ. Нека је w једна од могућих вредности тежине W и нека је S скуп свих функција $f \in R^D$ таквих да важи $W(f) = w$. Нека је на Декартовом производу $G \times H$ који се састоји од свих производа $g \times h$ за $g \in G, h \in H$ множење дефинисано једнакошћу:

$$(g \times h)(g' \times h') = (gg') \times (hh').$$

Сваком пару $g \times h \in G \times H$ доделимо функцију $\pi_{g \times h} : S \mapsto S$ дефинисану једнакошћу:

$$\pi_{g \times h} f_1 = f_2 \Leftrightarrow f_2 = h f_1 g^{-1}.$$

Докажимо да је $\pi_{g \times h}$ пермутација скупа S. Из $f_2 = h f_1 g^{-1}$ следи $f_1 \sim f_2$ па је $W(f_1) = W(f_2)$, тј. $\pi_{g \times h}$ пресликава скуп S у себе самог ($\pi_{g \times h} : S \to S$). Поред тога, $\pi_{g \times h}$ има инверзну функцију, пошто важи

$$h^{-1} f_2 (g^{-1})^{-1} = h^{-1} h f_1 g^{-1} (g^{-1})^{-1} = f_1.$$

Дакле, $\pi_{g \times h}$ је пермутација скупа S. Даље, пресликавање $g \times h \to \pi_{g \times h}$ представља хомоморфизам. Заиста, ако $g, g' \in G,\ h, h' \in H$, онда за свако $f \in S$ важи

$$\pi_{(g \times h)(g' \times h')} f = \pi_{gg' \times hh'} f = (hh') f (gg')^{-1}$$

и

$$\pi_{g \times h}(\pi_{g' \times h'} f) = \pi_{g \times h}(h' f g'^{-1}) = h(h' f g'^{-1}) g^{-1}$$

одакле следи:

$$\pi_{(g\times h)(g'\times h')} = \pi_{g\times h}\pi_{g'\times h'}.$$

Две функције f_1 и f_2 (два елемента скупа S) су еквивалентне ако постоје g и h такве да важи $\pi_{g\times h}f_2 = f_1$. Према томе, на основу Фробенијусове теореме, број шаблона који припадају скупу S износи:

$$\frac{1}{|G||H|}\sum_{g\in G}\sum_{h\in H}\psi_w(g,h), \tag{2.16}$$

где је $\psi_w(g,h)$ број функција f таквих да је $W(f) = w$ и $\pi_{g\times h}f = f$ (односно $hf = fg$). Када се израз (2.16) помножи са w и сумира по свим могућим вредностима за w, из чињенице да је збир тежина свих функција (које задовољавају наведене услове) једнак суми производа шаблона и њихових тежина, тј.

$$\sum_w \psi_w(g,h)w = \sum_{fg=hf} W(f),$$

следи тврђење теореме. □

Размотримо сада шаблоне 1-1 пресликавања. Дефинишимо тежину $W(f)$ било које функције $f \in R^D$ једнакошћу:

$$W(f) = \begin{cases} 1, & f \text{ је } 1-1 \\ 0, & f \text{ није } 1-1 \end{cases}$$

За $g \in G, h \in H$ пресликавање hfg^{-1} је 1-1 ако и само ако је f 1-1, па тежина $W(f)$ задовољава услов константности на класи еквиваленције функција:

$$f_1 = hf_2g^{-1} \Rightarrow W(f_1) = W(f_2), \text{ тј. } f_1 \sim f_2 \Rightarrow W(f_1) = W(f_2).$$

Теорема 2.2.4. *Број шаблона за 1-1 функције $f \in R^D$ уз претходно дефинисану релацију еквиваленције износи:*

$$Z_G\big(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \frac{\partial}{\partial x_3}, \dots\big) Z_H(1+x_1, 1+2x_2, 1+3x_3, \dots),$$

при чему се вредност израза рачуна у тачки $x_1 = x_2 = x_3 = \cdots = 0$.

Доказ. Да би се на основу теореме 2.2.3 одредио инвентар шаблона $\sum W(F)$ (једнак броју шаблона 1-1 функција), потребно је прво израчунати $\sum_{fg=hf} W(f)$.

Нека су $g \in G$ и $h \in H$ фиксиране пермутације. Нека је g типа $(b_1, b_2, b_3, \dots)$ и h типа $(c_1, c_2, c_3, \dots)$ (овде b_i, односно c_i, означавају број циклуса дужине i). Потребно је пронаћи број 1-1 пресликавања $f : D \mapsto R$ која задовољавају услов $fg = hf$, односно треба пронаћи број фиксних тачака.
Нека је f пресликавање које задовољава услов $fg = hf$ и нека елемент $d \in D$ припада циклусу дужине i. Тај циклус се састоји од елемената:

$$d,\ gd,\ g^2d, \dots, g^{i-1}d. \tag{2.17}$$

Пошто је циклус дужине i, важи $g^id = d$. Из $fg = hf$ следи:

$$fg^2 = fgg = hfg = hhf = h^2f$$

и слично:

$$fg^3 = fg^2g = h^2fg = h^2hf = h^3f.$$

Генерално, за произвољно i важи $h^ifd = fg^id = fd$. Дакле, елементе из циклуса (2.17) f слика у елементе:

$$h^ifd,\ hfd,\ h^2fd, \dots, h^{i-1}fd. \tag{2.18}$$

Из $h^ifd = fd$ следи да дужина циклуса из скупа R коме припада елемент fd мора бити делилац броја i.
До сада смо посматрали произвољну функцију $f \in R^D$. Ако се додатно уведе услов да је f 1-1 пресликавање, онда два различита елемента из (2.17) не могу добити исту вредност међу елементима из (2.18), односно међу елементима из списка (2.18) нема понављања. Одатле следи да је дужина циклуса коме припада елемент fd једнака i. Другим речима, циклус из D дужине i пресликава се у циклус из R који је такође дужине i. Пошто је f 1-1, различити циклуси из D сликају се у различите циклусе из R.
Сада је јасно да је при конструкцији 1-1 функције f, која задовољава услов $fg = gh$, потребно сваком циклусу из D узајамно једнозначно доделити циклус исте дужине из R. Приликом доделе циклуса дужине i из D циклусу из R, због кружне повезаности елемената унутар циклуса, могуће је сваком елементу циклуса из D доделити i елемената придруженог циклуса из R. Ако је скуп D састављен од b_i циклуса и скуп R од c_i циклуса дужине i, тада се таквим циклусима из D могу придружити циклуси из R на $\frac{c_i!}{(c_i-b_i)!} = c_i(c_i-1)(c_i-2)\cdots(c_i-b_i+1)$ начина. Ако је $c_i < b_i$, онда такво $1-1$

пресликавање не постоји; у производу неки чинилац постаје нула (за неко k, $c_i + k = b_i$), па је број пресликавања нула. Дакле, број $1-1$ пресликавања $f : D \to R$, $fg = gh$ једнак је:

$$\sum_{f}^{(g,h)} W(f) = \prod_{i:b_i>0} i^{b_i} c_i(c_i - 1)\cdots(c_i - b_i + 1). \tag{2.19}$$

Ако је $b_i = 0$, онда је производ $c_i \cdots (c_i - 0 + 1)$ без чинилаца, па се може сматрати да је једнак 1. Производ $i^c c(c-1)(c-2)\cdots(c-b+1)$ у ствари представља парцијални извод b-тог реда израза $(1+ix)^c$ по променљивој x у тачки $x = 0$. Због тога се производ у (2.19) може заменити низом парцијалних извода по променљивама $x_1, x_2, x_3, \dots$

$$\Big(\frac{\partial}{\partial x_1}\Big)^{b_1}\Big(\frac{\partial}{\partial x_2}\Big)^{b_2}\Big(\frac{\partial}{\partial x_3}\Big)^{b_3}\cdots(1+x_1)^{c_1}(1+2x_2)^{c_2}(1+3x_3)^{c_3}\cdots \tag{2.20}$$

у тачки $x_1 = x_2 = x_3 = \cdots = 0$.

Полазна претпоставка је била да су пермутације $g \in G$ и $h \in H$ фиксиране. Проласком кроз све пермутације $g \in G$ и $h \in H$ и дељењем са $|G||H|$, израз (2.20) постаје инвентар шаблона за $1-1$ пресликавања, што у овом случају уједно представља и број шаблона за $1-1$ пресликавања. Диференцијални оператор у (2.20) добија се од монома циклусног индекса $Z_G(z_1, z_2, \dots)$ заменама $z_i = \frac{\partial}{\partial x_i}$. Операнд у том изразу добија се заменама $z_i = 1 + ix_i$ у члану циклусног индекса $Z_H(z_1, z_2, \dots)$. Сумирањем се долази до тврђења теореме. □

У случају $|R| < |D|$ број $1-1$ пресликавања је нула. Пресликавање $1-1$ у случају $|R| = |D|$ постаје и „на" пресликавање, односно бијекција, па можемо формулисати следећу теорему.

Теорема 2.2.5. *Број шаблона за бијективне функције $f \in R^D$ уз претходно дефинисану релацију еквиваленције једнак је вредности израза*

$$Z_G\Big(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \frac{\partial}{\partial x_3}, \dots\Big) Z_H(x_1, 2x_2, 3x_3, \dots). \tag{2.21}$$

израчунатој у тачки $x_1 = x_2 = x_3 = \cdots = 0$.

Доказ. Из претпоставке $|D| = |R|$, следи $\sum_i b_i = \sum_i c_i$, па постоје две могућности: или је $b_1 = c_1, b_2 = c_2, \dots$ или је бар за један индекс i $b_i > c_i$.

У другом случају производ $\prod_{i:b_i>0} i^{b_i}c_i(c_i-1)\cdots(c_i-b_i+1)$ постаје нула и самим тим израз $Z_G\big(\frac{\partial}{\partial x_1},\frac{\partial}{\partial x_2},\frac{\partial}{\partial x_3},\dots\big)Z_H(1+x_1,1+2x_2,1+3x_3,\dots)$ постаје нула. Дакле, мора бити $b_1=c_1,b_2=c_2,\dots,b_i=c_i,\dots$ па је:

$$\prod_{i:b_i>0} i^{b_i}c_i(c_i-1)\cdots(c_i-b_i+1)=\prod_{i:b_i>0} i^{b_i}c_i(c_i-1)\cdots 1=\prod_{i:b_i>0} i^{b_i}c_i!.$$

Како за $b=c$ важи $i^c c!=\big(\frac{\partial}{\partial x}\big)^c(ix)^c=\big(\frac{\partial}{\partial x}\big)^b(ix)^c=i^b c!$ у тачки $x=0$, следи да производ $i^b c!$ представља b-ти парцијални извод израза $(ix)^c$ променљиве x у тачки $x=0$. Самим тим израз (2.20) увек има исту вредност као израз

$$\big(\frac{\partial}{\partial x_1}\big)^{b_1}\big(\frac{\partial}{\partial x_2}\big)^{b_2}\big(\frac{\partial}{\partial x_3}\big)^{b_3}\cdots(x_1)^{c_1}(2x_2)^{c_2}(3x_3)^{c_3}\cdots \tag{2.22}$$

израчунат у тачки $x_1=x_2=x_3=\cdots=0$. □

Пошто бијективно пресликавање из D у R подразумева да постоји инверзно пресликавање из R у D, у претходном производу циклусних индекса групе трансформација могу заменити места:

$$Z_G\big(\frac{\partial}{\partial x_1},\frac{\partial}{\partial x_2},\dots\big)Z_H(x_1,2x_2,\dots)=Z_H\big(\frac{\partial}{\partial x_1},\frac{\partial}{\partial x_2},\dots\big)Z_G(x_1,2x_2,\dots) \tag{2.23}$$

Последица 2.2.2. *Специјално, ако је*

$$\begin{aligned} Z_G(f) &= \frac{1}{|G|}\sum_{g\in G} f^{\mathrm{type}(g)}=\frac{1}{|G|}\sum_{p\in P_n} g(p)f_1^{p_1}f_2^{p_2}\cdots f_n^{p_n}\\ &= \frac{1}{|G|}\sum_{p\in P_n} g(p)f^p. \end{aligned}$$

циклусни индекс групе G, једне од четири типа разматраних група, тада је

$$\begin{aligned} V_n(G) &= Z_G\big(\frac{\partial}{\partial t_1},\frac{\partial}{\partial t_2},\dots,\frac{\partial}{\partial t_N}\big)\cdot\\ &\quad Z_G(t_1,2t_2,\dots,Nt_N)\big|_{t_1=\cdots=t_N=0}\\ &= \frac{1}{|G|^2}\sum_{p\in P_N} g(p)^2\prod_{i=1}^{N} i^{p_i}p_i!. \end{aligned} \tag{2.24}$$

Следећа теорема може олакшати рачунање израза (2.22).

Теорема 2.2.6. *Сабирак облика:*

$$\Big[p\Big(\frac{\partial^{b_1}}{\partial x_{i_1}}\frac{\partial^{b_2}}{\partial x_{i_2}}\cdots\frac{\partial^{b_s}}{\partial x_{i_s}}\Big)q\Big((k_1x_{k_1})^{c_1}(k_2x_{k_2})^{c_2}\cdots(k_sx_{k_s})^{c_s}\Big)\Big]_{x_1=x_2=\cdots=x_s=0}$$

једнак је:

$$\begin{cases} pq\prod_{r=1}^{s} k_r^{b_r} b_r!, \text{ ако } i_1 = k_1, \ldots, i_s = k_s \\ 0, \text{ у супротном} \end{cases} \tag{2.25}$$

Доказ. Важи $b_1 = c_1, b_2 = c_2, \ldots b_s = c_s$. Треба приметити да уколико структура циклуса израза у диференцијалном оператору није иста као у изразима ван њега, резултат диференцирања је нула. Структура циклуса биће иста за $i_1 = k_1, \ldots, i_s = k_s$, одакле после примене диференцирања следи (2.25). □

Пример 2.2.6. *У случају инвертибилних Булових функција група C_2^n делује и на улазе и на излазе. Број различитих комплементирања улазних и излазних променљивих је $|G_x| = |G_f| = 2^n$, па је укупан број транформација $|G| = |G_x| \cdot |G_f| = 2^n 2^n = 2^{2n}$. Број фиксних тачака идентичке трансформације је једнак је броју Булових инвертибилних функција $2^n!$. Из циклусног индекса (видети пример 2.2.5) види се да постоји $2^n - 1$ неидентичких пермутација са по 2^{n-1} двочланих циклуса, што значи да се типови улазних и излазних циклуса поклапају у $(2^n - 1) \cdot (2^n - 1) = (2^n - 1)^2$ случајева. Број фиксних тачака неидентичке трансформације је $2^{n-1}!2^{2^{n-1}}$:*

- *2^{n-1} двочланих циклуса између себе могу заменити места на $2^{n-1}!$ начина, чиме Булова инвертибилна функција остаје непромењена.*
- *Уколико се примени кружна замена елемената унутар сваког двочланог циклуса, такође се добија фиксна тачка. Таквих замена има $2^{2^{n-1}}$.*

Према томе, број класа еквиваленције за инвертибилне Булове функције под дејством C_2^n износи:

$$V_n(C_2^n) = \frac{2^n! + (2^n - 1)^2 \cdot 2^{n-1}! \cdot 2^{2^{n-1}}}{2^{2n}}.$$

До истог резултата долази се применом теореме 2.2.5, која даје број класа еквиваленције када група C_2^n делује на улазе и на излазе:

$$Z_{C_2^n}\Big(\frac{\partial}{\partial x_1}\frac{\partial}{\partial x_2}\Big) Z_{C_2^n}\Big(x_1, 2x_2\Big) = \frac{1}{2^n}\Big(\frac{\partial^{2^n}}{\partial x_1} + (2^n - 1)\frac{\partial^{2^{n-1}}}{\partial x_2}\Big)\frac{1}{2^n}\Big(x_1^{2^n} + (2^n - 1)(2x_2)^{2^{n-1}}\Big)$$

Применом леме 2.2.6 или директним рачунањем добијају се чланови различити од нуле:

$$\frac{\partial^{2^n}}{\partial x_1} x_1^{2^n} = 2^n! \qquad \frac{\partial^{2^{n-1}}}{\partial x_2}(2x_2)^{2^{n-1}} = 2^{2^{n-1}} 2^{n-1}!$$

Према томе, тражени број класа еквиваленције једнак је:

$$Z_{C_2^n}\Big(\frac{\partial}{\partial x_1}\frac{\partial}{\partial x_2}\Big)Z_{C_2^n}\Big(x_1, 2x_2\Big) = \frac{2^n! + (2^n-1)^2 \cdot 2^{n-1}! \cdot 2^{2^{n-1}}}{2^{2n}}.$$

2.3 Циклусни индекси за четири групе трансформација

Нека су S'_n, G_n, GL_n и AGL_n редом група пермутација, група композиције пермутација и комплементирања променљивих, линеарна група и афина група које делују на B_n. У овом одељку приказује се поступак израчунавања циклусних индекса за све четири групе трансформација.

Де Бројн ([5, 6]) уводи уопштење Појине теореме [32]. Ашенхурст (Ashenhurst [2]) и Слепијан (Slepian [36]) изводе уопштени образац за Z_{G_n}. На основу њихових радова, Харисон [22, 23, 24] је извео изразе за циклусни индекс за S'_n, G_n, GL_n и AGL_n и приказује њихове вредности за $n \leqslant 6$. У циљу рачунања V_n, Применко (Primenko [33]) користи алтернативни приступ.

2.3.1 Група пермутација

Теорема 2.3.1. *Ако је d дужина циклуса пермутације $\sigma'_n \in S'_n$ индукованог циклусом $\sigma_n \in S_n$ дужине k, онда важи $d|k$.*

Доказ. За било који елемент $x \in B_n$ важи $\sigma^k(x) = x$. То значи да орбита елемента x има највише k елемената, тј. $d \leqslant k$. Из чињенице да је $\sigma^d(x) = x$ следи $d|k$. □

Пример 2.3.1. *За $n = k = 6$, $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$, орбита елемента* 001001 *је величине* 3 *($\sigma^3(001001) = 001001$), а орбита елемента* 010101 *је величине* 2 *($\sigma^2(010101) = 010101$). У оба случаја величина орбите дели $k = 6$.*

Нека је $e(d)$ број орбита дужине d у $\sigma' \in S'_n$. Циклус дужине k када делује на елементе скупа B^k, разлаже тај скуп на $e(d)$ орбита дужине d за све $d|k$, па је

$$e(k) = \begin{cases} 2, & k = 1 \\ \frac{1}{k}\left(2^k - \sum_{d|k, d\neq k} d \cdot e(d)\right), & k > 1. \end{cases} \tag{2.26}$$

Низ $e(n)$ такође означава број несводљивих полинома степена n над пољем GF(2) (или број различитих огрлица од n-перли обојених у 2 боје - огрлице

су апериодичне (не састоје се од поновљених низова, односно примитивни период је n), а бројање се врши „без превртања“ (без обртања редоследа перли) видети [30, низ A001037]).

Пример 2.3.2. *Могуће огрлице од* 5 *перли када замена две боје није дозвољена су:* $PPPPB, BBBBP, PPPBB, BBBPP, PBPPB, BPBBP$. *Уз дозвољену замену боја, парови који се међусобно преклапају представљају исту боју, па су такве огрлице облика:* $PPPPB, PPPBB, PBPPB$. *Дакле,* $e(5) = 6$.

Неколико ненула чланова низа $e(n)$ приказани су у табели 2.7.

Табела 2.7: Низ e.

n	1	2	3	4	5	6	7	8	9	10
$e(n)$	2	1	2	3	6	9	18	30	56	99

Теорема 2.3.2. *Циклус дужине* k *пермутације* $\sigma \in S_n$ *индукује циклус пермутације* $\sigma' \in S'_n$ *са циклусном структуром:*

$$\prod_{d|k} f_d^{e(d)}.$$

Пример 2.3.3. *Специјално, ако је* k *прост број, тада циклус дужине* k *индукује циклусну структуру* $f_1^2 f_k^{\frac{2^k-2}{k}}$, *тј. пермутацију која има две фиксне тачке и* $(2^k-2)/k$ *циклуса дужине* k. *На основу мале Фермаове теореме* $\frac{2^k-2}{k}$ *је цео број.*

Последица 2.3.1. *Пермутација* $\sigma \in S_n$ *типа* $p = \mathrm{type}(\sigma) \in P_n$ *индукује партицију типа* $\mathrm{type}(\sigma') = p' = (p'_1, p'_2, \ldots, p'_N)$ *са циклусном структуром*

$$f^{p'} = \bigtimes_{\substack{1 \leqslant j \leqslant n \\ p_j > 0}} \left(\prod_{d|j} f_d^{e(d)} \right)^{\times p_j}.$$

Пример 2.3.4. *За* $n = 4$ *постоје следеће партиције скупа од* n *елемената*

$$(0,0,0,1), (0,2,0,0), (1,0,1,0), (2,1,0,0), (4,0,0,0)$$

Овим партицијама одговарају редом пермутације са циклусном структуром одређеном мономима $t_4,\ t_2^2,\ t_1t_3,\ t_1^2t_2,\ t_1^4$. *На основу теореме 2.3.2 добијају се*

мономи који одговарају циклусним структурама одговарајућих индукованих пермутација из S_4'*:*

$$t_4 \to f_1^2 f_2 f_4^3, \quad t_2^2 = t_2 t_2 \to f_1^2 f_2 \times f_1^2 f_2, \quad t_1 t_3 \to f_1^2 \times f_1^2 f_3^2$$

$$t_1^2 t_2 = t_1 t_1 t_2 \to f_1^2 \times f_1^2 \times f_1^2 f_2 \quad t_1^4 = t_1 t_1 t_1 t_1 \to f_1^2 \times f_1^2 \times f_1^2 \times f_1^2$$

Пример 2.3.5. *Посматрајмо пермутацију из* S_4 *са структуром која одговара моному* $t_1 t_3$*. Из примера 2.3.4 коресподенција између* S_4 *и* S_4' *представљена је са* $t_1 t_3 \to f_1^2 \times f_1^2 f_3^2$*. Циклус* t_3 *делује на следећи начин:*

x_1	x_2	x_3	$p(x_1)$	$p(x_2)$	$p(x_3)$
0	0	0	0	0	0
0	0	1	1	0	0
0	1	0	0	0	1
0	1	1	1	0	1
1	0	0	0	1	0
1	0	1	1	1	0
1	1	0	0	1	1
1	1	1	1	1	1

Циклус (1 2 3) *индукује циклусе* (0)(1 4 2)(3 5 6)(7)*, тј.* t_3 *индукује* $f_1^2 f_3^2$*.*

Пример 2.3.6. *На елементе из* B_4 *пермутација* (1)(2 3 4) *са циклусном структуром* $t_1 t_3$ *делује на следећи начин:*

x_1	x_2	x_3	x_4	$p(x_1)$	$p(x_2)$	$p(x_3)$	$p(x_4)$
0	0	1	0	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	0
0	0	1	1	0	1	0	1
0	1	0	0	0	0	1	0
0	1	0	1	0	1	1	0
0	1	1	0	0	0	1	1
0	1	1	1	0	1	1	1
1	0	0	0	1	0	0	0
1	0	0	1	1	1	0	0
1	0	1	0	1	0	0	1
1	0	1	1	1	1	0	1
1	1	0	0	1	0	1	0
1	1	0	1	1	1	1	0
1	1	1	0	1	0	1	1
1	1	1	1	1	1	1	1

Прва колона излаза (пета колона табеле) је резултат дејства циклуса дужине 1*, док последње три колоне представљају* t_3*. Уколико изузмемо прву колону у улазу и излазу, горња и доња половина табеле су исте и идентичне са табелом из претходног примера. Према томе, циклусној структури индуковане пермутације одговара моном* $f_1^4 f_3^4$*.*

Претходно разматрање може се интерпретирати и на следећу начин: Нека су $A = \{a_1, b_1\}$ *и* $B = \{a_2, b_2, c_2, d_2, e_2, f_2, g_2, h_2\}$*. Нека на скуп* A *делује пермутација* $(a_1)(b_1)$*, а на скуп* B *пермутација* $(a_2)(b_2\ c_2\ d_2)(e_2\ f_2\ g_2)(h_2)$*. Тада се могу формирати следећи циклуси индуковане пермутације над скупом* $A \times B$*:*

$$(a_1, a_2)$$

$$(a_1, h_2)$$

$$(b_1, a_2)$$

$$(b_1, h_2)$$

$$(a_1, b_2) \to (a_1, c_2) \to (a_1, d_2)$$

$$(a_1, e_2) \to (a_1, f_2) \to (a_1, g_2)$$

$$(b_1, b_2) \to (b_1, c_2) \to (b_1, d_2)$$

$$(b_1, e_2) \to (b_1, f_2) \to (b_1, g_2)$$

Дакле, производ $f_1^2 \times f_1^2 f_3^2$ *представља упаривање елемената између скупа од* 2 *елемента и скупа од* $1 \cdot 2 + 3 \cdot 2 = 8$ *елемената. Унутар првог скупа (пермутације) постоје два једночлана циклуса, док унутар другог скупа постоје два једночлана и два трочлана циклуса. Циклусна форма првог скупа утиче на циклусну форму другог скупа, тако што се упарују циклуси првог скупа са циклусима другог скупа:* $f_1^2 \times f_1^2 f_3^2 = (f_1^2 \times f_1^2)(f_1^2 \times f_3^2) = f_1^4 f_3^4$. *Треба приметити да се унутар приказаних циклуса налазе сви парови из скупа* $A \times B$.

Циклусни индекс групе S'_n дат је формулом

$$Z_{S'_n}(f) = \frac{1}{n!} \sum_{p \in P_n} \frac{n!}{\prod_{i=1}^{n} i^{p_i} p_i!} \bigtimes_{\substack{1 \leqslant j \leqslant n \\ p_j > 0}} \left(\prod_{d|j} f_d^{e(d)} \right)^{\times p_j}, \tag{2.27}$$

Пример 2.3.7. *На основу теореме 2.3.2*

$$Z(S'_3) = \frac{f_1^8 + 2f_1^2 f_3^2 + 3f_1^4 f_2^2}{6}$$

па је на основу (2.15)

$$U_3(S'_3) = \frac{2^8 + 2 \cdot 2^2 \cdot 2^2 + 3 \cdot 2^4 \cdot 2^2}{6} = 80.$$

и на основу (2.24)

$$V_3(S'_3) = \frac{1^2 \cdot 1^8 \cdot 8! + \cdot 2^2 \cdot 1^2 \cdot 2! \cdot 3^2 \cdot 2! + 3^2 \cdot 1^4 \cdot 4! \cdot 2^2 \cdot 2!}{36} = 1172.$$

Табела 2.8 приказује циклусни индекс $Z_{S'_n}(f)$ за $1 \leqslant n \leqslant 8$, видети на пример [24].

2.3.2 Група пермутација и комплементирања

Нека је $C_2^n = \{(i_1, \ldots, i_n) \mid i_j \in \{0, 1\},\ 1 \leqslant j \leqslant n\}$. Ако је $i = (i_1, \ldots, i_n) \in C_2^n$, дефинишимо $i(x_1, \ldots, x_n) = (x_1^{i_1}, \ldots, x_n^{i_n})$ где је

$$x_j^{i_j} = \begin{cases} x_j, & i_j = 0 \\ \bar{x}_j, & i_j = 1 \end{cases}$$

Табела 2.8: Циклусни индекс $Z_n(S'_n)$, $1 \leqslant n \leqslant 8$.

n	$Z_n(S'_n)$
1	f_1^2
2	$\frac{1}{2}\left(f_1^4 + f_1^2 f_2\right)$
3	$\frac{1}{6}\left(f_1^8 + 3f_1^4 f_2^2 + 2f_1^2 f_3^2\right)$
4	$\frac{1}{24}\left(f_1^{16} + 6f_1^8 f_2^4 + 3f_1^4 f_2^6 + 8f_1^4 f_3^4 + 6f_1^2 f_2 f_4^3\right)$
5	$\frac{1}{120}\left(f_1^{32} + 10f_1^{16} f_2^8 + 15f_1^8 f_2^{12} + 20f_1^8 f_3^8 + 30f_1^4 f_2^2 f_4^6 + 20f_1^4 f_2^2 f_3^4 f_6^2 + 24f_1^2 f_5^6\right)$
6	$\frac{1}{720}\left(f_1^{64} + 15f_1^{32} f_2^{16} + 45f_1^{16} f_2^{24} + 40f_1^{16} f_3^{16} + 15f_1^8 f_2^{28} + 90f_1^8 f_2^4 f_4^{12} + 120f_1^8 f_2^4 f_3^8 f_6^4 + 40f_1^4 f_3^{20} f_1^4 + 90f_2^6 f_4^{12} + 144f_1^4 f_5^{12} + 120f_1^2 f_2 f_3^2 f_6^9\right)$
7	$\frac{1}{5040}\left(f_1^{128} + 21f_1^{64} f_2^{32} + 105f_1^{32} f_2^{48} + 70f_1^{32} f_3^{32} + 105f_1^{16} f_2^{56} + 210f_1^{16} f_2^8 f_4^{24} + 420f_1^{16} f_2^8 f_3^{16} f_6^8 + 280f_1^8 f_3^{40} + 630f_1^8 f_2^{12} f_4^{24} + 504f_1^8 f_5^{24} + 210f_1^8 f_2^{12} f_3^8 f_6^{12} + 840f_1^4 f_2^2 f_3^4 f_6^{18} + 504f_1^4 f_2^2 f_5^{12} f_{10}^6 + 420f_1^4 f_2^2 f_3^4 f_4^6 f_6^2 f_{12}^6 + 720f_1^2 f_7^{18}\right)$
8	$\frac{1}{40320}\left(f_1^{256} + 28f_1^{128} f_2^{64} + 210f_1^{64} f_2^{96} + 112f_1^{64} f_3^{64} + 420f_1^{32} f_2^{112} + 420f_1^{32} f_2^{16} f_4^{48} + 1120f_1^{32} f_2^{16} f_3^{32} f_6^{16} + 105f_1^{16} f_2^{120} + 1120f_1^{16} f_3^{80} + 2520f_1^{16} f_2^{24} f_4^{48} + 1344f_1^{16} f_5^{48} + 1680f_1^{16} f_2^{24} f_3^{16} f_6^{24} + 1260f_1^8 f_2^{28} f_4^{48} + 3360f_1^8 f_2^4 f_3^8 f_6^{36} + 1120f_1^8 f_2^4 f_3^{40} f_6^{20} + 4032f_1^8 f_2^4 f_5^{24} f_{10}^{12} + 3360f_1^8 f_2^4 f_3^8 f_4^{12} f_6^4 f_{12}^{12} + 1260f_1^4 f_2^6 f_4^{60} + 3360f_1^4 f_2^6 f_3^4 f_6^{38} + 5760f_1^4 f_7^{36} + 2688f_1^4 f_3^4 f_5^{12} f_{15}^{12} + 5040f_1^2 f_2 f_4^3 f_8^{30}\right)$

Размотримо скуп векторских инвертибилних Булових функција (у даљем тексту функција), односно скуп S_N пермутација скупа B_n, где је $N = 2^n$. Функција $F \in S_N$ пресликава n-торку $X = (x_1, ..., x_n) \in B_n$ у $Y = (y_1, ..., y_n) = F(X)$. Ако дозволимо и комплементирања променљивих, онда је индукована друга група, $C_2^n \times S_n$, реда $n!2^n$. Елемент групе $(i, \sigma) \in C_2^n \times S_n$ пресликава $X = (x_1, ..., x_n) \in B_n$ у $G_n = (x_{\sigma(1)}^{i_1}, \ldots, x_{\sigma(n)}^{i_n}) \in B_n$.

Нека $g(n)$ означава број апериодичних различитих огрлица од n-перли обојених у 2 боје где се бројање врши „без превртања“, али тако да две боје могу бити замењене (видети [30], низ A000048). Тада је $g(n) = 0$ за свако непарно n, $g(2) = 1$, и

$$g(2k) = \frac{1}{2k}\left(2^k - \sum_{d|2k, d\nmid k, d<2k} d \cdot g(d)\right), \quad k > 1.$$

Ако је $\sigma \in S_n$ циклична пермутација (пермутација која има један циклус дужине n), циклус дужине k из (i, σ), уколико је $\mathrm{wt}(i)$ парно, у σ' индукује пермутацију са мономом циклусног индекса

$$\prod_{d|k} f_d^{e(d)}.$$

У супротном, ако је $\mathrm{wt}(i)$ непарно, циклус дужине k индукује

$$\prod_{d|2k, d\nmid k} f_d^{g(d)},$$

па циклус дужине k из σ (узимајући у обзир сва могућа комплементирања i) индукује 2^k пермутација којима одговара сума монома

$$b_k = 2^{k-1}\left(\prod_{d|k} f_d^{e(d)} + \prod_{d|2k,d\nmid k} f_d^{g(d)}\right).$$

Неколико ненула чланова низа $g(n)$ приказани су у табели 2.9.

Табела 2.9: Низ g.

n	1	2	3	4	5	6	7	8	9	10
$g(2n)$	1	1	1	2	3	5	9	16	28	51

Циклусни индекс $Z_{G_n}(f)$ дат је са

$$\sum_{p\in P_n} \frac{\bigtimes\limits_{\substack{1\leqslant j\leqslant n\\ p_j>0}} \left(\prod\limits_{d|i} f_d^{e(d)} + \prod\limits_{d|2i,d\nmid i} f_d^{g(d)}\right)^{\times p_i}}{\prod_{i=1}^{n}(2i)^{p_i}p_i!}. \tag{2.28}$$

Пример 2.3.8. *Размотримо циклусни индекс групе G_3.*

$$\begin{aligned}
t_1^3 &\longrightarrow b_1\times b_1\times b_1 = (f_1^2+f_2)\times(f_1^2+f_2)\times(f_1^2+f_2)\\
&= \Big((f_1^2\times f_1^2)+(f_1^2\times f_2)+(f_2\times f_1^2)+(f_2\times f_2)\Big)\times(f_1^2+f_2)\\
&= (f_1^4+f_2^2+f_2^2+f_2^2)\times(f_1^2+f_2) = (f_1^4+3f_2^2)\times(f_1^2+f_2)\\
&= (f_1^4\times f_1^2)+(f_1^4\times f_2)+(3f_2^2\times f_1^2)+(3f_2^2\times f_2)\\
&= f_1^8+f_2^4+3f_2^4+3f_2^4 = f_1^8+7f_2^4\\
t_1t_2 &\longrightarrow b_1\times b_2 = (f_1^2+f_2)\times 2(f_1^2f_2+f_4)\\
&= 2\cdot\Big((f_1^2\times f_1^2f_2)+(f_1^2\times f_4)+f_2\times f_1^2f_2)+(f_2\times f_4)\Big)\\
&= 2\cdot\Big((f_1^2\times f_1^2)(f_1^2\times f_2)+f_4^2+(f_2\times f_1^2)(f_2\times f_2)+f_4^2\Big)\\
&= 2\cdot(f_1^4f_2^2+f_4^2+f_2^2f_2^2+f_4^2) = 2\cdot(f_1^4f_2^2+2f_4^2+f_2^4)\\
&= 2f_1^4f_2^2+4f_4^2+2f_2^4\\
t_3 &\longrightarrow b_3 = 2^2\cdot(f_1^2f_3^2+f_2f_6) = 4f_1^2f_3^2+4f_2f_6
\end{aligned}$$

Полином циклусног индекса $Z(G_3)$ дат је изразом:

$$Z(G_3) = \frac{f_1^8+7f_2^4+3(2f_1^4f_2^2+4f_4^2+2f_2^4)+2(4f_1^2f_3^2+4f_2f_6)}{3!2^3}$$

Приметимо да $\left\{(i,\sigma)|\,\mathrm{type}(\sigma)=(1,1,1)\right\}$ *и* $\left\{(j,\sigma)|\,\mathrm{type}(\sigma)=(1,2)\right\}$ *за неко* $i\in C_2^n$ *и* $j\in C_2^n$ *производе исти тип монома* (f_2^4)*. Након сабирања чланова истог типа добија се:*

$$Z(G_3)=\frac{f_1^8+13f_2^4+6f_1^4f_2^2+12f_4^2+8f_1^2f_3^2+8f_2f_6}{48}$$

На основу (2.15) *важи:*

$$U_3(G_3) \;=\; \frac{2^8+13\cdot 2^4+6\cdot 2^4\cdot 2^2+12\cdot 2^2+8\cdot 2^2\cdot 2^2+8\cdot 2^1\cdot 2^1}{48}=22$$

Разлика између S_n' *и* G_n *јасно се види у расподели бројева њихових фиксних тачака приликом дејства парова тачака на скуп инвертибилних Булових функција. Према* (3.4)*, расподела фиксних тачака за* $n=3$ *за све пермутације у композицији са идентичком трансформацијом комплементирања (тј. расподела за* S_3'*) приказана је у табели 2.10:*

Табела 2.10: Расподела фиксних тачака под дејством групе $S_3'\times S_3'$

	2 1 0 (1)(0 2)	1 2 0 (0 1 2)	2 0 1 (0 2 1)	0 2 1 (0)(1 2)	0 1 2 (0)(1)(2)	1 0 2 (0 1)(2)
(1)(0 2)	192	0	0	192	0	192
(0 1 2)	0	36	36	0	0	0
(0 2 1)	0	36	36	0	0	0
(0)(1 2)	192	0	0	192	0	192
(0)(1)(2)	0	0	0	0	40320	0
(0 1)(2)	192	0	0	192	0	192

Примећује се да се фиксне тачке постоје једино у случају када је тип пермутације улазних променљивих једнак типу пермутације излазних променљивих. Расподела фиксних тачака за $n=3$ *свих пермутација у композицији са свим комплементирањима (тј. расподела за* G_3*) дата је циклусним индексом:*

$$Z(G_3)=\frac{f_1^8+7f_2^4+3(2f_1^4f_2^2+4f_4^2+2f_2^4)+2(4f_1^2f_3^2+4f_2f_6)}{48}$$

и приказана је у табели 2.11. Све улазне трансформације упарују се са свим

Табела 2.11: Расподела фиксних тачака под дејством групе $G_3 \times G_3$

	2 1 0 (1)(0 2)	1 2 0 (0 1 2)	2 0 1 (0 2 1)	0 2 1 (0)(1 2)	0 1 2 (0)(1)(2)	1 0 2 (0 1)(2)
(1)(0 2)	2816	0	0	2816	5376	2816
(0 1 2)	0	768	768	0	0	0
(0 2 1)	0	768	768	0	0	0
(0)(1 2)	2816	0	0	2816	5376	2816
(0)(1)(2)	5376	0	0	5376	59136	5376
(0 1)(2)	2816	0	0	2816	5376	2816

излазним трансформацијама и производе следеће бројеве фиксних тачака:

$$\begin{aligned}
t_1^3 \circ t_1^3 &\longrightarrow 1^2 \cdot 8! \cdot 1^8 + 7^2 \cdot 4! \cdot 2^4 = 40320 + 18816 = 59136 \\
t_1t_2 \circ t_1t_2 &\longrightarrow 2^2 \cdot 4! \cdot 1^4 \cdot 2! \cdot 2^2 + 4^2 \cdot 2! \cdot 2^4 + 2^2 \cdot 4! \cdot 2^4 = 768 + 512 + 1536 = 2816 \\
t_3 \circ t_3 &\longrightarrow 4^2 \cdot 2! \cdot 1^2 \cdot 2! \cdot 3^2 + 4^2 \cdot 1! \cdot 2 \cdot 1! \cdot 6 = 576 + 192 = 768 \\
t_1^3 \circ t_1t_2 &\longrightarrow 7 \cdot 2 \cdot 4! \cdot 2^4 = 5376
\end{aligned}$$

па је на основу (2.24)*:*

$$\begin{aligned}
V_3(G_3) &= \frac{1^2 \cdot 59136 + 3^2 \cdot 2816 + 2^2 \cdot 768 + 2 \cdot 3 \cdot 5376}{(3! \cdot 2^3)^2} = \frac{59316 + 25344 + 3072 + 32256}{48^2} \\
&= \frac{119808}{2304} = 52.
\end{aligned}$$

2.3.3 Линеарна група

У овој тачки изводи се циклусни индекс за линеарну групу. Теореме 2.3.3 и 2.3.4 наводе се без доказа.

Теорема 2.3.3. *[18] Нека су елементарни делитељи матрице* $A \in M_n(\mathrm{GF}(q))$

$$\underbrace{f^1, \ldots, f^1}_{\mu_1}, \ldots, \underbrace{f^s, \ldots, f^s}_{\mu_s}$$

где је $f \in \mathrm{GF}(q)[x]$ *моничкн несводљиви полином степена* d*. Тада је*

$$|C_{\mathrm{GL}(n,q)}(A)| = q^{d\sum_{1 \leqslant i,j \leqslant s} \min(i,j)\mu_i\mu_j} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (1 - q^{-du}). \tag{2.29}$$

Теорема 2.3.4. *[18] Нека су елементарни делитељи матрице* $A \in M_n(\mathrm{GF}(q))$

$$\underbrace{f_1^1,\ldots,f_1^1}_{\mu_1^{(1)}},\ldots,\underbrace{f_1^{s_1},\ldots,f_1^{s_1}}_{\mu_{s_1}^{(1)}}$$
$$\ldots$$
$$\underbrace{f_t^1,\ldots,f_t^1}_{\mu_1^{(t)}},\ldots,\underbrace{f_t^{s_t},\ldots,f_t^{s_t}}_{\mu_{s_t}^{(t)}}$$

ūge su $f_1,\ldots,f_t \in \mathrm{GF}(q)[x]$ *mонички несводљиви ūолиноми сшūеūена* $deg(f_k) = d_k$. *Taga je*

$$|C_{\mathrm{GL}(n,q)}(A)| = q^{\sum_{k=1}^{t} d_k \sum_{1\leqslant i,j\leqslant s_k} \min(i,j)\mu_i^{(k)}\mu_j^{(k)}} \prod_{k=1}^{t}\prod_{i=1}^{s_k}\prod_{u=1}^{\mu_i^{(k)}}(1-q^{-d_k u}). \tag{2.30}$$

Нека $P_n(x)$ означава n-ти несводљиви полином над GF(2) ако је искључен полином x (као једини несводљиви полином са константним чланом 0). Нека d_i означава степен полинома $P_i(x)$, и нека e_i означава ред полинома $P_i(x)$, тј. $e_i = \min_{k>0} P_i(x) \mid x^k - 1$ (дељивост је дефинисана у $\mathrm{GF}(2)[x]$). Неколико првих чланова низова $P_i(x)$, d_i, e_i приказани су у табели 2.12; полиноми су лексикографски поређани као тројке (d_i, e_i, P_i).

Табела 2.12: Листа првих 8 несводљивих полинома $P_i(x)$, заједно са њиховим степенима d_i и редовима e_i.

i	$P(i)$	d_i	e_i
1	$1+x$	1	1
2	$1+x+x^2$	2	3
3	$1+x+x^3$	3	7
4	$1+x^2+x^3$	3	7
5	$1+x+x^2+x^3+x^4$	4	5
6	$1+x+x^4$	4	15
7	$1+x^3+x^4$	4	15
8	$1+x+x^2+x^3+x^5$	5	31

Нека је матрица $A \in \mathrm{GL}(2,n)$ дата у канонској форми изразима (2.11) и (2.12) (тј. као блок дијагонална матрица хипер-придружених матрица несводљивих полинома над пољем GF(2)). Нека је

$$\chi_A(x) = \prod_{i=1}^{s} P_i(x)^{a_i}$$

где је $a_i = \sum_j j\alpha_j^{(i)} = \sum_j j\alpha_{ij}$ и $\sum_{i=1}^{s} a_i d_i = n$ (видети изразе (2.11) и (2.12)). Сваки несводљиви полином може се појавити као делилац карактеристичног

полинома матрице $A \in \mathrm{GL}(2, n)$, па важи

$$\chi_A(x) = \prod_{i=1}^{t_n} P_i(x)^{a_i}.$$

Дејство матрице A може се представити као директни производ (видети израз (2.13))

$$\bigtimes_{i=1}^{t_n} \bigtimes_{j=1}^{a_i} H(P_i^j)^{\times \alpha_{ij}}. \tag{2.31}$$

Дакле, да би смо знали циклусни тип матрице A, довољно је знати типове индукованих хипер-придружених матрица. Циклусни тип хипер-придружене матрице несводљивог полинома може се извести из његовог реда.

Теорема 2.3.5. *Нека је $P(x)$ несводљиви полином степена d. Нека елементарном делитељу $P(x)^k$ реда e_k одговара хипер-придружена матрица $H(P(x)^k)$ димензије kd. Нека је V векторски простор над пољем F_2^{kd}. Циклусна структура коју индукује $H(P(x)^k)$ је*

$$f_1 \prod_{i=1}^{k} f_{e_i}^{(2^{id}-2^{(i-1)d})/e_i}.$$

Доказ. $H(P(x)^k)$ индукује циклусе чији је збир дужина 2^{kd}. На основу Теореме 2.1.12, дужина неког индукованог циклуса је e_k. Дејство матрице $H(P(x)^k)$ на векторе са првих d координата једнаким нули аналогно је дејству матрице $H(P(x)^{k-1})$ над векторима над пољем $F_2^{(k-1)d}$ (краћим за првих d координата) чија дужина циклуса на основу Теореме 2.1.16 дели e_{k-1}. Приметимо да важи $e_j = e_1 2^{\lceil log_2 j \rceil}$. Дакле, циклусна структура индукована дејством $H(P(x)^k)$ на векторе код којих првих d координата нису истовремено нула је $f_{e_k}^{(2^{kd}-2^{(k-1)d})/e_k}$. Вектор састављен од свих нула увек индукује циклус f_1. □

Нека је $e(m)$ број несводљивих полинома степена m над GF(2) (видети табелу 2.7). Нека је t_n број несводљивих полинома степена највише n над GF(2), када је искључен полином првог степена x, тј.

$$t_n = \sum_{m=1}^{n} e(m) - 1.$$

Погодности ради, нека је $t_0 = 0$. Нека је A_n скуп решења $a = (a_1, \ldots, a_{t_n})$ у скупу ненегативних целих бројева једначине $\sum_{i=1}^{t_n} a_i d_i = n$, тј.

$$A_n = \left\{ (a_1, \ldots, a_{t_n}) \mid \sum_{i=1}^{t_n} a_i d_i = n. \right\} \tag{2.32}$$

За $1 \leqslant i \leqslant t_n$ и $1 \leqslant j \leqslant n$ нека је

$$q_{ij} = e_i 2^{\lceil log_2 j \rceil}, \qquad h_{ij} = \frac{2^{d_i(j-1)}(2^{d_i}-1)}{q_{ij}}.$$

Теорема 2.3.6. *За дати ненегативни цео низ $\beta = (\beta_1, \beta_2, \ldots)$ са коначним бројем позитивних елемената, нека је $b = \sum_{i=1}^{\infty} i\beta_i$ (према томе $\beta_i = 0$ за $i > b$) и нека $S(\beta)$ означава суму*

$$S(\beta) = \sum_{j=1}^{b} \left(\beta_j^2(j-1) + \frac{(\beta_j - 1)\beta_j}{2} \right) + \sum_{j=1}^{b-1} \sum_{k=j+1}^{b} 2j\beta_j\beta_k. \tag{2.33}$$

Тада је Z_{GL_n} једнак

$$\frac{1}{M_n} \sum_{a \in A_n} \sum_{\alpha \in P_{a_1} \times \cdots \times P_{a_{t_n}}} M_n \frac{\bigtimes\limits_{\substack{1 \leqslant i \leqslant t_n \\ a_i > 0}} \bigtimes\limits_{\substack{1 \leqslant j \leqslant a_i \\ \alpha_{ij} > 0}} \left(f_1 \prod\limits_{k=1}^{j} f_{q_{ik}}^{h_{ik}} \right)^{\times \alpha_{ij}}}{\prod\limits_{i=1}^{t_n} 2^{d_i S(\alpha_i)} \prod\limits_{j=1}^{a_i} \prod\limits_{k=1}^{\alpha_{ij}} (2^{kd_i} - 1)}, \tag{2.34}$$

ѓде је $M_n = \prod_{p=0}^{n-1}(2^n - 2^p)$ величина ѓрупе, индекс α је t_n-шорка $\alpha = (\alpha_1, \ldots, \alpha_{t_n})$ и

$$\alpha_i = \begin{cases} (\alpha_{i,1}, \ldots, \alpha_{i,a_i}), & a_i > 0 \\ (0), & a_i = 0 \end{cases}.$$

Доказ. Преформулишимо израз (2.29) за $q = 2$:

$$\begin{aligned}
|C_{\mathrm{GL}(n,2)}(A)| &= 2^{d\sum_{1 \leqslant i,k \leqslant s} \min(i,k)\mu_i\mu_k} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (1 - 2^{-du}) \\
&= 2^{d\sum_{i=1}^{s} \left(\sum_{k=1}^{i} k\mu_k + \sum_{k=i+1}^{s} i\mu_k \right)\mu_i} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (1 - 2^{-du}) \\
&= 2^{d\left(\sum_{i=1}^{s} \sum_{k=1}^{i} k\mu_k\mu_i + \sum_{i=1}^{s} \sum_{k=i+1}^{s} i\mu_k\mu_i \right)} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (1 - 2^{-du}) \\
&= 2^{d\left(\sum_{i=1}^{s} i\mu_i^2 + 2\sum_{i=1}^{s} \sum_{k=i+1}^{s} i\mu_k\mu_i \right)} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} 2^{-du}(2^{du} - 1) \\
&= 2^{d\left(\sum_{i=1}^{s} i\mu_i^2 + \sum_{i=1}^{s} \sum_{k=i+1}^{s} 2i\mu_k\mu_i - \sum_{i=1}^{s} (\frac{\mu_i(\mu_i+1)}{2}) \right)} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (2^{du} - 1) \\
&= 2^{d\left(\sum_{i=1}^{s} i\mu_i^2 + \sum_{i=1}^{s-1} \sum_{k=i+1}^{s} 2i\mu_k\mu_i - \sum_{i=1}^{s} (\mu_i^2 - \frac{\mu_i(\mu_i-1)}{2}) \right)} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (2^{du} - 1) \\
&= 2^{d\left(\sum_{i=1}^{s} ((i-1)\mu_i^2 + \frac{\mu_i(\mu_i-1)}{2}) + \sum_{i=1}^{s-1} \sum_{k=i+1}^{s} 2i\mu_k\mu_i \right)} \prod_{i=1}^{s} \prod_{u=1}^{\mu_i} (2^{du} - 1).
\end{aligned}$$

Заменом ознака $k = u,\ j = i,\ d = d_i,\ s = a_i,\ \mu_i = \alpha_{ij}$, из (2.30) добија се израз за централизатор у изразу (2.34). Из (2.31) следи тврђење теореме. □

2.3.4 Афина група

У овој тачки изводи се циклусни индекс за афину групу.

Лема 2.3.1. *Нека је R комутативни прстен са јединицом. Нека је $A : R^n \to R^n$ линеарно пресликавање и $b \in R^n$. Ако је пресликавање $v \to Av - v$ бијекција, тада пресликавање $v \to B(v) = Av + b$ има исту циклусну структуру као и пресликавање $v \to Av$.*

Доказ. Пошто је $A - I$ бијекција, пресликавање $c = (A - I)^{-1}(b)$ је добро дефинисано. Пресликавање $T : R^n \to R^n,\ T(v) = v - c$ је пермутација R^n и важи

$$(T^{-1} \circ B \circ T)(v) = (T^{-1} \circ B)(v - c) = T^{-1}(A(v - c) + b).$$

Како је $T^{-1}(v) = v + c$ и $(A - I)c = b$, следи:

$$(T^{-1} \circ B \circ T)(v) = A(v-c)+b+c = A(v)-A(c)+b+c = Av-(A-I)c+b = Av.$$

Дакле, пресликавања $v \to B(v)$ и $v \to Av$ су конјугати, па имају исту циклусну структуру. □

Дејство $(A, b) \in \mathrm{AGL}(2, n)$ на F_2^n може се посматрати као директни производ дејства (A', b) на потпросторе F_2^n где је A' хипер-придружена матрица несводљивих полинома $P_i(x) \in F_2[x]$. За $P_i(x) \neq x - 1$, пресликавање $v \to H(P_i^j)v - v$ је регуларно линеарно пресликавање, па на основу леме 2.3.1, циклусни тип пресликавања $(H(P_i^j), b)$ не зависи од b и једнак је циклусном типу пресликавања $(H(P_i^j), 0)$.

Нека је $P_i(x) = x - 1$. Тада је

$$A := H(P_i^j) = \begin{bmatrix} 1 & 0 & & 0 & 0 \\ 1 & 1 & \ddots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & & 1 & 1 \end{bmatrix}.$$

Нека је

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_j \end{bmatrix} \in F_2^j,\ b' = \begin{bmatrix} b_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in F_2^j,\ c = \begin{bmatrix} -b_2 \\ -b_3 \\ \vdots \\ -b_j \\ 0 \end{bmatrix} \text{ и } T(v) := v + c.$$

Треба приметити да важи $(A - I)(c) + b = b'$. Нека је $B(v) = Av + b$. T је пермутација у пољу F_2^j и пошто је

$$\begin{aligned} T^{-1}BT(v) &= T^{-1}B(v + c) = T^{-1}(A(v + c) + b) = A(v + c) + b - c \\ &= Av + Ac + b - c = Av + (A - I)c + b = Av + b' \end{aligned}$$

следи да су пресликавања $v \to Av + b$ и $v \to Av + b$' конјугати у односу на пресликавање T. Дакле, за свих 2^{j-1} вектора из скупа $\{b \in F_2^j : \ b_1 = 0\}$, афина пресликавања облика (A, b) и $(A, 0)$ имају исту циклусну структуру.

На крају, када је $b_1 \neq 0$, потребно је израчунати циклусну структуру пресликавања $v \to B(v) = Av + b'$. Нека је $A' := H(P_i^{j+1}) \in \mathrm{GL}(2, j + 1)$. Тада важи

$$A' \begin{bmatrix} b_1 \\ v \end{bmatrix} = \begin{bmatrix} b_1 \\ B(v) \end{bmatrix}.$$

Пошто је $b_1 \neq 0$, сви елементи $\begin{bmatrix} b_1 \\ v \end{bmatrix} \in F_2^{j+1}$ имају исти минимални полином P_i^{j+1} (у односу на A), па образују $2^j/q_{i,j+1}$ циклуса матрице A' дужине $q_{i,j+1}$.

За $1 \leqslant i \leqslant t_n$ и $1 \leqslant j \leqslant n$ нека је

$$u_{ij} = \begin{cases} 2^{j-1} f_1 \prod_{k=1}^{j} f_{q_{1k}}^{h_{1k}} + 2^{j-1} f_{q_{1(j+1)}}^{\frac{2^j}{q_{1(j+1)}}},\ i = 1 \\ 2^{jd_i} f_1 \prod_{k=1}^{j} f_{q_{ik}}^{h_{ik}},\ i > 1 \end{cases}$$

Израз за циклусни индекс групе AGL_n сличан је изразу (2.34); израз $f_1 \prod_{k=1}^{j} f_{q_{ik}}^{h_{ik}}$

замењен је са u_{ij}, уз додатно множење са 2^{-n}:

$$\frac{1}{2^n M_n} \sum_{a \in A_n} \sum_{\alpha \in P_{a_1} \times \cdots \times P_{a_{t_n}}} \frac{M_n \bigtimes\limits_{\substack{1 \leqslant i \leqslant t_n \\ a_i > 0}} \bigtimes\limits_{j=1}^{a_i} u_{ij}^{\times \alpha_{ij}}}{\prod\limits_{\substack{1 \leqslant i \leqslant t_n \\ a_i > 0}} 2^{d_i S(\alpha_i)} \prod\limits_{j=1}^{a_i} \prod\limits_{k=1}^{\alpha_{ij}} (2^{k d_i} - 1)}. \tag{2.35}$$

Глава 3

Пребројавање класа еквиваленције Булових и инвертибилних Булових функција

Из израза

$$U_n(G) = Z_G(2, 2, \ldots, 2) = \frac{1}{|G|} \sum_{p \in P_N} g(p) 2^{\sum_{i=1}^{N} p_i} \tag{3.1}$$

и

$$\begin{aligned} V_n(G) &= Z_G\big(\frac{\partial}{\partial t_1}, \frac{\partial}{\partial t_2}, \ldots, \frac{\partial}{\partial t_N}\big) \cdot \\ &\quad Z_G(1 + t_1, 1 + 2t_2, \ldots, 1 + Nt_N)\big|_{t_1 = \cdots = t_N = 0} \\ &= \frac{1}{|G|^2} \sum_{p \in P_N} g(p)^2 \prod_{i=1}^{N} i^{p_i} p_i! \end{aligned} \tag{3.2}$$

следи да се из познавања циклусног индекса могу израчунати бројеви класа еквиваленције Булових U_n и инвертибилних Булових функција V_n. Међутим, општи изрази за израчунавање не омогућавају добијање циклусног индекса за иоле веће вредности n. У наставку се приказују неки приступи ефикасног рачунања израза за циклусне индексе за све четири групе трансформација. Прво се разматрају заједничка побољшања за све четири групе, а потом и специфична убрзања везана за појединачне групе.

Следећа табела сумира добијене у односу на претходно познате резултате.

Табела 3.1: Старе и нове вредности за U_n и V_n.

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

У овом поглављу приказује се ефикасно рачунање циклусног индекса и бројева U_n и V_n за све четири групе трансформација.

3.1 Коришћење полинома од једне променљиве уместо монома од променљивих f_1, f_2, ...

Мономи који се појављују у току рачунања циклусног индекса, генерално су доста ретки - користе се само неки од производа променљивих f_1, f_2, ..., па је рачунање Декартовог производа два монома (2.6) прилично неефиксано. Овај проблем може се решити заменом израза f_i^j мономом jx^i, будући да Wolfram Mathematica не штеди меморијски простор при раду са мономима, али ефикасно ради са ретким полиномима. Декартов производ (имплементиран применом оператора крст (2.7)), у овој нотацији постаје

$$jx^p \times kx^q = jk(p,q)x^{\langle p,q\rangle},$$

и крст два монома (2.6) постаје

$$\Big(\sum_{p=1}^{a} j_p x^p\Big) \times \Big(\sum_{q=1}^{b} k_q x^q\Big) = \sum_{p=1}^{a}\sum_{q=1}^{b} \big(j_p x^p \times k_q x^q\big)$$
$$= \sum_{p=1}^{a}\sum_{q=1}^{b} j_p k_q (p,q) x^{\langle p,q\rangle}.$$

Пошто се у репрезентацији циклусних индекса мономима користи операција сабирања, линеарна комбинација монома

$$\sum_{k=1}^{p} u_k \prod_{i=1}^{N} f_i^{j_{i,k}}$$

представљена је листом парова

$$\left(u_k, \sum_{i=1}^{N} j_{i,k} x^i\right), \quad 1 \leqslant k \leqslant p.$$

Ако крст две листе садржи два пара (u_1, M_1) и (u_2, M_2) где је $M_1 = M_2$, тада та два пара могу бити замењена паром $(u_1 + u_2, M_1)$. Крст две такве листе

$$\begin{aligned}&\big((u'_1, M'_1), (u'_2, M'_2), \ldots, (u'_p, M'_p)\big) \bigtimes \\ &\quad \big((u''_1, M''_1), (u''_2, M''_2), \ldots, (u''_q, M''_q)\big)\end{aligned}$$

је листа свих парова

$$(u'_i u''_j, M'_i \times M''_j), \quad 1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q.$$

Парови са једнаком другом компонентом могу се пронаћи сортирањем резултирајуће листе по другој компоненти својих парова.

Пример 3.1.1. *Крст два полинома*

$$\begin{aligned}& (f_1^2 + f_2) \times (2f_1^2 f_2 + 2f_4) = \\ = \;& (f_1^2 \times 2f_1^2 f_2) + (f_1^2 \times 2f_4) + (f_2 \times 2f_1^2 f_2) + (f_2 \times 2f_4) \\ = \;& 2f_1^4 f_2^2 + 2f_4^2 + 2f_2^2 f_2^2 + 2f_4^2 \\ = \;& 2f_1^4 f_2^2 + 4f_4^2 + 2f_2^4\end{aligned}$$

замењен је крстом две листе парова

$$\begin{aligned}& \big((1, 2x), (1, x^2)\big) \times \big((2, 2x + x^2), (2, x^4)\big) = \\ = \;& \big((2, 2x \times (2x + x^2)), (2, 2x \times x^4),\ (2, x^2 \times (2x + x^2)), (2, x^2 \times x^4)\big) \\ = \;& \big((2, 4x + 2x^2), (2, 2x^4), (2, 2x^2 + 2x^2), (2, 2x^4)\big) = \\ = \;& \big((2, 4x + 2x^2), (4, 2x^4), (2, 4x^2)\big).\end{aligned}$$

Израчунавање циклусног индекса након ове замене постаје знатно ефикасније. Једноставности ради, у примерима који следе биће задржана нотација са променљивама f_1, f_2, ...

3.2 Унапред израчунате табеле

Показаћемо у наставку да се сви изрази за циклусне индексе (2.27), (2.28), (2.34), (2.35) могу представити у облику:

$$Z_G(f) = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} H_{i,p_i}, \tag{3.3}$$

где је $H = [H_{ij}]$ одговарајућа унапред израчуната табела димензија $n \times n$. Овакво представљање циклусног индекса значајно убрзава његово рачунање, пошто се избегава понављање израчунавања елемената табеле H. Следеће убрзање постиже се смањењем броја скупих крст операција. Ова идеја илустрована је следећим примером.

Пример 3.2.1. *За $n = 5$, P_n се састоји од 7 елемената*

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Циклусни индекс

$$Z_G(f) = H_{5,1} + H_{4,1} \times H_{1,1} + H_{3,1} \times H_{2,1} + H_{3,1} \times H_{1,2} + H_{2,2} \times H_{1,1} + H_{1,3} \times H_{2,1} + H_{1,5}.$$

садржи два израза $H_{3,1}$, па $Z_G(f)$ може бити израчунат са једном мање операцијом крст:

$$H_{5,1} + H_{4,1} \times H_{1,1} + H_{3,1} \times (H_{2,1} + H_{1,2}) + H_{2,2} \times H_{1,1} + H_{1,3} \times H_{2,1} + H_{1,5}.$$

Није тешко генерализовати овај приступ. Након опадајућег лексикографског сортирања елемената из P_n, обавља се њихово груписање по позицији k и по величини p_k ненула елемената са највећим индексом. Размотримо произвољно овакво груписање. Како сви крст изрази унутар групе почињу

са H_{k,p_k}, заједнички фактор H_{k,p_k} може бити извучен испред заграде. Сума унутар заграда одговара изразу P_{n-kp_k} и може бити рекурзивно израчуната коришћењем истог приступа. Исти метод може бити коришћен при рачунању одговарајућих бројева U_n; при томе, могуће је израчунати U_n без рачунања комплетног циклусног индекса. Алгоритам је представљен следећим кодом.

```
part(n, k, term)
[Рачунање дела Z_G придруженог елементу p ∈ P_n
за који је p_{k+1} = ··· = p_n = 0]
[term је крст израза изван заграда
насталих из претходних рекурзивних позива]
[sum је глобална променљива за формирање Z_G]
[U_n је глобална променљива за формирање U_n]
if n = 0 then [Тренутни term је завршен]
    sum ← sum + term [Крај рекурзивног позива]
    U_n ← U_n + term(2, ..., 2)
  return
else
  if k > 1 then
    for i = ⌊n/k⌋ downto 0 step −1 do
      if i > 0 then [Ажурирање тренутног term]
        part(n − ik, min{n − ik, k − 1}, term × H[k, i])
      else
        part(n, k − 1, term)
  else
    part(0, 0, term × H[1, n])
  return
```

Изрази за Z_G и број U_n добијају се рекурзивним позивом $part(n, n, 1)$; за добијање израза за Z_G без разломака, тј. у облику $|G|Z_G$, иницијални позив је $part(n, n, |G|)$. Ако $p(n)$ означава број партиција броја n, тада је $p(n) = O(\exp(\pi\sqrt{2n/3}))$, видети на пример [13]. Просечан број делова партиција броја n је $O(\sqrt{n}\log n)$, видети [14]. На тај начин, без описаног алгоритамског убрзања, број операција крст у току рачунања Z_G облика (3.3) грубо је $O(p(n)\sqrt{n}\log n)$. Нека $T(n, k)$ у алгоритму $part(n, k, term)$ представља број операција крст у току рачунања Z_G облика (3.3), који одговара партицијама

од највише k делова. Тада је

$$T(n,k) = \begin{cases} -1, & n = k = 0 \\ 0, & k = 1 \\ \lfloor n/k \rfloor + \sum_{i=0}^{\lfloor n/k \rfloor} T(n-ik, \min(n-ik, k-1)), & n > 0,\ k > 1. \end{cases}$$

Нека $p(n,k)$ означава број партиција од највише k делова. Из познате рекурентне једначине $p(n,k) = p(n-k,k) + p(n,k-1)$ произилази слична рекурентна једначина

$$p(n,k) = \begin{cases} 1, & n = k = 0 \text{ или } k = 1 \\ \sum_{i=0}^{\lfloor n/k \rfloor} p(n-ik, \min(n-ik, k-1)), & n > 0,\ k > 1. \end{cases}$$

Лема 3.2.1. *За свако $n \geqslant 1$, $1 \leqslant k \leqslant n$, важи неједнакост*

$$T(n,k) = p(n,k) - 1$$

.

Доказ. Доказ се изводи индукцијом по k. Једнакост је тачна за $n = k = 0$ и $k = 1$. Претпоставимо да је тачна када је други аргумент мањи од k. Тада је

$$\begin{aligned} p(n,k) - T(n,k) &= \sum_{i=0}^{\lfloor n/k \rfloor - 1} (p(n-ik, k-1) - T(n-ik, k-1)) - \lfloor n/k \rfloor \\ &+ p(n \bmod k, n \bmod k) - T(n \bmod k, n \bmod k) \\ &= \sum_{i=0}^{\lfloor n/k \rfloor - 1} 1 - \lfloor n/k \rfloor + 1 = 1. \end{aligned}$$

□

Из доказаног следи специјално да је $T(n,n) <= p(n,n) = p(n)$, тј. $T(n,n) = O(p(n))$. Из ове неједнакости следи да је убрзање алгоритма у односу на директно рачунање (3.3) реда $O(\sqrt{n} \log n)$.

За велике вредности n, могуће је да величина израза за Z_G превазилази меморијско ограничење. Тада је ипак могуће добити вредности U_n без рачунања Z_G, изостављањем ажурирања промењиве sum. Вредности V_n не могу бити израчунате на овај начин без рачунања циклусног индекса, пошто израз (2.24) није линеаран у односу на коефицијенте циклусног индекса.

3.3 Група пермутација променљивих S'_n

Теорема 3.3.1. *Нека је*

$$F_{i,j} = \prod_{d|i} \left(f_d^{e(d)} \right)^{\times j}, \quad K_{i,j} = i^j j!,$$
$$H_{i,j} = \frac{F_{i,j}}{K_{i,j}}, \ 1 \leqslant i \leqslant n, \ 1 \leqslant j \leqslant \left\lfloor \frac{n}{i} \right\rfloor.$$

Тада циклусни индекс (2.27) *постаје*

$$Z_{S'_n}(f) = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} H_{i,p_i},$$

Доказ.

$$Z_{S'_n}(f) = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} \frac{F_{i,p_i}}{K_{i,p_i}} = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} H_{i,p_i}.$$

□

Пример 3.3.1. *За* $n = 3$, *добија се*

$$F_{3,1} = f_1^{e(1)} f_3^{e(3)} = f_1^2 f_3^2,$$
$$F_{1,3} = (f_1^{e(1)})^{\times 3} = f_1^2 \times f_1^2 \times f_1^2 = f_1^4 \times f_1^2 = f_1^8,$$

и

$$K_{3,1} = 3^1 1! = 3, \quad K_{1,3} = 1^3 3! = 6.$$

Комплетне унапред израчунате табеле су

$$F = \begin{bmatrix} f_1^2 & f_1^4 & f_1^8 \\ f_1^2 f_2 & 0 & 0 \\ f_1^2 f_3^2 & 0 & 0 \end{bmatrix},$$

$$K = \begin{bmatrix} 1 & 2 & 6 \\ 2 & 0 & 0 \\ 3 & 0 & 0 \end{bmatrix},$$

и

$$H = \begin{bmatrix} f_1^2 & \frac{1}{2} f_1^4 & \frac{1}{6} f_1^8 \\ \frac{1}{2} f_1^2 f_2 & 0 & 0 \\ \frac{1}{3} f_1^2 f_3^2 & 0 & 0 \end{bmatrix},$$

где 0 означава елемент табеле који се не користи. Према томе

$$\begin{aligned} Z_{S_3'} &= H_{3,1} + H_{1,1} \times H_{2,1} + H_{1,3} = \\ &= \tfrac{1}{3} f_1^2 f_3^2 + f_1^2 \times \tfrac{1}{2} f_1^2 f_2 + \tfrac{1}{6} f_1^8 = \\ &= \tfrac{1}{3} f_1^2 f_3^2 + \tfrac{1}{2} f_1^4 f_2^2 + \tfrac{1}{6} f_1^8. \end{aligned}$$

3.4 Алтернативни приступ за групу S_n'

Вредности $U_n(S_n')$ и $V_n(S_n')$ могуће је директно израчунати, без рачунања циклусног индекса.

Теорема 3.4.1. *Нека декомпозиција $n = k_1 + k_2 + \cdots + k_m$ одговара партицији p и нека је*

$$S(p) = \sum_{z_1 | k_1} \cdots \sum_{z_m | k_m} \frac{\prod_{j=1}^{m} z_j e(z_j)}{< z_1, z_2, \ldots, z_m >},$$

где је $e(n)$ низ дефинисан изразом (2.26)*. Тада важи*

$$U_n(S_n') = \sum_{p \in P_n} \frac{2^{S(p)}}{\prod_{i=1}^{n} i^{p_i} p_i!}.$$

Доказ. Размотримо део циклусног индекса симетричне групе (2.27)

$$GS(p, f) = \bigtimes_{\substack{1 \leqslant j \leqslant n \\ p_j > 0}} \left(\prod_{d | j} f_d^{e(d)} \right)^{\times p_j}$$

који одговара фиксираној партицији $p \in P_n$. Нека је $(k_1, k_2, \ldots, k_m)$ низ састављен од p_j целих бројева j, $1 \leqslant j \leqslant n$. Тада је

$$\begin{aligned} GS(p, f) &= \bigtimes_{j=1}^{m} \prod_{z_j | k_j} f_{z_j}^{e(z_j)} = \prod_{z_1 | k_1} \cdots \prod_{z_m | k_m} \bigtimes_{j=1}^{m} f_{z_j}^{e(z_j)} \\ &= \prod_{z_1 | k_1} \cdots \prod_{z_m | k_m} f_{<z_1, z_2, \ldots, z_m>}^{\prod_{i=1}^{m} z_i e(z_i) / <z_1, z_2, \ldots, z_m>} \end{aligned}$$

Нека је $S(p) = \log_2 \left(GS(p, f) \mid_{f_1 = \cdots = f_n = 2} \right)$. Тада је $2^{S(p)} / \prod_{i=1}^{n} i^{p_i} p_i!$ део суме U_n (2.15) који одговара партицији $p \in P_n$. Дакле

$$U_n(S_n') = \sum_{p \in P_n} \frac{2^{S(p)}}{\prod_{i=1}^{n} i^{p_i} p_i!}.$$

□

Произвољном пару пермутација променљивих $(\rho, \sigma) \in S_n^2$ одговара пресликавање $T_{\rho,\sigma} : S_N \to S_N$, које произвољну векторску инвертибилну функцију $F \in S_N$ пресликава у векторску инвертибилну функцију $F' = T_{\rho,\sigma}(F) = \rho' \circ F \circ \sigma'$, такву да је $F'(x) = \rho'(F(\sigma'(x)))$ за свако $x \in B_n$. Ако се n-торке из скупа B_n кодирају бројевима из интервала $[0, N-1]$, онда је скуп свих пресликавања $T_{\rho,\sigma}$ подгрупа групе $S_{N!}$.

Да би се на основу Фробенијусове теореме одредио број класа еквиваленције Булових инвертибилних функција, потребно је за сваки пар $(\rho, \sigma) \in S_n^2$, одредити број фиксних тачака. Трансформација $T_{\rho,\sigma}$ је фиксна тачка ако и само ако важи $F' = F$.

Трансформација $T_{\rho,\sigma}$ има барем једну фиксну тачку ако и само ако $\mathrm{type}(\sigma) = \mathrm{type}(\rho)$ [21]. За произвољну партицију $p \in P_n$ и групу пермутација G (било ког од четири разматрана типа), нека је $G_p = \{\sigma \in G \mid \mathrm{type}(\sigma) = p\}$ подскуп пермутација из групе G са циклусном структуром описаном партицијом p (p_i циклуса дужине i, $i \geqslant 1$). Нека је $g(p) = |G_p|$. Специјално, ако је G група S_n, тада је $(S_n)_p = \{\sigma \in S_n \mid \mathrm{type}(\sigma) = p\}$. Нека је $\sigma \in (S_n)_p$ и нека је тип индуковане пермутације $\mathrm{type}(\sigma') = p' = (p'_1, p'_2, \ldots, p'_N)$. За сваку дужину циклуса i постоји $p'_i!$ могућих упаривања између улазних и излазних циклуса (пермутације σ, односно ρ) истог типа. Пошто унутар сваког циклуса постоји i ротација елемената, при којима структура циклуса није нарушена, број фиксних тачака трансформације $T_{\sigma,\sigma}$ зависи само од партиције p и једнак је

$$N_p = \prod_i i^{p'_i} p'_i!. \tag{3.4}$$

Из претходног излагања и последице 2.1.1 следи:

$$g(p) = |(S_n)_p| = \frac{|S_n|}{|C_{S_n}(\sigma)|} = \frac{n!}{\prod_{i=1}^{n} i^{p_i} p_i!}.$$

Теорема 3.4.2. *Свака пермутација $\sigma \in S_n$ јединствено одређује пермутацију $\sigma' \in S'_n$. За произвољно $p \in P_n$ нека је $\mathrm{type}(\sigma) = p$ и $\mathrm{type}(\sigma') = (p'_1, \ldots, p'_n)$. Тада важи*

$$V_n(S'_n) = \sum_{p \in P_n} \frac{\prod_i i^{p'_i} p'_i!}{\left(\prod_i i^{p_i} p_i!\right)^2}. \tag{3.5}$$

Доказ. Пермутација $F \in S_N$ је фиксна тачка трансформације $T_{\rho,\sigma}$ ако $T_{\rho,\sigma}(F(X)) = F(X)$ важи за свако $X \in B_n$. Нека је $I(\rho, \sigma)$ број фиксних тачака трансформације $T_{\rho,\sigma}$. На основу Фробенијусове теореме, број класа еквиваленције једнак

је

$$V_n = \frac{1}{(n!)^2} \sum_{\sigma \in S_n} \sum_{\rho \in S_n} I(\rho, \sigma) = \frac{1}{(n!)^2} \sum_{p \in P_n} \sum_{\rho \in (S_n)_p} \sum_{q \in P_n} \sum_{\sigma \in (S_n)_q} I(\rho, \sigma).$$

Нека је $(S_n)_p = \{\sigma \in S_n \mid \text{type}(\sigma) = p\}$. Број фиксних тачака трансформације $T_{\rho,\sigma}$ која одговара пермутацијама $\rho \in (S_n)_p$ и $\sigma \in (S_n)_q$ једнак је

$$I(\rho, \sigma) = \begin{cases} 0, & p \neq q \\ N_p, & p = q \end{cases}$$

пошто је за добијање фиксне тачке потребно и довољно да тип (односно структура) улазних циклуса одговара типу излазних циклуса. Према томе

$$\begin{aligned} V_n &= \frac{1}{(n!)^2} \sum_{p \in P_n} \sum_{\rho \in (S_n)_p} \sum_{q \in \{p\}} \sum_{\sigma \in (S_n)_p} N_p = \frac{1}{(n!)^2} \sum_{p \in P_n} \sum_{\rho \in (S_n)_p} \sum_{\sigma \in (S_n)_p} N_p \\ &= \frac{1}{(n!)^2} \sum_{p \in P_n} N_p \sum_{\rho \in (S_n)_p} \sum_{\sigma \in (S_n)_p} 1 = \frac{1}{(n!)^2} \sum_{p \in P_n} N_p \cdot |(S_n)_p|^2 \\ &= \sum_{p \in P_n} \frac{\prod_i i^{p_i'} p_i'!}{\left(\prod_i i^{p_i} p_i! \right)^2} \end{aligned}$$

□

Да би се израчунала вредност овог израза, потребно је одредити структуру одговарајућег монома циклусног индекса који одговара индукованој пермутацији σ'.

Теорема 3.4.3. *Нека је $p \in P_n$ произвољна партиција и нека је $\sigma \in (S_n)_p$. Нека је $\sigma = \alpha_1 \alpha_2 \ldots \alpha_m$ разлагање σ на дисјунктне циклусе. Нека је дужина циклуса α_i једнака k_i, $1 \leqslant i \leqslant m$. Моном циклусног индекса $\prod_i f_i^{p_i'}$ који одговара пермутацији σ' дат је изразом*

$$\prod_i f_i^{p_i'} \equiv \bigtimes_{i=1}^{m} \left(\prod_{z_i | k_i} f_{z_i}^{e(z_i)} \right) = \prod_{z_1 | k_1} \prod_{z_2 | k_2} \cdots \prod_{z_m | k_m} f_{<z_1, z_2, \ldots, z_m>}^{\prod_{i=1}^m z_i e(z_i) / <z_1, z_2, \ldots, z_m>}.$$

Доказ. Циклус дужине k_i пермутације σ индукује производ циклуса пермутације σ' у облику монома $\prod_{z_i | k_i} f_{z_i}^{e(z_i)}$. Производ пермутација са мономом $\prod_{i=1}^n t_i^{p_i} = \prod_{i=1}^m t_{k_i}$ у σ индукује пермутацију са мономом циклусног индекса $\times_{i=1}^m \prod_{z_i | k_i} f_{z_i}^{e(z_i)}$ у σ'. Део циклусног индекса који одговара пермутацији σ' добија се на основу израза (2.1.6)

$$\prod_i f_i^{p_i'} = \prod_{z_1 | k_1} \prod_{z_2 | k_2} \cdots \prod_{z_m | k_m} f_{<z_1, z_2, \ldots, z_m>}^{\prod_{i=1}^m z_i e(z_i) / <z_1, z_2, \ldots, z_m>}.$$

□

Описаним алтернативним приступом, вредности $U_n(S'_n)$ и $V_n(S'_n)$ израчунате су за $n \leqslant 30$. Алтернативни поступак израчунавања вредности U_n и V_n захтева мање меморије у односу на приступ који користи циклусни индекс. С друге стране, приступ у коме се израчунава циклусни индекс временски брже израчунава вредност U_n, а спорије вредност V_n. Ово следи из чињенице да се у току креирања циклусног индекса вредност U_n може сукцесивно повећавати, док је пре рачунања вредности V_n потребно креирати комплетан циклусни индекс.

3.5 Група пермутација и комплементирања променљивих G_n

Теорема 3.5.1. *За $1 \leqslant i \leqslant n$ и $1 \leqslant j \leqslant \left\lfloor \frac{n}{i} \right\rfloor$ нека је*

$$F_{i,j} = \left(2^{i-1} \Big(\prod_{d|i} f_d^{e(d)} + \prod_{d|2i, d\nmid i} f_d^{g(d)} \Big) \right)^{\times j},$$

$$K_{i,j} = i^j j!, \quad H_{i,j} = \frac{F_{i,j}}{2^{ij} K_{i,j}}.$$

Тада је

$$Z_{G_n}(f) = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} H_{i,p_i}.$$

Доказ. Једнакост (2.27) постаје

$$Z_{G_n}(f) = \sum_{p \in P_n} \frac{1}{\prod_{i=1}^n (2^{i-1})^{p_i} (2i)^{p_i} p_i!} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} F_{i,p_i}.$$

Из

$$\prod_{i=1}^n (2^{i-1})^{p_i} (2i)^{p_i} p_i! = \prod_{i=1}^n 2^{ip_i} i^{p_i} p_i! = \prod_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} 2^{ip_i} K_{i,p_i},$$

следи

$$Z_{G_n}(f) = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} \frac{F_{i,p_i}}{2^{ip_i} K_{i,p_i}} = \sum_{p \in P_n} \bigtimes_{\substack{1 \leqslant i \leqslant n \\ p_i > 0}} H_{i,p_i}.$$

□

Пример 3.5.1. *За $n = 3$, добија се*

$$\begin{aligned} F_{3,1} &= 2^2 f_1^{e(1)} f_3^{e(3)} + 2^2 f_2^{g(2)} f_6^{g(6)} \\ &= 4f_1^2 f_3^2 + 4f_2 f_6, \end{aligned}$$

$$\begin{aligned} F_{1,3} &= (f_1^{e(1)} + f_2^{g(2)})^{\times 3} \\ &= (f_1^2 + f_2) \times (f_1^2 + f_2) \times (f_1^2 + f_2) \\ &= (f_1^4 + 3f_2^2) \times (f_1^2 + f_2^2) = f_1^8 + 7f_2^4, \end{aligned}$$

и

$$K_{3,1} = 3^1 1! = 3, \quad K_{1,3} = 1^3 3! = 6.$$

Унапред израчунате табеле су

$$F = \begin{bmatrix} f_1^2 + f_2 & f_1^4 + 3f_2^2 & f_1^8 + 7f_2^4 \\ 2f_1^2 f_2 + 2f_4 & 0 & 0 \\ 4f_1^2 f_3^2 + 4f_2 f_6 & 0 & 0 \end{bmatrix}$$

$$K = \begin{bmatrix} 1 & 2 & 6 \\ 2 & 0 & 0 \\ 3 & 0 & 0 \end{bmatrix}$$

и

$$H = \begin{bmatrix} \frac{1}{2}f_1^2 + \frac{1}{2}f_2 & \frac{1}{8}f_1^4 + \frac{3}{8}f_2^2 & \frac{1}{48}f_1^8 + \frac{7}{48}f_2^4 \\ \frac{1}{4}f_1^2 f_2 + \frac{1}{4}f_4 & 0 & 0 \\ \frac{1}{6}f_1^2 f_3^2 + \frac{1}{6}f_2 f_6 & 0 & 0 \end{bmatrix}$$

3.6 Линеарна група трансформација GL_n

У овом одељку, најпре се анализирају разлози због којих је директно рачунање на основу израза (2.34) неефикасно, а затим се показује како се уз помоћ унапред израчунатих табела H, циклусни индекс може ефикасно израчунати користећи израз (3.3).

3.6.1 Скуп A_n

Директна имплементација на основу израза (2.34) није ефикасна. Чак је и први корак, добијање скупа A_n (2.32), проблематичан: уопштени метод за

добијање решења линеарне диференцне једначине (`FrobeniusSolve[]` у програму Mathematica) веома је неефикасан већ за $n = 10$. Међутим, није тешко директно израчунати чланове низа скупова A_n. Једначина

$$\sum_{i=1}^{t_n} a_i d_i = n \tag{3.6}$$

еквивалентна је са

$$\sum_{i=1}^{n} i \sum_{j=t_{i-1}+1}^{t_i} a_j = n,$$

пошто за $j = t_{i-1} + 1, \ldots, t_i$ важи $d_j = i$. Како је P_n скуп решења $p = (p_1, p_2, \ldots, p_n)$ једначине $\sum_{i=1}^{n} p_i i = n$, део A_n који одговара партицији $p \in P_n$ једнак је Декартовом производу $\binom{p_i+t_i-t_{i-1}-1}{p_i}$ композиција p_i на $t_i - t_{i-1}$ ненегативних делова, $1 \leqslant i \leqslant n$.

Дужина низова у скупу A_n једнака је $t_n \leqslant \sum_{i=1}^{n}(2^i - 2)/i$ (видети на пример [4]), што је $O(2^n)$. Број таквих низова је 2^{n-1} (видети напомену 3.6.1). Дакле, сложеност рачунања на основу листе свих низова из A_n је $O(4^n)$.

Пример 3.6.1. *Елементи P_4 су врсте матрице*

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{bmatrix}.$$

Четири елемента ових вектора распоређени су у низовима $a \in A_4$ на позицијама $1 = t_1$, $2 = t_2$, од $3 = t_2 + 1$ до $4 = t_3$, и од $5 = t_3 + 1$ до $7 = t_4$ (видети табелу 3.2).

Табела 3.2: Партиције које одговарају низовима $a \in A_4$.

Партиција				Низ a						
				1	2	3	4	5	6	7
0	0	0	1	0	0	0	0	0	0	1
				0	0	0	0	0	1	0
				0	0	0	0	1	0	0
1	0	1	0	1	0	0	1	0	0	0
				1	0	1	0	0	0	0
0	2	0	0	0	2	0	0	0	0	0
2	1	0	0	2	1	0	0	0	0	0
4	0	0	0	4	0	0	0	0	0	0

Напомена 3.6.1. *Свако решење једначине* (3.6), $a \in A_n$ *једнозначно одговара полиному* $\prod_{i=1}^{t_n} P_i(x)^{a_i}$ *степена* n, *који није дељив са* x (*пошто* x *није укључен у низ* $P_i(x)$, $i = 1, 2, \ldots$, *јер је то једини полином коме је константни члан различит од* 1). *Таквих полинома има* 2^{n-1}, *па је* $|A_n| = 2^{n-1}$, *и важи идентитет*

$$\sum_{p \in P_n} \prod_{i=1}^{n} \binom{p_i + t_i - t_{i-1} - 1}{p_i} = 2^{n-1}.$$

3.6.2 Несводљиви полиноми

Циклусни индекс (2.34) зависи само од степена d_i и реда e_i полинома $P_i(x)$. Према томе, у циљу одређивања њихових степенова d_i и њихових редова e_i, $1 \leqslant i \leqslant t_i$, није неопходно одредити комплетну листу несводљивих полинома $P_i(x)$. Број $N(d, e)$ несводљивих полинома степена d и реда e је познат (видети на пример [27]). Постоји само један несводљиви полином $(x + 1)$ степена 1 и реда 1 (ред искљученог полинома x је недефинисан), па је $N(1, 1) = 1$. Ако је $d > 1$, полиноми степена d и реда e постоје ако и само ако је ред од 2 по модулу e једнак d (тј. $e \mid 2^d - 1$ и $e \nmid 2^k - 1$ за $k < d$); тада је број оваквих полинома једнак

$$N(d, e) = \phi(e)/d,$$

где је $\phi(e)$ Ојлерова функција ϕ. Скуп

$$m(d) = \{e \mid N(d, e) > 0\}$$

дефинише се рекурзивно изразом

$$m(d) = \{r \;\big|\; r \mid 2^d - 1\} \setminus \bigcup_{i=1}^{d-1} m(i),$$

(видети [30, низ A059912]). Ови скупови приказани су у табели 3.3 за $d \leqslant 7$. Последња колона уствари представља скуп $\{N(d, e) \mid e \in m(d)\}$.

Табела 3.3: Редови несводљивих полинома степена d, $d \leqslant 7$.

d	$\{r \mid r \mid 2^d - 1\}$	$m(d)$	$\lvert m(d)\rvert$	$N(d, e)$
1	$\{1\}$	$\{1\}$	1	$\{1\}$
2	$\{1, 3\}$	$\{3\}$	1	$\{1\}$
3	$\{1, 7\}$	$\{7\}$	1	$\{2\}$
4	$\{1, 3, 5, 15\}$	$\{5, 15\}$	2	$\{1, 2\}$
5	$\{1, 31\}$	$\{31\}$	1	$\{6\}$
6	$\{1, 3, 7, 9, 21, 63\}$	$\{9, 21, 63\}$	3	$\{1, 2, 6\}$
7	$\{1, 127\}$	$\{127\}$	1	$\{18\}$

Несводљиви полиноми $P_i(x)$ могу се поређати произвољним редоследом, па се може претпоставити да су поређани у складу са лексикографским поретком парова (d_i, e_i). За фиксирани пар (d_i, e_i), полиноми придружени $N(d_i, e_i)$ могу се такође поређати произвољним редоследом. Означимо са S_n скуп различитих парова $(d_i, e_i), 1 \leqslant i \leqslant t[n]$, тј.

$$S_n = \{(d_i, e_i) \mid (d_i, e_i) \neq (d_j, e_j), 1 \leqslant j < i \leqslant t[n]\}.$$

Нека је $s_n = |S_n|$, $n \geqslant 1$, и нека је због једноставности $s_0 = 0$. Нека (d'_k, e'_k) представља k-ти елемент S_n у лексикографском поретку. Означимо са

$$n_k = N(d'_k, e'_k) = \phi(e'_k)/d'_k \tag{3.7}$$

број несводљивих полинома степена d'_k и реда e'_k. Нека је $N_0 = 0$, и $N_k = N_{k-1} + n_k$, $k \geqslant 1$. Неколико првих чланова низова d_i, e_i, d'_k, e'_k, n_k, N_k, t_n и s_n приказани су у табелама 3.4, 3.5 и 3.6.

Табела 3.4: Низови d и e.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
d_i	1	2	3	3	4	4	4	5	5	5	5	5	5
e_i	1	3	7	7	5	15	15	31	31	31	31	31	31

Табела 3.5: Низови d', e', n_k и N_k.

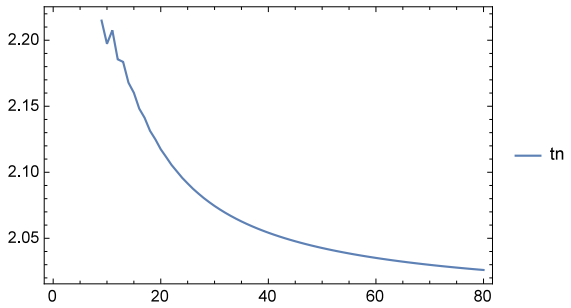
k	0	1	2	3	4	5	6	7	8	9	10
d'_k		1	2	3	4	4	5	6	6	6	7
e'_k		1	3	7	5	15	31	9	21	63	127
n_k		1	1	2	1	2	6	1	2	6	18
N_k	0	1	2	4	5	7	13	14	16	22	40

Табела 3.6: Низови t_n и s_n.

n	0	1	2	3	4	5	6	7	8	9	10
t_n	0	1	2	4	7	13	22	40	70	126	225
s_n	0	1	2	3	5	6	9	10	14	16	21

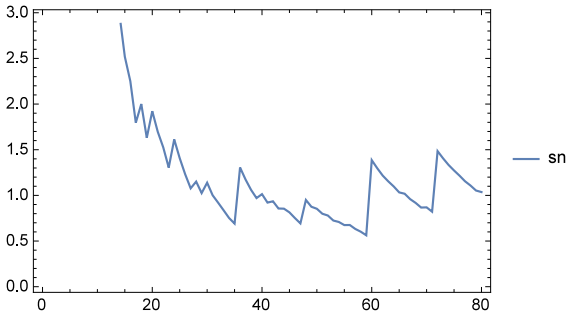
Нека $s_0(n)$ означава број делилаца броја n, који се грубо може апроксимирати са $s_0(n) = O(\log n)$, видети [9, Dirichlet Divisor Problem]. Одавде проистиче груба оцена $s_n \leqslant \sum_{i=1}^{n} s_0(2^i - 1) = O(n^2)$. Однос $s_n/(n^4/2500)$,

$1 \leqslant n \leqslant 80$, приказан на слици 3.1 сугерише да прецизнија оцена може да буде $s_n \sim n^4/2500$, бар за $n \leqslant 80$. Број t_n може бити оцењен са $t_n = O(2^n)$. У ствари, однос $t_n/(2^n/n)$, $1 \leqslant n \leqslant 80$, приказан на слици 3.2, упућује на оцену $t_n \sim 2^{n-1}/n$, $1 \leqslant n \leqslant 80$. Може се закључити да t_n расте много брже него s_n, односно да је за велико n низ A_n много дужи од низа S_n.



Слика 3.1: Однос $\frac{t_n}{2^n/n}$, $1 \leqslant n \leqslant 80$

,



Слика 3.2: Однос $\frac{s_n}{n^4/2500}$, $1 \leqslant n \leqslant 80$

,

3.6.3 Групе еквивалентних низова у скупу A_n

Ако уведемо ознаку

$$GL(a) = \sum_{\alpha \in P_{a_1} \times \cdots \times P_{a_{t_n}}} \frac{M_n \bigtimes_{i=1}^{t_n} \bigtimes_{j=1}^{a_i} \left(f_1 \prod_{k=1}^{j} f_{q_{ik}}^{h_{ik}}\right)^{\times \alpha_{ij}}}{\prod_{i=1}^{t_n} 2^{d_i S(\alpha_i)} \prod_{j=1}^{a_i} \prod_{k=1}^{\alpha_{i,j}} (2^{kd_i} - 1)}$$

(за ознаку $S(\cdot)$ видети (2.33)), тада је

$$Z_{\mathrm{GL}_n} = \frac{1}{M_n} \sum_{a \in A_n} GL(a).$$

За фиксирано i, $1 \leqslant i \leqslant s_n$, постоји n_i (3.7) несводљивих полинома $\{P_k(x) \mid N_{i-1} < k \leqslant N_i\}$ са истим степеном d_i' и истим редом e_i'. Пошто $GL(a)$ зависи само од броја c_j елемента a_k, $N_{i-1} < k \leqslant N_i$, који су једнаки j, $j = 0, 1, \ldots, \lfloor n/d_i' \rfloor$, није неопходно рачунати свих 2^{n-1} израза придружених елементима скупа A_n у (2.34).

Пример 3.6.2. *За $n = 5$, постоји 6 таквих група индекса у низу a:* $\{1\}$, $\{2\}$, $\{3, 4\}$, $\{5\}$, $\{6, 7\}$, *и* $\{8, 9, \ldots, 13\}$, *види табелу 3.4.*

За фиксирано $a \in A_n$ нека

$$C(a) = [c_{i,j}], \quad 1 \leqslant i \leqslant s_n, \quad 0 \leqslant j \leqslant \lfloor n/d_i' \rfloor$$

означава матрицу са елементима

$$c_{i,j}(a) = |\{k \mid N_{i-1} + 1 \leqslant k \leqslant N_i,\ a_k = j\}|.$$

Ова матрица описује низ a: вредности $GL(a)$ за све низове $a \in A_n$ са истом матрицом $C(a)$ су једнаки, тј. ти низови су узајамно еквивалентни. У циљу рачунања циклусног индекса, довољно је израчунати $GL(a)$ за само један низ из класе таквих низова (”канонски” низ) и помножити добијену вредност величином класе:

$$N(a) = \prod_{i=1}^{s_n} \binom{n_i}{c_{i,0}, c_{i,1}, \ldots, c_{i,\lfloor n/d_i' \rfloor}}$$

За $k_1 + k_2 + \cdots + k_p = n$

$$\binom{n}{k_1, k_2, \ldots, k_p} = \frac{n!}{k_1! k_2! \cdots k_p!}$$

означава мултиномијални коефицијент. За ”канонски” низ a може се узети низ за који важи $a_{N_{i-1}+1} \geqslant a_{N_{i-1}+2} \geqslant \cdots \geqslant a_{N_i}$.

Ако уведемо ознаку $B_n = \{(b_1, b_2, \ldots, b_{s_n}) \mid \sum_{i=1}^{s_n} b_i d_i' = n$, тада је број канонских низова

$$c_n = \sum_{b \in B_n} \prod_{i=1}^{s_n} p(b_i, n_i).$$

Овај број може се израчунати знатно ефикасније. Ако је a низ ненегативних целих бројева, нека је $a[i..j] = \{a_i, a_{i+1}, \ldots, a_j\}$. Означимо са

$$C(m,k) = \{a[1..k] \mid \sum_{i=1}^{k} a_i = m\}$$

скуп композиција броја m од највише k делова. Тада је

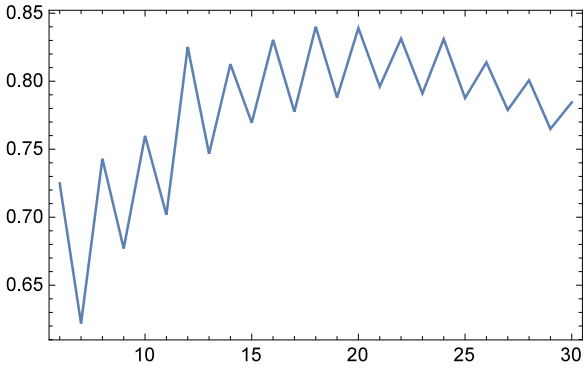
$$c_n = \sum_{p\in P_n} \prod_{d=1}^{n} \sum_{m[1..s_d-s_{d-1}]\in C(p_d,s_d-s_{d-1})} \prod_{k=1}^{s_d-s_{d-1}} p(m_k, n_{s_{d-1}+k}).$$

Табела 3.7 приказује број c_n канонских низова и $|A_n|$ за $n \leqslant 12$. Слика 3.3 приказује однос $c_n/1.784^k$, што сугерише оцену $c_n \sim 1.784^k$, барем за $n \leqslant 30$. Дакле, за велико n, број канонских низова знатно је мањи од укупног броја низова у скупу A_n.

Табела 3.7: Бројеви c_n и $|A_n| = 2^{n-1}$.

n	2	3	4	5	6	7	8	9	10	11	12
c_n	2	3	6	8	16	21	38	52	87	119	206
$\|A_n\|$	2	4	8	16	32	64	128	256	512	1024	2048

Слика 3.3: Однос $c_n/1.784^k$, $n \leqslant 30$.



Пример 3.6.3. *За $n = 5$ међу 16 низова a, постоји 8 канонских. Сума $Z_{\mathrm{GL}_5} = \frac{1}{M_5}\sum_{a\in A_5} GL(a)$ са 16 сабирака може се заменити сумом сабирака $N(a)GL(a)$ по скупу од 8 канонских низова (видети табелу 3.8).*

Табела 3.8: Бројеви $N(a)$ и $GL(a)$, $n = 5$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	$N(a)$
d_i	1	2	3	3	4	4	4	5	5	5	5	5	5	
	Низ a													
1	0	0	0	0	0	0	0	1	0	0	0	0	0	6
2	0	1	1	0	0	0	0	0	0	0	0	0	0	2
3	1	0	0	0	0	1	0	0	0	0	0	0	0	2
4	1	0	0	0	1	0	0	0	0	0	0	0	0	1
5	1	2	0	0	0	0	0	0	0	0	0	0	0	1
6	2	0	1	0	0	0	0	0	0	0	0	0	0	2
7	3	1	0	0	0	0	0	0	0	0	0	0	0	1
8	5	0	0	0	0	0	0	0	0	0	0	0	0	1

$N(a)$	$GL(a)$
6	$322560 f_1 f_{31}$
2	$476160 f_1 f_3 f_7 f_{21}$
2	$666624 f_1^2 f_{15}^2$
1	$666624 f_1^2 f_5^6$
1	$833280 f_1^2 f_3^2 f_6^4 + 55552 f_1^2 f_3^{10}$
2	$714240 f_1^2 f_2 f_7^2 f_{14} + 238080 f_1^4 f_7^4$
1	$833280 f_1^2 f_2 f_3^2 f_4 f_6 f_{12} + 416640 f_1^4 f_2^2 f_3^4 f_6^2$ $+19840 f_1^8 f_3^8$
1	$624960 f_1^2 f_2 f_4^3 f_8^2 + 78120 f_1^4 f_2^6 f_4^4 +$ $312480 f_1^4 f_2^2 f_4^6 + 6510 f_1^8 f_2^{12} +$ $651026040 f_1^8 f_2^4 f_4^4 + 465 f_1^{16} f_{2^8} + f_1^{32}$

3.6.4 Табеле H

Поред доказа теореме 3.6.1 да се Z_{GL_n} може представити изразом (3.3), доказују се три помоћне леме.

Лема 3.6.1. *Нека је*

$$F'_{ijk} = \big(f_1 \prod_{p=1}^{j} f_{q_{ip}}^{h_{ip}}\big)^{\times k}, \quad 1 \leqslant i \leqslant t_n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{d_i} \right\rfloor,\ 1 \leqslant k \leqslant \left\lfloor \frac{n}{j d_i} \right\rfloor,$$

$$D_{ij} = \prod_{p=1}^{j} (2^{ip} - 1), \quad 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{i} \right\rfloor,$$

и

$$G'_{i,a} = \sum_{\alpha \in P_a} 2^{-d_i S(\alpha)} \bigtimes_{\substack{1 \leqslant j \leqslant a \\ \alpha_j > 0}} \frac{F'_{i,j,\alpha_j}}{D_{d_i,\alpha_j}}, \quad 1 \leqslant i \leqslant t_n,\ 1 \leqslant a \leqslant n.$$

Тада је

$$Z_{\mathrm{GL}_n} = \sum_{a\in A_n} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} G'_{i,a_i} \tag{3.8}$$

Доказ. Ако означимо

$$F''_{i,j,\alpha_{ij}} = \frac{F'_{i,j,\alpha_{ij}}}{2^{d_i S(\alpha_i)/a_i} D_{d_i,\alpha_{ij}}},$$

тада циклусни индекс Z_{GL_n} постаје

$$\begin{aligned}
&\sum_{a\in A_n} \sum_{\alpha\in P_{a_1}\times\cdots\times P_{a_{t_n}}} \frac{\displaystyle\bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} F'_{i,j,\alpha_{ij}}}{\displaystyle\prod_{i=1}^{t_n} 2^{d_i S(\alpha_i)} \prod_{j=1}^{a_i} D_{d_i,\alpha_{ij}}}\\
&= \sum_{a\in A_n} \sum_{\alpha\in P_{a_1}\times\cdots\times P_{a_{t_n}}} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} F''_{i,j,\alpha_{ij}}\\
&= \sum_{a\in A_n} \left(\left(\sum_{\alpha_1\in P_{a_1}} \bigtimes_{\substack{1\leqslant j\leqslant a_1\\ \alpha_{1,j}>0}} F''_{1,j,\alpha_{1,j}} \right) \times \cdots \quad \times \left(\sum_{\alpha_{t_n}\in P_{a_{t_n}}} \bigtimes_{\substack{1\leqslant j\leqslant a_{t_n}\\ \alpha_{t_n,j}>0}} F''_{t_n,j,\alpha_{t_n,j}} \right) \right)\\
&= \sum_{a\in A_n} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} \sum_{\alpha_i\in P_{a_i}} \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} F''_{i,j,\alpha_{ij}}\\
&= \sum_{a\in A_n} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} \sum_{\alpha_i\in P_{a_i}} \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} \frac{F'_{i,j,\alpha_{ij}}}{2^{d_i S(\alpha_i)/a_i} D_{d_i,\alpha_{ij}}}\\
&= \sum_{a\in A_n} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} \sum_{\alpha_i\in P_{a_i}} 2^{-d_i S(\alpha_i)} \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} \frac{F'_{i,j,\alpha_{ij}}}{D_{d_i,\alpha_{ij}}}
\end{aligned}$$

Према томе,

$$Z_{\mathrm{GL}_n} = \sum_{a\in A_n} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} G'_{i,a_i}$$

□

Вредности $G'_{i,a}$, $1 \leqslant i \leqslant t_n$, $1 \leqslant a \leqslant n$, могу се унапред израчунати, упамтити и потом искористити за ефикасније рачунање Z_{GL_n}. Добијени израз сличан је изразу (3.3); разлика је у броју сабирака: t_n расте много брже од $|P_n|$. Брисањем поновљених врста, ова табела димензија $t_n \times n$ може се сачувати у компримованом

облику у виду табеле G димензија $s_n \times n$. Прецизније, све врсте матрице G' са индексима i, $1 \leqslant i \leqslant t_n$, где је $(d_i, e_i) = (d, e)$ замењене су само једном врстом са индексом k таквим да је $(d'_k, e'_k) = (d, e)$ (видети табеле 3.4 и 3.5).

Пример 3.6.4. *Нека је $n = 3$; тада је*

$$F' = \begin{bmatrix} \{f_1^2, f_1^4, f_1^8\} & \{f_1^2 f_2\} & \{f_1^2 f_2 f_4\} \\ \{f_1 f_3, f_1 f_3^5\} & \{f_1 f_3 f_6^2\} & \{0\} \\ \{f_1 f_7\} & \{0\} & \{0\} \\ \{f_1 f_7\} & \{0\} & \{0\} \end{bmatrix}$$

(овде листе представљају трећу димензију у табели F'),

$$D = \begin{bmatrix} 1 & 3 & 21 \\ 3 & 45 & 0 \\ 7 & 0 & 0 \end{bmatrix}$$

и

$$G' = \begin{bmatrix} f_1^2 & \frac{1}{2} f_1^2 f_2 + \frac{1}{6} f_1^4 & \frac{1}{4} f_1^2 f_2 f_4 + \frac{1}{8} f_1^4 f_2^2 + \frac{1}{168} f_1^8 \\ \frac{1}{3} f_1 f_3 & 0 & 0 \\ \frac{1}{7} f_1 f_7 & 0 & 0 \\ \frac{1}{7} f_1 f_7 & 0 & 0 \end{bmatrix}.$$

Примећује се да табела G' садржи две исте врсте. Њиховом заменом једном врстом, добија се компримовани облик, табела G:

$$G = \begin{bmatrix} f_1^2 & \frac{1}{2} f_1^2 f_2 + \frac{1}{6} f_1^4 & \frac{1}{4} f_1^2 f_2 f_4 + \frac{1}{8} f_1^4 f_2^2 + \frac{1}{168} f_1^8 \\ \frac{1}{3} f_1 f_3 & 0 & 0 \\ \frac{1}{7} f_1 f_7 & 0 & 0 \end{bmatrix}.$$

Нека $|m(d)| = n_d$ означава број различитих редова несводљивих полинома степена n (видети 3.6.2), и нека

$$m(d) = \{E_1, E_2, \ldots, E_{n_d}\}, \quad E_1 < E_2 < \cdots < E_{n_d}$$

означава скуп тих редова. Нека $n(d, j) = N(d, E_j)$, $1 \leqslant j \leqslant n_d$, означава број полинома степена d и реда E_j. Нека је

$$S_{d,i} = \{j \mid 1 \leqslant j \leqslant t_d,\ d_j = d,\ e_j = E_i\}.$$

Следећа лема показује како израз (3.14) за Z_{GL_n} може бити додатно поједностављен.

Лема 3.6.2. *За $1 \leqslant d, q \leqslant n$ нека $H_{d,q}$ означава израз*

$$H_{d,q} = \sum_{a[t_{d-1}+1..t_d]\in C(q,t_d-t_{d-1})} \bigtimes_{\substack{t_{d-1}+1\leqslant i\leqslant t_d \\ a_i>0}} G'_{i,a_i}. \tag{3.9}$$

Тада је

$$Z_{\mathrm{GL}_n} = \sum_{p\in P_n} \bigtimes_{d=1}^{n} H_{d,p_d}.$$

Доказ. Израз (3.14) за Z_{GL_n} може се трансформисати на следећи начин

$$\begin{aligned}
&\sum_{p\in P_n} \sum_{a[t_0+1..t_1]\in C(p_1,t_1-t_0)} \cdots \sum_{a[t_{n-1}+1..t_n]\in C(p_n,t_n-t_{n-1})} \bigtimes_{\substack{1\leqslant i\leqslant t_n \\ a_i>0}} G'_{i,a_i} \\
= &\sum_{p\in P_n} \sum_{a[t_0+1..t_1]\in C(p_1,t_1-t_0)} \cdots \sum_{a[t_{n-1}+1..t_n]\in C(p_n,t_n-t_{n-1})} \\
&\left(\bigtimes_{\substack{t_0+1\leqslant i\leqslant t_1 \\ a_i>0}} G'_{i,a_i}\right) \times \cdots \times \left(\bigtimes_{\substack{t_{n-1}+1\leqslant i\leqslant t_n \\ a_i>0}} G'_{i,a_i}\right) \\
= &\sum_{p\in P_n} \bigtimes_{\substack{1\leqslant d\leqslant n \\ p_d>0}} \left(\sum_{a[t_{d-1}+1..t_d]\in C(p_d,t_d-t_{d-1})} \bigtimes_{\substack{t_{d-1}+1\leqslant i\leqslant t_d \\ a_i>0}} G'_{i,a_i}\right) \\
= &\sum_{p\in P_n} \bigtimes_{d=1}^{n} H_{d,p_d}.
\end{aligned}$$

□

Коришћење унапред израчунатих вредности $H_{d,q}$, $1 \leqslant d,\ q \leqslant n$, које се памте у табели, додатно поједностављује израчунавање Z_{GL_n}.

Пошто се сви елементи низова дужине t_n појављују у изразу (3.15), проблем се своди на ефикасно рачунање табеле H. Следећа лема показује како се тај проблем може решити коришћењем идеје канонских низова $a \in A_n$.

Лема 3.6.3. *Нека $s_{d,i}$ означава индекс j, такав да је $d'_j = d,\ e'_j = E_i$. Тада за $1 \leqslant d,\ q \leqslant n$ важи*

$$H_{d,q} = \sum_{\sum_{k=1}^{n_d} b_k = q} \bigtimes_{\substack{1\leqslant j\leqslant n_d \\ b_j>0}} \left(\sum_{\sum_{k=0}^{b_j} kc_k = b_j} \binom{b_j}{c_0, c_1, \ldots, c_{b_j}} \bigtimes_{\substack{1\leqslant k\leqslant b_j \\ c_k>0}} G_{s_{d,i},k}^{\times c_k}\right). \tag{3.10}$$

Доказ. Израз (3.15) представља суму по свим композицијама $a[t_{d-1}+1..t_d]$ броја q на $t_d - t_{d-1}$ делова. Ове композиције могу се добити од композиција бројева $b[1..n_d]$, надовезивањем n_d композиција $b[j]$ у сабирке $\{a[i],\ i \in S_{d,j}\}$, $1 \leqslant j \leqslant n_d$. На тај начин, израз (3.15) за $H_{d,q}$ може се трансформисати у облик

$$\begin{aligned}
&\sum_{a[t_{d-1}+1..t_d]\in C(q,t_d-t_{d-1})} \bigtimes_{\substack{t_{d-1}+1\leqslant i\leqslant t_d\\ a_i>0}} G'_{i,a_i} \\
&= \sum_{b[1..n_d]\in C(q,n_d)} \sum_{\sum_{k_1\in S_{d,1}} a_{k_1} = b_1} \cdots \sum_{\sum_{k_{n_d}\in S_{d,n_d}} a_{k_{n_d}} = b_{n_d}} \bigtimes_{\substack{i_1\in S_{d,1}\\ a_{i_1}>0}} G'_{i_1,a_{i_1}} \cdots \bigtimes_{\substack{i_{n_d}\in S_{d,n_d}\\ a_{i_{n_d}}>0}} G'_{i_{n_d},a_{i_{n_d}}} \\
&= \sum_{b[1..n_d]\in C(q,n_d)} \left(\sum_{\sum_{k\in S_{d,1}} a_k = b_1} \bigtimes_{\substack{i_1\in S_{d,1}\\ a_{i_1}>0}} G'_{i_1,a_{i_1}} \right) \bigtimes \cdots \bigtimes \left(\sum_{\sum_{k\in S_{d,n_d}} a_k = b_{n_d}} \bigtimes_{\substack{i_{n_d}\in S_{d,n_d}\\ a_{i_{n_d}}>0}} G'_{i_{n_d},a_{i_{n_d}}} \right) \\
&= \sum_{b[1..n_d]\in C(q,n_d)} \bigtimes_{\substack{1\leqslant j\leqslant n_d\\ b_j>0}} \left(\sum_{\sum_{k\in S_{d,j}} a_k = b_j} \bigtimes_{\substack{i_j\in S_{d,j}\\ a_{i_j}>0}} G'_{i_j,a_{i_j}} \right).
\end{aligned}$$

Вредност $G'_{i_j,a_{i_j}}$ унутар групе $S_{d,j}$ зависи само од другог индекса, a_{i_j}. Први индекс може бити произвољно изабран, рецимо $\min S_{d,j}$. Поред тога, табела G' може се заменити мањом табелом G, зато што је $G'_{\min S_{d,j},a_{i_j}} = G_{s_{d,j},a_{i_j}}$. Дакле, унутрашња сума у последњем изразу постаје

$$\sum_{\sum_{k\in S_{d,j}} a_k = b_j} \bigtimes_{\substack{i\in S_{d,j}\\ a_i>0}} G_{s_{d,j},a_i}.$$

Свих

$$\binom{b_j}{c_0, c_1, \ldots, c_{b_j}}$$

сабирака у суми придружених скупу $\{a_k \mid k \in S_{d,j}\}$ таквих да је $|\{k \mid a_k = i\}| = c_i$, $1 \leqslant i \leqslant b_j$, међусобно су једнаки. Стога се унутрашња сума може представити у облику

$$\sum_{\sum_{k=0}^{b_i} kc_k = b_i} \binom{b_j}{c_0, c_1, \ldots, c_{b_j}} \bigtimes_{\substack{1\leqslant k\leqslant b_j\\ c_k>0}} G^{\times c_k}_{s_{d,j},k}.$$

Коначно је

$$H_{d,q} = \sum_{\substack{\sum_{k=1}^{n_d} b_k = q \\ 1\leqslant j\leqslant n_d \\ b_j>0}} \bigtimes \left(\sum_{\sum_{k=0}^{b_j} kc_k = b_j} \binom{b_j}{c_0, c_1, \ldots, c_{b_j}} \bigtimes_{\substack{1\leqslant k\leqslant b_j \\ c_k>0}} G_{s_{d,i},k}^{\times c_k} \right).$$

□

Пример 3.6.5. *За $n = 3$ је*

$$H = \begin{bmatrix} f_1^2 & \frac{1}{2}f_1^2 f_2 + \frac{1}{6}f_1^4 & \frac{1}{4}f_1^2 f_2 f_4 + \frac{1}{8}f_1^4 f_2^2 + \frac{1}{168}f_1^8 \\ \frac{1}{3}f_1 f_3 & 0 & 0 \\ \frac{2}{7}f_1 f_7 & 0 & 0 \end{bmatrix}.$$

Обједињавањем претходно изнетих чињеница долази се до наредног тврђења.

Теорема 3.6.1. *За $1 \leqslant i \leqslant s_n$ и $1 \leqslant j \leqslant n$ нека је (видети 3.6.2)*

$$q'_{ij} = e'_i 2^{\lceil log_2 j \rceil}, \qquad h'_{ij} = \frac{2^{d'_i(j-1)}(2^{d'_i} - 1)}{q'_{ij}}. \tag{3.11}$$

Означимо

$$F_{ijk} = \big(f_1 \prod_{p=1}^{j} f_{q'_{ip}}^{h'_{ip}}\big)^{\times k}, \quad 1 \leqslant i \leqslant s_n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{d_i} \right\rfloor,\ 1 \leqslant k \leqslant \left\lfloor \frac{n}{jd_i} \right\rfloor,$$

$$D_{ij} = \prod_{p=1}^{j} (2^{ip} - 1), \quad 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{i} \right\rfloor,$$

и

$$G_{i,a} = \sum_{\alpha \in P_a} 2^{-d_i S(\alpha)} \bigtimes_{\substack{1\leqslant j\leqslant a \\ \alpha_j>0}} \frac{F_{i,j,\alpha_j}}{D_{d_i,\alpha_j}}, \quad 1 \leqslant i \leqslant s_n,\ 1 \leqslant a \leqslant n. \tag{3.12}$$

Нека $s_{d,i}$ означава индекс j, такав да $d'_j = d$, $e'_j = E_i$. Означимо са $H_{d,q}$, $1 \leqslant d, q \leqslant n$, следећи израз

$$\sum_{\substack{\sum_{k=1}^{n_d} b_k = q \\ 1\leqslant j\leqslant n_d \\ b_j>0}} \bigtimes \left(\sum_{\sum_{k=0}^{b_j} kc_k = b_j} \binom{b_j}{c_0, c_1, \ldots, c_{b_j}} \bigtimes_{\substack{1\leqslant k\leqslant b_j \\ c_k>0}} G_{s_{d,i},k}^{\times c_k} \right). \tag{3.13}$$

Тада је

$$Z_{\mathrm{GL}_n} = \sum_{p \in P_n} \bigtimes_{d=1}^{n} H_{d,p_d}.$$

3.7 Афина група трансформација AGL_n

Израз за циклусни индекс (2.35) изводи се слично као и за линеарну групу.

Лема 3.7.1. *За $1 \leqslant i \leqslant s_n$ и $1 \leqslant j \leqslant n$ нека је (видети (3.11))*

$$u_{ij} = \begin{cases} 2^{j-1} f_1 \prod_{k=1}^{j} f_{q'_{1k}}^{h'_{1k}} + 2^{j-1} f_{q'_{1(j+1)}}^{\overline{q'^{2^j}_{1(j+1)}}}, & i = 1 \\ 2^{jd_i} f_1 \prod_{k=1}^{j} f_{q'_{ik}}^{h'_{ik}}, & i > 1 \end{cases}$$

и нека је

$$F'_{ijk} = u_{ij}^{\times k}, \quad 1 \leqslant i \leqslant t_n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{d_i} \right\rfloor,\ 1 \leqslant k \leqslant \left\lfloor \frac{n}{jd_i} \right\rfloor,$$

$$D_{ij} = \prod_{p=1}^{j} (2^{ip} - 1), \quad 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{i} \right\rfloor,$$

и

$$G'_{i,a} = \sum_{\alpha \in P_a} 2^{-d_i S(\alpha)} \bigtimes_{\substack{1 \leqslant j \leqslant a \\ \alpha_j > 0}} \frac{F'_{i,j,\alpha_j}}{D_{d_i,\alpha_j}}, \quad 1 \leqslant i \leqslant t_n,\ 1 \leqslant a \leqslant n.$$

Тада је

$$Z_{\mathrm{AGL}_n} = \sum_{a \in A_n} \bigtimes_{\substack{1 \leqslant i \leqslant t_n \\ a_i > 0}} \frac{G'_{i,a_i}}{2^{a_i d_i}} \tag{3.14}$$

Доказ. Увођењем ознака

$$F''_{i,j,\alpha_{ij}} = \frac{F'_{i,j,\alpha_{ij}}}{2^{d_i S(\alpha_i)/a_i} D_{d_i,\alpha_{ij}}},$$

добија се

$$
\begin{aligned}
Z_{\mathrm{AGL}_n} &= \frac{1}{2^n}\sum_{a\in A_n}\ \sum_{\alpha\in P_{a_1}\times\cdots\times P_{a_{t_n}}} \frac{\bigtimes\limits_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \bigtimes\limits_{j=1}^{a_i} u_{ij}^{\times\alpha_{ij}}}{\prod\limits_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}} 2^{d_iS(\alpha_i)}\prod\limits_{j=1}^{a_i}\prod\limits_{k=1}^{\alpha_{ij}}(2^{kd_i}-1)}\\
&= \frac{1}{2^n}\sum_{a\in A_n}\ \sum_{\alpha\in P_{a_1}\times\cdots\times P_{a_{t_n}}} \frac{\bigtimes\limits_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \bigtimes\limits_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} F'_{i,j,\alpha_{ij}}}{\prod\limits_{i=1}^{t_n} 2^{d_iS(\alpha_i)}\prod\limits_{j=1}^{a_i} D_{d_i,\alpha_{ij}}}.\\
&= \frac{1}{2^n}\sum_{a\in A_n}\ \sum_{\alpha\in P_{a_1}\times\cdots\times P_{a_{t_n}}} \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} F''_{i,j,\alpha_{ij}}\\
&= \frac{1}{2^n}\sum_{a\in A_n}\left(\left(\sum_{\alpha_1\in P_{a_1}}\ \bigtimes_{\substack{1\leqslant j\leqslant a_1\\ \alpha_{1,j}>0}} F''_{1,j,\alpha_{1,j}}\right)\times\cdots\quad\times\left(\sum_{\alpha_{t_n}\in P_{a_{t_n}}}\ \bigtimes_{\substack{1\leqslant j\leqslant a_{t_n}\\ \alpha_{t_n,j}>0}} F''_{t_n,j,\alpha_{t_n,j}}\right)\right)\\
&= \frac{1}{2^n}\sum_{a\in A_n}\ \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \sum_{\alpha_i\in P_{a_i}}\ \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} F''_{i,j,\alpha_{ij}}\\
&= \frac{1}{2^n}\sum_{a\in A_n}\ \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \sum_{\alpha_i\in P_{a_i}}\ \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} \frac{F'_{i,j,\alpha_{ij}}}{2^{d_iS(\alpha_i)/a_i}D_{d_i,\alpha_{ij}}}\\
&= \sum_{a\in A_n}\ \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \frac{1}{2^{a_id_i}}\sum_{\alpha_i\in P_{a_i}} 2^{-d_iS(\alpha_i)}\ \bigtimes_{\substack{1\leqslant j\leqslant a_i\\ \alpha_{i,j}>0}} \frac{F'_{i,j,\alpha_{ij}}}{D_{d_i,\alpha_{ij}}}
\end{aligned}
$$

односно

$$Z_{\mathrm{AGL}_n} = \sum_{a\in A_n}\ \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\ \frac{G'_{i,a_i}}{2^{a_id_i}}$$

□

Лема 3.7.2. *За $1\leqslant d,q\leqslant n$ нека $H_{d,q}$ означава израз*

$$H_{d,q} = \frac{1}{2^{dq}}\sum_{a[t_{d-1}+1..t_d]\in C(q,t_d-t_{d-1})}\ \bigtimes_{\substack{t_{d-1}+1\leqslant i\leqslant t_d\\ a_i>0}} G'_{i,a_i}. \tag{3.15}$$

Тада је

$$Z_{\mathrm{AGL}_n} = \sum_{p\in P_n}\ \bigtimes_{d=1}^{n} H_{d,p_d}.$$

Доказ. Израз (3.14) за Z_{AGL_n} може се трансформисати на следећи начин

$$
\begin{aligned}
&\sum_{p\in P_n}\ \sum_{a[t_0+1..t_1]\in C(p_1,t_1-t_0)}\cdots\sum_{a[t_{n-1}+1..t_n]\in C(p_n,t_n-t_{n-1})}\ \bigtimes_{\substack{1\leqslant i\leqslant t_n\\ a_i>0}}\frac{G'_{i,a_i}}{2^{a_i d_i}}\\
=&\sum_{p\in P_n}\ \sum_{a[t_0+1..t_1]\in C(p_1,t_1-t_0)}\cdots\sum_{a[t_{n-1}+1..t_n]\in C(p_n,t_n-t_{n-1})}\\
&\left(\bigtimes_{\substack{t_0+1\leqslant i\leqslant t_1\\ a_i>0}}\frac{G'_{i,a_i}}{2^{a_i d_i}}\right)\times\cdots\times\left(\bigtimes_{\substack{t_{n-1}+1\leqslant i\leqslant t_n\\ a_i>0}}\frac{G'_{i,a_i}}{2^{a_i d_i}}\right)\\
=&\sum_{p\in P_n}\ \sum_{a[t_0+1..t_1]\in C(p_1,t_1-t_0)}\cdots\sum_{a[t_{n-1}+1..t_n]\in C(p_n,t_n-t_{n-1})}\\
&\left(\prod_{\substack{t_0+1\leqslant i\leqslant t_1\\ a_i>0}}\frac{1}{2^{a_i d_i}}\bigtimes_{\substack{t_0+1\leqslant i\leqslant t_1\\ a_i>0}}G'_{i,a_i}\right)\times\cdots\times\left(\prod_{\substack{t_{n-1}+1\leqslant i\leqslant t_n\\ a_i>0}}\frac{1}{2^{a_i d_i}}\bigtimes_{\substack{t_{n-1}+1\leqslant i\leqslant t_n\\ a_i>0}}G'_{i,a_i}\right)\\
=&\sum_{p\in P_n}\ \bigtimes_{\substack{1\leqslant d\leqslant n\\ p_d>0}}\left(\sum_{a[t_{d-1}+1..t_d]\in C(p_d,t_d-t_{d-1})}\ \prod_{\substack{t_{d-1}+1\leqslant i\leqslant t_d\\ a_i>0}}\frac{1}{2^{a_i d_i}}\bigtimes_{\substack{t_{d-1}+1\leqslant i\leqslant t_d\\ a_i>0}}G'_{i,a_i}\right)\\
=&\sum_{p\in P_n}\ \bigtimes_{\substack{1\leqslant d\leqslant n\\ p_d>0}}\frac{1}{2^{dp_d}}\sum_{a[t_{d-1}+1..t_d]\in C(p_d,t_d-t_{d-1})}\ \bigtimes_{\substack{t_{d-1}+1\leqslant i\leqslant t_d\\ a_i>0}}G'_{i,a_i}\\
=&\sum_{p\in P_n}\ \bigtimes_{d=1}^{n}H_{d,p_d}.
\end{aligned}
$$

□

Лема 3.7.3. *Нека $s_{d,i}$ означава индекс j, $\overline{\text{такав}}$ да је $d'_j = d$, $e'_j = E_i$. Вредност $H_{d,q}$ (3.15) једнака је*

$$
\frac{1}{2^{dq}}\sum_{\sum_{k=1}^{n_d}b_k=q}\ \bigtimes_{\substack{1\leqslant j\leqslant n_d\\ b_j>0}}\left(\sum_{\sum_{k=0}^{b_j}kc_k=b_j}\binom{b_j}{c_0,c_1,\ldots,c_{b_j}}\bigtimes_{\substack{1\leqslant k\leqslant b_j\\ c_k>0}}G_{s_{d,i},k}^{\times c_k}\right). \tag{3.16}
$$

Доказ. Доказ се изводи аналогно као у леми 3.6.3. □

Теорема 3.7.1. *Нека је*

$$
F_{ijk}=u_{ij}^{\times k},\qquad 1\leqslant i\leqslant s_n,\ 1\leqslant j\leqslant\left\lfloor\frac{n}{d_i}\right\rfloor,\ 1\leqslant k\leqslant\left\lfloor\frac{n}{jd_i}\right\rfloor.
$$

$$D_{ij} = \prod_{p=1}^{j}(2^{ip}-1), \quad 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant \left\lfloor \frac{n}{i} \right\rfloor,$$

и

$$G_{i,a} = \sum_{\alpha \in P_a} 2^{-d_i S(\alpha)} \bigtimes_{\substack{1 \leqslant j \leqslant a \\ \alpha_j > 0}} \frac{F_{i,j,\alpha_j}}{D_{d_i,\alpha_j}}, \quad 1 \leqslant i \leqslant s_n,\ 1 \leqslant a \leqslant n. \tag{3.17}$$

Нека је елемент $H_{d,q}$, $1 \leqslant d, q \leqslant n$, матрице H дефинисан изразом

$$\frac{1}{2^{dq}} \sum_{\substack{n_d \\ \sum_{k=1} b_k = q}} \bigtimes_{\substack{1 \leqslant j \leqslant n_d \\ b_j > 0}} \left(\sum_{\substack{b_j \\ \sum_{k=0} k c_k = b_j}} \binom{b_j}{c_0, c_1, \ldots, c_{b_j}} \bigtimes_{\substack{1 \leqslant k \leqslant b_j \\ c_k > 0}} G_{s_{d,i},k}^{\times c_k} \right).$$

Тада је циклусни индекс Z_{AGL_n} дат изразом

$$Z_{\mathrm{AGL}_n} = \sum_{p \in P_n} \bigtimes_{d=1}^{n} H_{d,p_d}.$$

Приметимо да се (3.13) разликује од (3.16) за фактор $1/2^{dp}$ и да су елементи матрице у $H_{d,p}$ линеарне комбинације монома. Приметимо такође да се у изразу за u_{ij} појављује променљива $f_{q'_{1(j+1)}}$, тако да табеле F и D имају колону више у односу на одговарајуће табеле у изразу за GL_n.

Пример 3.7.1. *За $n = 3$ претходно израчунате табеле F', D, G и H су:*

$$F' = \left[\begin{array}{cccc} \{f_1^2, f_1^4, & \{f_1^2 f_2, & \{f_1^2 f_2 f_4\} & \{f_1^2 f_2 f_4^3\} \\ f_1^8, f_1^{16}\} & f_1^4 f_2^6\} & & \\ \hline \{f_1 f_3, f_1 f_3^5\} & \{f_1 f_3 f_6^2\} & \{1\} & \{1\} \\ \hline \{f_1 f_7\} & \{1\} & \{1\} & \{1\} \\ \hline \{f_1 f_7\} & \{1\} & \{1\} & \{1\} \end{array}\right],$$

$$D = \begin{bmatrix} 1 & 3 & 21 & 315 \\ 3 & 45 & 0 & 0 \\ 7 & 0 & 0 & 0 \end{bmatrix},$$

$$G = \left[\begin{array}{ccc} f_1^2 + f_2 & \frac{1}{6}f_1^4 + \frac{1}{2}f_2^2 + & \frac{f_1^8}{168} + \frac{7}{24}f_2^4 + \frac{3}{2}f_4^2 + \\ & +f_4 + f_1^2 f_2 & +\frac{1}{4}f_1^4 f_2^2 + f_1^2 f_2 f_4 \\ \hline \frac{4}{3}f_1 f_3 & 0 & 0 \\ \hline \frac{8}{7}f_1 f_7 & 0 & 0 \end{array}\right],$$

$$H = \left[\begin{array}{ccc} \frac{1}{2}f_1^2+ & \frac{1}{24}f_1^4+\frac{1}{8}f_2^2+ & \frac{f_1^8}{1344}+\frac{7}{192}f_2^4+\frac{3}{16}f_4^2+ \\ +\frac{1}{2}f_2 & +\frac{1}{4}f_4+\frac{1}{4}f_1^2f_2 & +\frac{1}{32}f_1^4f_2^2+\frac{1}{8}f_1^2f_2f_4 \\ \hline \frac{1}{3}f_1f_3 & 0 & 0 \\ \hline \frac{2}{7}f_1f_7 & 0 & 0 \end{array}\right].$$

3.8 Анализа добијених резултата

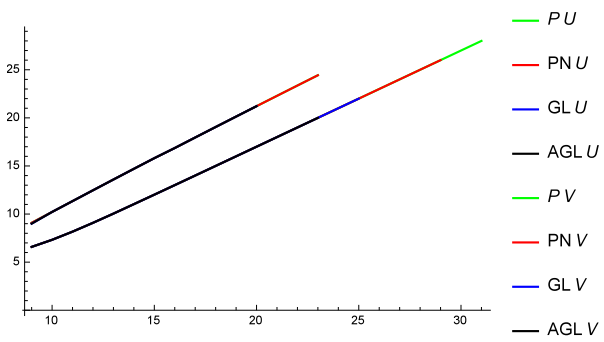
Табела 3.9 приказује максималну вредност n за коју су израчунате вредности U_n и V_n за све четири групе трансформација.

Табела 3.9: Добијени резултати

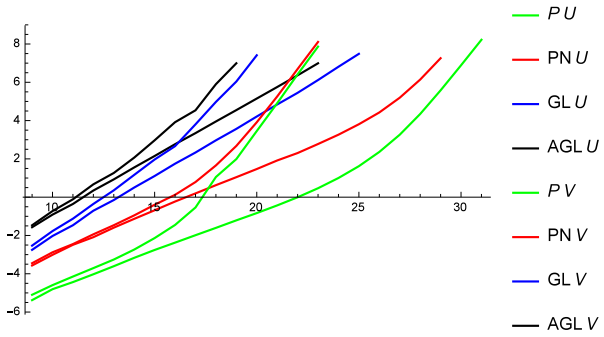
	S'_n	G_n	GL_n	AGL_n
U_n	33	32	31	31
V_n	27	27	26	26

Саме вредности U_n и V_n, $n \leqslant 10$, дате су у прилогу. За $n \geqslant 10$ уместо U_n и V_n приказан је број децималих цифара, првих 10 и последњих 10 децималних цифара тих бројева.

Пошто је $\log U_n = \Theta(2^n)$ и $\log V_n = \Theta(n2^n)$, логаритам величине потребног меморијског простора расте експоненцијално. Слика 3.4 приказује логаритам за основу 2 меморијског заузећа у току рачунања U_n и V_n за све четири групе (у даљем тексту подразумева се да је основа логаритма 2). Примећује се да заузеће меморије практично не зависи од конкретне групе трансформација. Бројеви U_n и V_n грубо се добијају дељењем 2^{2^n} и $2^{2^n!}$ са величинама четири групе, а те величине су мале у односу на укупне бројеве Булових и инвертибилних Булових функција. Време извршавања расте експоненцијално; слика 3.5 приказује логаритам времена извршавања израженог у милисекундама за U_n и V_n за све четири групе. Примећује се такође, да се на сликама 3.4 и 3.5, (где два дијаграма исте боје одговарају истој групи трансформација) дијаграм за V_n увек налази изнад одговарајућег дијаграма за U_n.

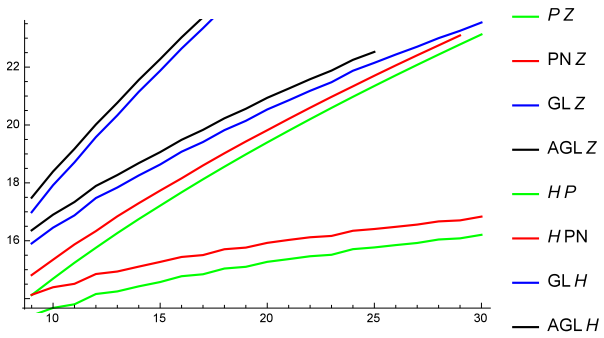


Слика 3.4: Логаритам величине потребног меморијског простора за U_n и V_n за све четири групе.

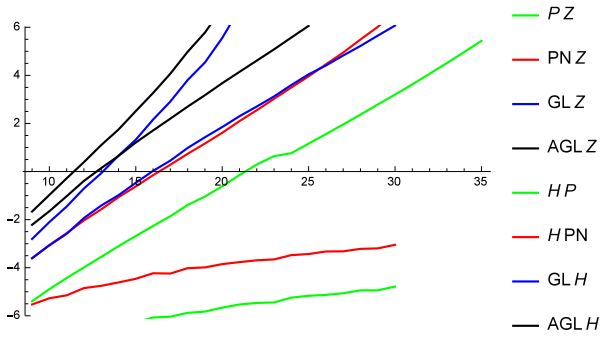


Слика 3.5: Логаритам времена извршавања израженог у милисекундама за U_n и V_n за све четири групе.

Број чланова циклусног индекса није лако оценити. Дијаграм на слици 3.6 сугерише да величине циклусног индекса и табеле H у бајтовима расту практично експоненцијално. Чини се да је и време извршавања при рачунању циклусног индекса и унапред израчунатих табела H такође експоненцијално, (видети слику 3.7). Користећи табелу H, рачунање циклусног индекса на основу израза (3.3) може се паралелизовати. У том смислу, табела H представља сажети облик циклусног индекса.

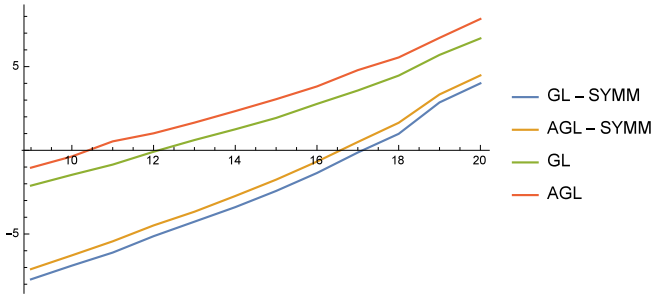


Слика 3.6: Логаритам меморијског заузећа при одређивању циклусног индекса и табеле H за све четири групе.



Слика 3.7: Логаритам времена извршавања у милисекундама при одређивању циклусног индекса и табеле H за све четири групе.

Дијаграм на слици 3.8 приказује резултат поређења логаритма времена извршавања при рачунању циклусног индекса за GL_n и AGL_n коришћењем последње верзије програма Symmetrica [15] у односу на наш програм. Програм Symmetrica је много бржи, али највеће вредности n које достиже су 21 за GL_n и 20 за AGL_n (узрок је вероватно меморијско заузеће, с обзиром да се циклусни индекс не користи у компримованом облику). Нагиб дијаграма програма Symmetrica нешто је већи од нагиба друга два дијаграма.



Слика 3.8: Логаритам времена извршавања у милисекундама при одређивању циклусног индекса за GL_n и AGL_n нашег Mathematica програма и програма Symmetrica [15].

Глава 4

Пребројавање класа еквиваленције монотоних Булових функција

Булова функција $f : \{0,1\}^n \mapsto \{0,1\}$ је монотона Булова функција од n променљивих ако за сваки пар вектора $x, y \in \{0,1\}^n$ из $x \leqslant y$ важи $f(x) \leqslant f(y)$. Две монотоне Булове функције су еквивалентне ако се пермутацијом улазних променљивих једна може добити од друге (видети одељак 2.1.7).

Нека је d_n број монотоних Булових функција n променљивих (такође познат као Дедекиндов број) и нека је r_n број нееквивалентних монотоних Булових функција. Одређивање бројева d_n и r_n је давно постављен проблем и вредности ових бројева до скоро су биле познате редом за $n \leqslant 8$ и $n \leqslant 7$ (видети табелу 4.1). У овом раду приказан је поступак рачунања $r_8 = 139219554888993358$. Резултат је пронађен практично у исто време када је објављен у раду [31] (такође видети [30], низ A003182).

Тренутно израчунате вредности за d_n и r_n, приказане су у табели 4.1 [30]. Табела познатих вредности допуњена је новодобијеном вредношћу r_8.

Пермутације улазних n-торки индукују пермутацију индукованих 2^n-торки. Као што је речено у трећем поглављу, да би се израчунао $U_n(S'_n)$ - број класа еквиваленције Булових функција с обзиром на групу пермутације променљивих, довољно је пронаћи структуру индукованих циклуса за сваку пермутацију и сваки циклус посматрати као фиксну тачку. Функција која је фиксна тачка пермутације на свим n-торкама произвољног циклуса пермутације треба да има исту вредност, 0 или 1.

Све пермутације које одговарају истој партицији броја n имају исту циклусну структуру. Скуп фиксних тачака пермутације може се представити усмереним графом у коме сваком индукованом циклусу одговара чвор (видети одељак 4.1). Моното-

Табела 4.1: Познате вредности за d_n и r_n.

n	d_n	r_n
1	3	3
2	6	5
3	20	10
4	168	30
5	7581	210
6	7828354	16353
7	2414682040998	490013148
8	56130437228687557907788	1392195548889993358

ним Буловим функцијама које су фиксне тачке пермутације тада одговарају монотоне доделе вредности 0 или 1 чворовима графа. Услов монотоности при додели вредности чворова графа подразумева да чвор следбеник не може узети мању вредност од чвора претходника.

У овом поглављу 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 $n \leqslant 8$.

4.1 Рачунање r_n на основу Фробенијусове теореме

У даљем тексту приказана је стратегија за добијање вредности r_8 на основу Фробенијусове теореме, као пондерисане аритметичке средине бројева монотоних Булових функција - фиксних тачака различитих класа пермутација $\pi' \in S'_n$ придружених партицијама из P_8. Бројеви фиксних тачака рачунају се применом три различита приступа:

- оптимизованом процедуром претраге коришћењем основне теореме 4.1.2;
- полазећи од скупа фиксних тачака који одговара скупу монотоних Булових функција од 6 променљивих
  - за партиције код којих су последња два сабирка једнака 1, видети одељак 4.2;

– за партиције где су сви сабирци једнаки 2, видети одељак 4.3.

Избором одговарајућег приступа за сваку партицију из P_8, вредност r_8 је израчуната након 45 часова рада Јава програма на персоналном рачунару.

Произвољна функција $f \in \mathcal{B}_n$ може се представити усмереним графом са $N = 2^n$ чворова:

- са чворовима $x \in B_n$ којима је додељена вредност функције $f(x)$,
- и са гранама $(x, y) \in B_n \times B_n$, где је $x < y$ и $w(x \oplus y) = 1$.

Пример оваквог графа за $n = 3$ приказан је у првој колони на слици 4.1. Нека је $\pi \in S_n$ произвољна пермутација. Придружена индукована пермутација π' разлаже B_n на циклусе, који су истовремено орбите пермутације π када делује на B_n. Орбита произвољног елемента $x \in B_n$ је скуп $\mathrm{orb}(x) = \{x, \pi(x), \pi^2(x), \ldots, \pi^{k-1}(x)\}$, где је $k = \min_{i \geqslant 1} \pi^i(x) = x$. Генерално, за задато $p = (p_1, p_2, \ldots, p_n) \in P_n$ нека је $G_p = (V_p, E_p)$ граф одређен разлагањем $n = a_1 + a_2 + \cdots + a_k$, у сабирке $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_k > 0$ које одговара партицији p (p у индексу графа одговара листи сабирака n која одговара партицији p) на следећи начин:

- Партиција p одређује пермутацију $\pi = \pi(p)$

$$(1\ 2\ \ldots\ a_1)(a_1+1\ \ldots\ a_1+a_2)\cdots(a_1+\cdots+a_{k-1}\ \ldots\ a_1+\cdots+a_k),$$

  која се састоји од k циклуса дужине редом $a_1, a_2, \ldots, a_k$.

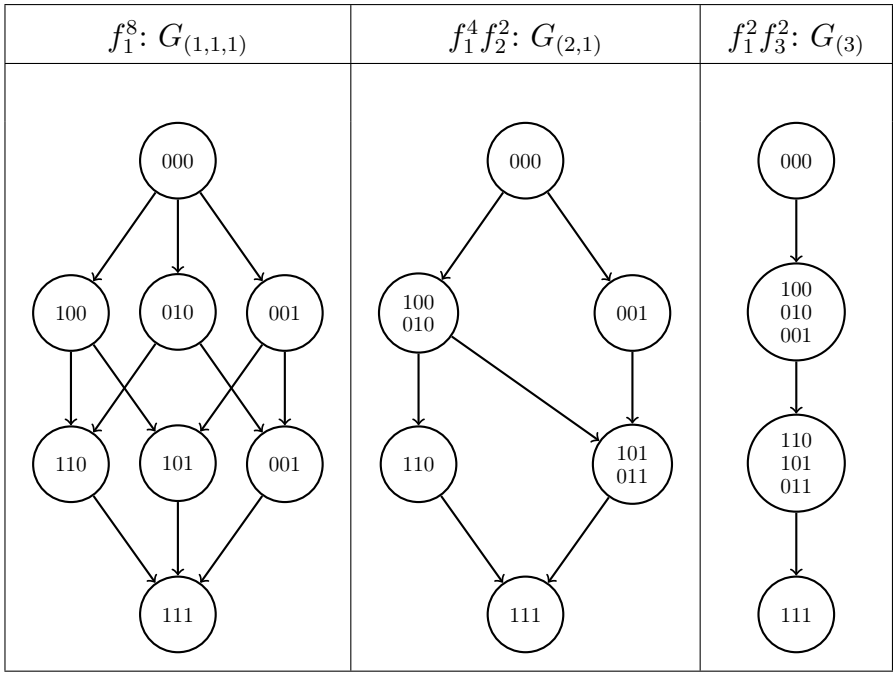
- Скуп чворова $V_p = \{\mathrm{orb}(x) \mid x \in B_n\}$ је скуп орбита у које π разлаже B_n.
- Скуп E_p састоји се од парова (u, v), $u, v \in V_p$, таквих да за неко $y \in v$ постоји $x \in u$, при чему је $x < y$ и $w(x \oplus y) = 1$.

Приметимо да се уместо пермутације $\pi(p)$, партицији p може доделити било која пермутација таква да важи $\mathrm{type}(\pi) = p$, пошто различите пермутације истог типа одговарају међусобно изоморфним графовима. Елементи произвољне орбите пермутације π имају исту Хемингову тежину. Ово омогућава да се дефинише *ниво* односно *слој* чвора v као $\mathrm{layer}(v) = w(x)$, где је x било која n-торка $x \in v$. Јасно је да у скупу G_p постоји барем један чвор на сваком нивоу $k = 0, 1, \ldots, n$, а чворови нивоа 0 и n састоје се редом од тачно једне n-торке $(0, 0, \ldots, 0)$ и $(1, 1, \ldots, 1)$.

Пример 4.1.1. *Партиције из* $P_3 = \{(3), (2,1), (1,1,1)\}$ *одређују редом пермутације* $(1\ 2\ 3)$, $(1\ 2)(3)$ *и* $(1)(2)(3)$, *и редом индуковане пермутације*

$$(0)(1\ 4\ 2)(3\ 5\ 6)(7),\ (0)(1)(2\ 4)(3\ 5)(6)(7) \text{ и } (0)(1)(2)(3)(4)(5)(6)(7)$$

Слика 4.1: Графови придружени партицијама из P_3.



(због јасноће, 1*-циклуси су експлицитно приказани). Типови ових пермутација редом одговарају трећем, другом и првом сабирку у циклусном индексу* $Z_{S_3'} = \frac{1}{6}(f_1^8 + 3f_1^4 f_2^2 + 2f_1^2 f_3^2)$*. Придружени графови редом имају* 8*,* 6 *и* 4 *чворова (видети слику 4.1).*

За фиксирану партицију $p \in P_n$, нека је $G = G_p = (V, E)$. Ако $V_k = \{v \in V \mid w(v) = k\}$ означава скуп чворова нивоа $k = 0, 1, \ldots, n$, тада се V разлаже на дисјунктну унију $V = V_0 \cup V_1 \cup \cdots \cup V_n$. Свака грана $(u, v) \in E$ повезује нека два чвора суседних нивоа, тј. $u \in V_k$ и $v \in V_{k+1}$ за неко k, $0 \leqslant k < n$. Нека је $t_k = |V_k|$ и $V_k = \{v_{k,1}, \ldots, v_{k,t_k}\}$, $0 \leqslant k \leqslant n$. Свако пресликавање $S : V \mapsto B_1$ једнозначно одговара Буловој функцији са константном вредношћу на орбитама пермутације π. Такве функције су фиксне тачке индуковане пермутације $\pi' : B_n \mapsto B_n$. Нека је $S = (S_0, S_1, \ldots, S_n)$, $S_k = \{S_{k,1}, \ldots, S_{k,t_k}\} \in B_{t_k}$, и за свако $k \in [0..n]$, $i \in [1..t_k]$ нека је $S_{k,i} = f(x)$ за свако $x \in V_{k,i}$. Вектор S придружен Буловој функцији f са константном вредношћу на n-торкама у сваком чвору је *стање* графа G; ако је f монотона функција, кажемо да је стање S такође монотоно. Нека $\mathrm{fix}(G)$ означава скуп свих монотоних стања графа G.

Напомена 4.1.1. *Нека је* $D_n = G_p$ *граф који је придружен партицији* $n = 1 + 1 + \cdots + 1$*. Скуп чворова графа* D_n *је* $\{\{x\} \mid x \in B_n\}$*, пошто је дужина сваке орбите идентичке пермутације једнака један; зато је* $\mathrm{fix}(D_n) = \mathcal{D}_n$ *скуп монотоних Бу-*

лових функција од n променљивих и $|\operatorname{fix}(D_n)| = d_n$. Вредности d_n познате су као Дедекиндови бројеви.

Пример 4.1.2. *Постоји 5 монотоних стања графа $G_{(3)}$ придруженог партицији броја $n = 3$ са једним сабирком једнаким 3 (чворови су нумерисани одозго на доле):*

$$\operatorname{fix}(G_{(3)}) = \{\{0,0,0,0\},\{1,0,0,0\},\{1,1,0,0\},\{1,1,1,0\},\{1,1,1,1\}\}.$$

За преостале две партиције броја 3 важи $|\operatorname{fix}(G_{(1,1,1)})| = d_3 = 20$ и $|\operatorname{fix}(G_{(2,1)})| = 10$.

Теорема 4.1.1. *Знајући $|\operatorname{fix}(G_p)|$ за свако $p \in P_n$, вредност r_n може се израчунати на основу израза*

$$r_n = \sum_{p \in P_n} \frac{|\operatorname{fix}(G_p)|}{\prod_i i^{p_i} p_i!}.$$

Доказ. За фиксирано $p \in P_n$ све пермутације типа p имају исти број монотоних стања као и пермутација $\pi = \pi(p)$. Пошто је $S_n \mapsto S'_n$ мономорфизам [24], број таквих пермутација је $g(p) = \frac{n!}{\prod_i i^{p_i} p_i!}$. Свако монотоно стање графа G_p једнозначно одговара фиксној тачки пермутације π', па доказ следи из Фробенијусове теореме. □

Пример 4.1.3. *Настављајући претходни пример, добија се*

$$r_3 = \tfrac{20}{1^3 3!} + \tfrac{10}{1^1 1! \cdot 2^1 1!} + \tfrac{5}{3^1 1!} = 10.$$

Фиксирано стање S_k чвора нивоа k у G, $0 \leqslant k < n$, потпуно одређује скуп $N^+_{k+1}(S_k)$ могућих монотоних стања S_{k+1} нивоа $k+1$, скупа t_{k+1}-торки $S_{k+1} \in B_{t_{k+1}}$ таквих да за сваку грану $(v_{k,i}, v_{k+1,j}) \in E$, $1 \leqslant i \leqslant t_k$, $1 \leqslant j \leqslant t_{k+1}$ важи неједнакост $S_{k,i} \leqslant S_{k+1,j}$. За фиксирано стање S_k нивоа k означимо са $T^+_k(S_k)$ стабло са ознакама чворова такво да корен има ознаку $S_k \in B_{t_k}$, а скуп конкатенација ознака на свим путевима од корена ка листовима представља скуп свих могућих стања $(S_k, S_{k+1}, \ldots, S_n)$. Ово стабло може се рекурзивно дефинисати на следећи начин:

$$T^+_k(S_k) = \begin{cases} \text{један чвор — корен,} & \text{за } k = n \\ \text{стабло са подстаблима } T^+_{k+1}(S_{k+1),}\ S_{k+1} \in N^+_{k+1}(S_k), & \text{за } k < n. \end{cases}$$

Нека је $G^+_k(S_k)$ број листова стабла $T^+_k(S_k)$, тј. број могућих вектора $(S_k, S_{k+1}, \ldots, S_n)$. Специјално, за $k = 0$, добија се $|\operatorname{fix}(G)| = G^+_0(\{0\}) + G^+_0(\{1\}) = G^+_0(\{0\}) + 1$.

Вредност $|\operatorname{fix}(G)|$ алтернативно се може добити одређивањем скупа свих могућих стања графа G у обрнутом редоследу, од виших ка нижим слојевима. Стање $S_k \in B_{t_k}$ чворова слоја k, $0 < k \leqslant n$, одређује скуп $N^-_{k-1}(S_k)$ свих могућух стања $S_{k-1} \in B_{t_{k-1}}$ слоја $k-1$, таквих да је $S_{k-1,i} \leqslant S_{k,j}$ за сваку грану $(v_{k-1,i}, v_{k,j}) \in E$, $1 \leqslant i \leqslant t_{k-1}$, $1 \leqslant j \leqslant t_k$. За фиксирано стање S_k слоја k графа G означимо са $T^-_k(S_k)$ стабло

са ознакама додељеним чворовима такво да корен има ознаку $S_k \in B_{t_k}$, а скуп конкатенација ознака на свим путањама од корена до листова је скуп свих могућих стања $(S_0, S_1, \ldots, S_k)$. Ово стабло се може дефинисати рекурзивно на следећи начин:

$$T_k^-(S_k) = \begin{cases} \text{један чвор — корен,} & \text{за } k = 0 \\ \text{стабло са подстаблима } T_{k-1}^-(S_{k-1}),\ S_{k-1} \in N_{k-1}^-(S_k), & \text{за } k > 0. \end{cases}$$

Нека $G_k^-(S_k)$ означава број листова стабла $T_k^-(S_k)$, тј. број могућих вектора $(S_0, S_1, \ldots, S_k)$. За $k = n$, добија се $|\operatorname{fix}(G)| = G_n^-(\{0\}) + G_n^-(\{1\}) = G_n^-(\{1\}) + 1$.

Комбиновањем ова два приступа долази се до ефикаснијег начина за одређивање $|\operatorname{fix}(G)|$, полазећи од скупа B_{t_k} свих могућих стања S_k средњег слоја $k = \lfloor n/2 \rfloor$. Пошто се за фиксирано стање S_k свако стање облика $(S_0, S_1, \ldots, S_k)$ може се упарити са сваким стањем облика $(S_k, S_{k+1}, \ldots, S_n)$, доказана је следећа теорема.

Теорема 4.1.2. *Нека је $p \in P_n$, $G = G_p$ и $0 < k < n$. Тада је*

$$|\operatorname{fix}(G)| = \sum_{S \in B_{t_k}} G_k^+(S) G_k^-(S).$$

Теорема омогућава рачунање $|\operatorname{fix}(G)|$ полазећи од скупа могућих стања изабраног слоја k. Поступак је најефикаснији ако се полази од средњег слоја $k = \lfloor n/2 \rfloor$.

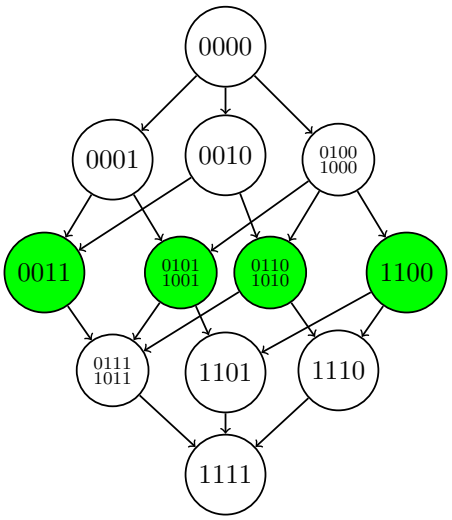
Пример 4.1.4. *За $n = 4$, граф $G_{(2,1,1)}$ има 12 чворова, видети слику 4.2. У средњем слоју 2 постоји $|S_2| = 4$ чвора (на слици су ти чворови обојени зеленом бојом). Табела поред слике приказује $G_2^+(S_2)$, $G_2^-(S_2)$ и $G_2^+(S_2)G_2^-(S_2)$ за свако могуће стање S_2. Збир ових производа једнак је $|\operatorname{fix}(G_{(2,1,1)})| = 50$. Стабла $T^+(S_2)$ и $T^-(S_2)$ за $S_2 = (1, 0, 1, 0)$ приказана су на десној страни слике 4.2.*

Рачунање $|\operatorname{fix}(G)|$ може се обавити још ефикасније коришћењем симетрија графа G. Нека је $\phi : V \mapsto V$ произвољни аутоморфизам графа G. Нека је S неко стање слоја V_k и нека је S' стање добијено из S, тако да важи $S'(v) = S(\phi(v))$ за свако $v \in V_k$. Тада је $G_k^+(S') = G_k^+(S)$, $G_k^-(S') = G_k^-(S)$. Према томе, може се:

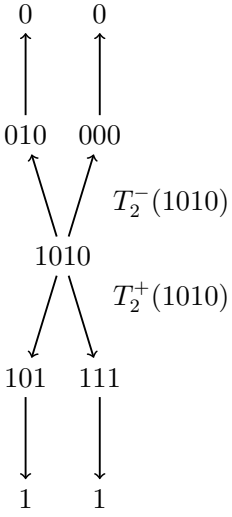
- одредити скуп представника класа еквиваленције скупа свих могућих стања слоја $k = \lfloor n/2 \rfloor$,
- одредити $G_k^+(S)$ и $G_k^-(S)$ за сваког представника S и
- израчунати суму производа $|C(S)|G_k^+(S)G_k^-(S)$, где $C(S)$ означава величину класе еквиваленције којој припада представник S.

Табела 4.5 приказује број аутоморфизама a_p графа G_p за све партиције $p \in P_8$.

Слика 4.2: Рачунање $|\operatorname{fix}(G_{(2,1,1)})|$ полазећи од скупа могућих стања средњег слоја.



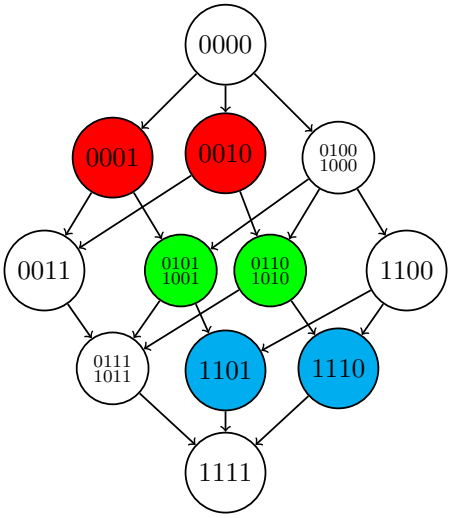
S_2	G_2^+	G_2^-	$G_2^+G_2^-$
0000	1	9	9
0001	1	2	2
0010	1	2	2
0011	1	1	1
0100	1	2	2
0101	1	1	1
0110	1	1	1
0111	2	1	2
1000	1	4	4
1001	1	1	1
1010	2	2	4
1011	2	1	2
1100	2	2	4
1101	2	1	2
1110	4	1	4
1111	9	1	9
$\lvert\operatorname{fix}(G_{(2,1,1)})\rvert$			50



Пример 4.1.5. *Настављајући претходни пример, означимо чворове графа на следећи начин:* $a = (1)$, $b = (2)$, $c = (5\ 9)$, $d = (6\ 10)$, $e = (13)$ *и* $f = (14)$, *видети слику 4.3. Група аутоморфизама састоји се од идентичке трансформације и пермутације* $(a\ b)(c\ d)(e\ f)$. *Аутоморфизам* $(a\ b)(c\ d)(e\ f)$ *разлаже скуп од* 16 *могућих стања* S_2 *на* 12 *класа еквиваленције; парови чворова означени истом бојом чине орбите аутоморфизма. Стања која припадају истој класи еквиваленције уписана су у табели унутар слике 4.3.*

Сложеност израчунавања $|\operatorname{fix}(G_p)|$ ограничена је с доње стране бројем различитих стања средњег слоја графа G_p. Табела 4.5 приказује величине m_p средњег слоја графа G_p за сваку партицију $p \in P_8$. Највећи средњи слој од 70 чворова има граф D_8 придружен партицији f_1^8. На сву срећу, број d_8 монотоних стања графа D_8 већ је познат. Наредни случај по тежини је граф придружен партицији $f_1^6 f_2$ са 50 чворова у средњем слоју, због чега је рачунање $|\operatorname{fix}(G_p)|$ на основу теореме 4.1.2 крајње неефиксано. У следећем одељку, приказује се ефикаснији начин рачунања $|\operatorname{fix}(G_p)|$ у случају када су у партицији $p \in P_8$ последња два сабирка јединице; полази се од

Слика 4.3: Коришћење аутоморфизама графа у циљу ефикаснијег одређивања броја монотоних стања.



S_2	G_2^+	G_2^-	$\lvert\operatorname{fix}(G)\rvert$	$C(S_2)$
0000	1	9	9	1
0001	1	2	2	1
0010, 0100	1	2	2	2
0011, 0101	1	1	1	2
0110	1	1	1	1
0111	2	1	2	1
1000	1	4	4	1
1001	1	1	1	1
1010, 1100	2	2	4	2
1011, 1101	2	1	2	2
1110	4	1	4	1
1111	9	1	9	1

скупа монотоних стања графа који одговара партицији $n-2=6$ која је добијена од полазне партиције изостављањем последње две јединице.

4.2 Партиције у којима су последња два сабирка јединице

Нека је $q \in P_n$ партиција која одговара разлагању $n = a_1 + a_2 + \cdots + a_k$, $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_k$, где је $a_{k-1} = a_k = 1$. Нека је $p \in P_{n-2}$ партиција која одговара разлагању $n-2 = a_1 + a_2 + \cdots + a_{k-2}$. Нека је $G_p = (V_p, E_p)$ и $G_q = (V_q, E_q)$. Следећа теорема показује како се може израчунати $\lvert\operatorname{fix}(G_q)\rvert$ ако је познат скуп $\operatorname{fix}(G_p)$.

Теорема 4.2.1. *Нека је*

$$\mu(S) = |T \in \operatorname{fix}(G_p) \mid T \geqslant S|$$

и

$$\eta(S) = |T \in \operatorname{fix}(G_p) \mid T \leqslant S|.$$

Тада важи

$$|\operatorname{fix}(G_q)| = \sum_{S \in \operatorname{fix}(G_p)} \sum_{T \in \operatorname{fix}(G_p)} \mu(S \vee T)\eta(S \wedge T).$$

Доказ. Пермутација $\sigma = \pi(q)$ када делује на $x = (x_1, x_2, \ldots, x_n) \in B_n$, фиксира елементе x_{n-1} и x_n. Према томе, из $x' = (x'_1, \ldots, x'_n) \in v = \operatorname{orb}(x) \in V_q$ следи $x'_{n-1} =$

x_{n-1} и $x'_n = x_n$. Нека је

$$V_{ij} = \{v \in V_q \mid v = \mathrm{orb}(x), (x_{n-1}, x_n) = (i,j)\}, \quad (i,j) \in B_2.$$

За свако $v \in V_p$ постоје четири чвора $v_{ij} \in V_q$, $(i,j) \in B_2$, таква да ако је $x = (x_1, x_2, \ldots, x_{n-2}) \in v$, онда $x_{ij} := (x_1, x_2, \ldots, x_{n-2}, i, j) \in v_{ij}$. Према томе, V_q се разлаже у дисјунктну унију $V_q = V_{00} \cup V_{01} \cup V_{10} \cup V_{11}$. Сваки подграф G_{ij} графа G_q индукован скупом V_{ij} изоморфан је графу G_p. Између два чвора $u \in V_{pq}$ и $v \in V_{rs}$, $(p,q) \neq (r,s)$, постоји грана ако и само ако:

- $u = w_{pq}$ и $v = w_{rs}$ за неко $w \in V_p$, и
- $(p,q) < (r,s)$ и $|w((p,q) \oplus (r,s))| = 1$.

Нека је S_{ij} вектор чије су компоненте стања чворова из V_{ij}, $(i,j) \in B_2$. Нека је S'_{ij} вектор који се од S_{ij} добија уклањањем последње две компоненте. Четворка $(S_{00}, S_{01}, S_{10}, S_{11})$ једнозначно одговара стању $S \in \mathrm{fix}(G_q)$ (са пермутованим компонентама) ако и само ако:

- $S'_{ij} \in \mathrm{fix}(G_p)$ за свако $(i,j) \in B_2$,
- $S_{11} \geqslant S_{01}$ и $S_{11} \geqslant S_{10}$, и
- $S_{01} \geqslant S_{00}$ и $S_{10} \geqslant S_{00}$.

Последња два услова еквивалентна су редом условима $S_{11} \geqslant S_{01} \vee S_{10}$ и $S_{00} \leqslant S_{01} \wedge S_{10}$. Према томе, скуп могућих четворки $(S_{00}, S_{01}, S_{10}, S_{11})$ добија се на следећи начин:

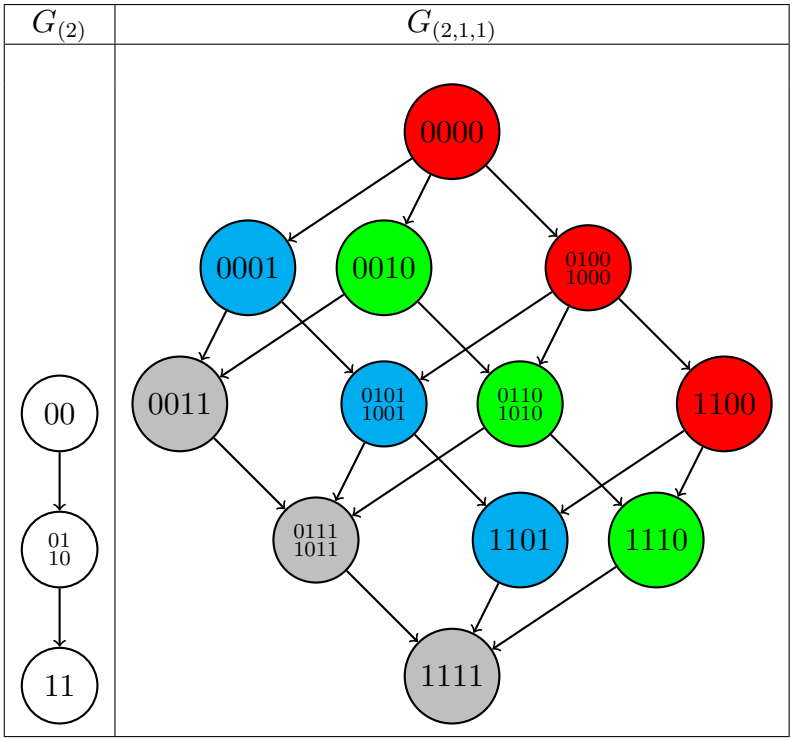
- сваком пару (S_{01}, S_{10}) који одговара пару $(S'_{01}, S'_{10}) \in \mathrm{fix}(G_p) \times \mathrm{fix}(G_p)$ одговарају сви могући парови $(S_{00}, S_{11}) \in \eta(S_{01} \wedge S_{10}) \times \mu(S_{01} \vee S_{10})$.

Величина овог скупа једнака је $|\mathrm{fix}(G_q)| = \sum_{S \in \mathrm{fix}(G_p)} \sum_{T \in \mathrm{fix}(G_p)} \mu(S \vee T)\eta(S \wedge T)$. □

Напомена 4.2.1. *Теорема 4.2.1 представља директно уопштење поступка примењеног за рачунање d_7 [3] и d_8 [40].*

Пример 4.2.1. *Графови $G_{(2)}$ и $G_{(2,1,1)}$ приказани су на слици 4.4. Чворови индукованих подграфова G_{00}, G_{01}, G_{10}, G_{11} обојени су редом сивом, плавом, зеленом и црвеном бојом.*

Слика 4.4: Граф $G_{(2,1,1)}$ састављен од четири подграфа изоморфна са $G_{(2)}$.



Табела 4.2: Рачунање $|\mathrm{fix}(G_{(2,1,1)})|$ из примера 4.2.1.

S' \ T'	000	100	110	111
000	$(1,4)$	$(1,3)$	$(1,2)$	$(1,1)$
100	$(1,3)$	$(2,3)$	$(2,2)$	$(2,1)$
110	$(1,2)$	$(2,2)$	$(3,2)$	$(3,1)$
111	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$

Ако су чворови у овим графовима распоређени одозго на доле, слева на десно, онда је:

$$\mathrm{fix}(G_p) = \{\{0,0,0\},\{0,0,1\},\{0,1,1\},\{1,1,1\}\}$$

У пресеку врсте која представља стање S' графа G_{01} и колоне која представља стање T' графа G_{10}, табела 4.2 приказује парове $(\mu(S' \wedge T'), \eta(S' \vee T'))$. Сума производа ових парова једнака је

$$\sum_{S'} \sum_{T'} \eta(S' \wedge T')\mu(S' \vee T') = 50.$$

Број сабирака у овој суми једнак је $|\operatorname{fix}(G_p)|^2$. Пошто су вредности $|\operatorname{fix}(G_p)|$ за партиције $(2,2,2)$, $(2,2,1,1)$ и $(2,1,1,1,1)$ релативно мале (редом су једнаке 8600, 24302 и 160948), теорема 4.2.1 омогућава ефикасно рачунање $|\operatorname{fix}(G_q)|$ за одговарајуће веће графове. Могуће убрзање овог рачунања постиже се у спољњој петљи, проласком кроз скуп представника класа еквиваленције скупа $\operatorname{fix}(G_p)$. Следеће једноставно убрзање за фактор 2 постиже се коришћењем симетрије због комутативности операција $\wedge$ и $\vee$. Рачунање вредности $|\operatorname{fix}(G_q)|$ је дакле много ефикасније применом теореме 4.2.1 него применом теореме 4.1.2.

Напомена 4.2.2. *Вредност $r_7 = 490013148$ израчуната је готово тренутно комбинованим коришћењем теореме 4.2.1 и теореме 4.1.2.*

Једини преостали проблематичан случај везан је за партицију $p \in P_8$ која одговара разлагању $8 = 2+2+2+2$. У следећем одељку разматра се како се за ову партицију може ефикасно одредити $|\operatorname{fix}(G_p)|$.

4.3 Партиција у којој су сви сабирци двојке

За $n = 2k$, нека је $q \in P_n$ партиција која одговара разлагању $n = 2 + 2 + \cdots + 2$, и нека је $H_n = G_q$. Анализираћемо графове H_n и показати како се одређује $|\operatorname{fix}(H_n)|$ полазећи од $\operatorname{fix}(H_{n-2})$ и $\operatorname{fix}(D_{n-2})$, чиме се решава проблем са последњом преосталом партицијом.

Нека је

$$\sigma_n = \pi(q) = (1\ 2)(3\ 4)\cdots(n-3\ n-2)(n-1\ n) \in S_n.$$

Пермутација σ_n има орбите дужине 1 и 2, па се скуп чворова V_q графа G_q састоји од једноструких и двоструких чворова. Чвор $\{x\}$, $x = (x_1, x_2, \ldots, x_n) \in B_n$, је једноструки ако и само ако $\sigma_n(x) = x$, тј. $x_{2i-1} = x_{2i}$, $1 \leqslant i \leqslant k$. Према томе, у скупу V_q постоји 2^k једноструких чворова. Преосталих $2^{2k} - 2^k$ n-торки груписано је у $(2^{2k} - 2^k)/2$ двоструких чворова $\{x, \sigma_n(x)\}$, $x \in B_n$, $x < \sigma_n(x)$.

Свакој $(n-2)$-торки $x = (x_1, x_2, \ldots, x_{2k-3}, x_{2k-2})$ одговарају четири n-торке

$$x_{ij} = (x_1, x_2, \ldots, x_{2k-3}, x_{2k-2}, i, j), \quad (i,j) \in B_2,$$

добијене проширивањем x паром $(i,j) \in B_2$. Пермутација σ_n садржи циклус $(n-1\ n)$ који делује на овај пар. Нека је V скуп чворова графа H_n и нека су V_{00}, $V_{01,10}$ и V_{11} подскупови графа V који редом садрже n-торке са последња два бита $\{(0,0)\}$, $\{(0,1),(1,0)\}$ и $\{(1,1)\}$. На тај начин, V се разлаже у дисјунктну унију од три подскупа: $V = V_{00} \cup V_{01,10} \cup V_{11}$. Следећа лема описује структуру графа H_n.

Лема 4.3.1. *Нека су G_{00}, $G_{01,10}$ и G_{11} подграфови графа H_n редом индуковани подскуповима чворова V_{00}, $V_{01,10}$ и V_{11}. Тада*

1. *Подграфови G_{00} и G_{11} изоморфни су са графом H_{n-2}.*
2. *Подграф $G_{01,10}$ изоморфан је са графом D_{n-2} (видети напомену 4.1.1).*
3. *Једине гране графа H_n које не припадају подграфовима G_{00}, $G_{01,10}$ и G_{11} су следеће:*
   - *за сваки једноструки чвор $\{x\}$ графа H_{n-2}, $x = \sigma_{n-2}(x)$, постоје три чвора графа H_n: $\{x_{00}\} \in V_{00}$, $\{x_{01}, x_{10}\} \in V_{01,10}$ и $\{x_{11}\} \in V_{11}$, повезана са две гране $(\{x_{00}\}, \{x_{01}, x_{10}\})$, $(\{x_{01}, x_{10}\}, \{x_{11}\})$;*
   - *за сваки двоструки чвор $\{x, y\}$ графа H_{n-2}, такав да је $y := \sigma_{n-2}(x) > x$, постоје четири чвора графа H_n: $\{x_{00}, y_{00}\} \in V_{00}$, $\{x_{01}, y_{10}\}, \{x_{10}, y_{01}\} \in V_{01,10}$ и $\{x_{11}, y_{11}\} \in V_{11}$, повезана са четири гране $(\{x_{00}, y_{00}\}, \{x_{01}, y_{10}\})$, $(\{x_{00}, y_{00}\}, \{x_{10}, y_{01}\})$, $(\{x_{01}, y_{10}\}, \{x_{11}, y_{11}\})$ и $(\{x_{10}, y_{01}\}, \{x_{11}, y_{11}\})$.*

Доказ. 1. Пресликавање $\phi_{ii} : V_{n-2} \mapsto V_{ii}$ дефинисано са $\phi_{ii}(\mathrm{orb}(x)) = \mathrm{orb}(x_{ii})$, $i \in B_1$, представља изоморфизам између H_{n-2} и G_{ii}, с обзиром да у графу H_{n-2} постоји грана између чворова $\mathrm{orb}(x')$ и $\mathrm{orb}(x'')$, $x', x'' \in B_{n-2}$, $x' \neq x''$, ако и само ако у графу G_{ii} постоји грана између $\mathrm{orb}(x'_{ii})$ и $\mathrm{orb}(x''_{ii})$.

2. Пресликавање $\phi_{01} : D_{n-2} \mapsto V_{01,10}$ дефинисано са

$$\phi_{01}(\{x\})) = \mathrm{orb}(x_{01}) = \begin{cases} \{x_{01}, x_{10}\}, & \sigma_{n-2}(x) = x \\ \{x_{01}, (\sigma_{n-2}(x))_{10}\}, & \sigma_{n-2}(x) \neq x \end{cases}$$

представља изоморфизам између D_{n-2} и $G_{01,10}$, с обзиром да у D_{n-2} постоји грана између $\{x'\}$ и $\{x''\}$), $x', x'' \in B_{n-2}$, $x' \neq x''$ ако и само ако постоји грана у $G_{01,10}$ између $\mathrm{orb}(x'_{01})$ и $\mathrm{orb}(x''_{01})$.

3. Разликујемо редом два случаја: када је чвор $\mathrm{orb}(x)$ једноструки односно двоструки.

   случај $\sigma_{n-2}(x) = x$**.** Изоморфизми ϕ_{00}, ϕ_{01} и ϕ_{11} редом пресликавају чвор $\{x\}$ у чворове $\mathrm{orb}(x_{00}) = \{x_{00}\} \in V_{00}$, $\mathrm{orb}(x_{01}) = \{x_{01}, x_{10}\} \in V_{01,10}$ и $\mathrm{orb}(x_{11}) = \{x_{11}\} \in V_{11}$. Претпоставимо да су $(n-2)$-торке x и x' најмање $(n-2)$-торке орбита којима припадају. Тада

   - постоји грана у H_n која повезује $\mathrm{orb}\, x_{00}$ и $\mathrm{orb}\, x'_{01}$ ако и само ако је $x = x'$; тада је та грана $(\{x_{00}\}, \{x_{01}, x_{10}\})$.

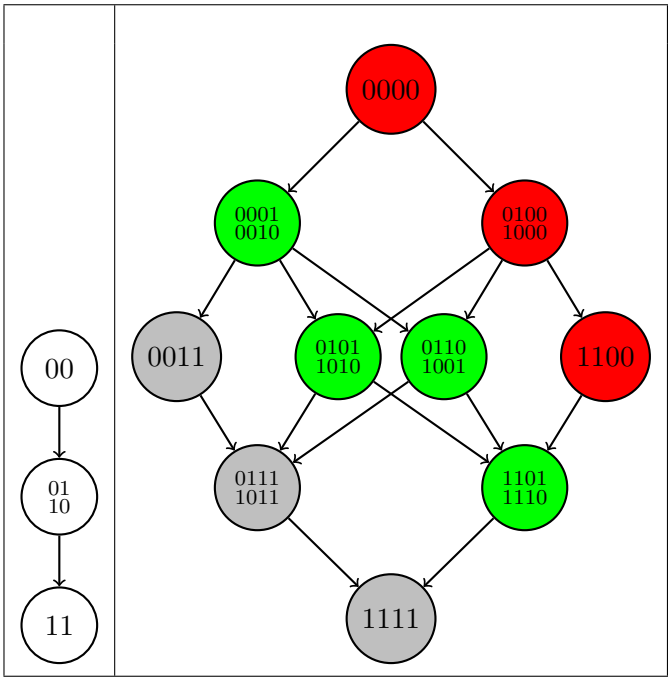
- постоји грана у H_n која повезује $\operatorname{orb} x_{01}$ и $\{x'_{11}\}$ ако и само ако је $x = x'$; тада је та грана $(\{x_{01}, x_{10}\}, \{x_{11}\})$.
- не може постојати грана између $\operatorname{orb}(x_{00})$ и $\{x'_{11}\}$, пошто из $x \leqslant x'$ следи $w(x'_{11}) \geqslant w(x_{00}) + 2$, што је немогуће.

случај $\sigma_{n-2}(x) > x$**.** Чвор $\operatorname{orb}(x) = \{x, y\}$ одговара групи од четири чвора $\operatorname{orb}(x_{00}) = \{x_{00}, y_{00}\} \in V_{00}$, $\operatorname{orb}(x_{01}) = \{x_{01}, y_{10}\} \in V_{01,10}$, $\operatorname{orb}(x_{10}) = \{x_{10}, y_{01}\} \in V_{01,10}$ и $\operatorname{orb}(x_{11}) = \{x_{11}, y_{11}\} \in V_{11}$. Слично претходном случају, закључујемо да ако постоји грана e у H_n између чворова добијених проширењем $\operatorname{orb}(x)$ и $\operatorname{orb}(x')$, тада e може повезати само два чвора из V_{00} и $V_{01,10}$, или два чвора из $V_{01,10}$ и V_{11}. Грана e мора припадати једном од четири типа наведених у формулацији леме.

□

Слика 4.5 илуструје лему 4.3.1 на примеру графова H_2 и H_4. Подграфови индуковани сиво, односно црвено обојеним чворовима изоморфни су са графом H_2. Граф индукован зелено обојеним чворовима изоморфан је са графом D_2.

Слика 4.5: Однос између графова H_2 и H_4.



Следећа теорема приказује могући начин рачунања $|\operatorname{fix}(H_n)|$.

Теорема 4.3.1. *За произвољно $R \in \mathrm{fix}(H_{n-2})$, нека је*

$$\mu(R) = |\{T \in \mathrm{fix}(H_{n-2}) \mid T \geqslant R\}|,$$

$$\eta(R) = |\{T \in \mathrm{fix}(H_{n-2}) \mid T \leqslant R\}|.$$

За свако $S \in \mathrm{fix}(D_{n-2})$ (тј. за сваку монотону Булову функцију од $n-2$ променљиве) нека су вектори $U(S), L(S) \in \mathrm{fix}(H_{n-2})$ дефинисани једнакостима:

$$U(S) = U(\mathrm{orb}(x_{00})) = \begin{cases} S(\{x\}), & \sigma_{n-2}(x) = x \\ S(\{x\}) \wedge S(\{\sigma_{n-2}(x)\}), & \sigma_{n-2}(x) < x \end{cases}, \quad \textit{за свако } x \in B_{n-2}$$

$$L(S) = L(\mathrm{orb}(x_{11})) = \begin{cases} S(\{x\}), & \sigma_{n-2}(x) = x \\ S(\{x\}) \vee S(\{\sigma_{n-2}(x)\}), & \sigma_{n-2}(x) < x \end{cases}, \quad \textit{за свако } x \in B_{n-2}$$

Тада је

$$|\mathrm{fix}(G_q)| = \sum_{S \in \mathrm{fix}(D_{n-2})} \mu(L(S))\eta(U(S)).$$

Доказ. Произвољно монотоно стање графа H_n одређено је монотоним стањима S_{00}, $S_{01,10}$ и S_{11} индукованих подграфова редом G_{00}, $G_{01,10}$ и G_{11}. Нека је $S_{01,10}$ произвољно монотоно стање графа $G_{01,10}$. Тројка $(S_{01,10}, S_{00}, S_{11})$ одговара монотоном стању графа H_n, ако и само ако

- S_{00}, S_{11} су монотона стања графова редом G_{00} и G_{11}, и
- задовољене су неједнакости за гране које повезују ове индуковане подграфове (видети последње тврђење леме 4.3.1).

Пошто су графови $G_{01,10}$ и D_{n-2} изоморфни, ове једнакости важе ако и само ако за свако $x \in B_{n-2}$ важи

$$S_{00}(\mathrm{orb}(x_{00})) \leqslant U(\mathrm{orb}(x_{00})) = \begin{cases} S_{01,10}(\mathrm{orb}(x_{01})), & \sigma(x) = x \\ S_{01,10}(\mathrm{orb}(x_{01})) \wedge S_{01,10}(\mathrm{orb}(x_{10})), & \sigma(x) < x \end{cases}$$

$$S_{11}(\mathrm{orb}(x_{11})) \geqslant L(\mathrm{orb}(x_{11})) = \begin{cases} S_{01,10}(\mathrm{orb}(x_{01})), & \sigma(x) = x \\ S_{01,10}(\mathrm{orb}(x_{01})) \vee S_{01,10}(\mathrm{orb}(x_{10})), & \sigma(x) < x \end{cases}$$

Ако је $S_{01,10} \in \mathrm{fix}(G_{01,10})$ монотоно стање, тада је $U(S_{00})$ горња граница монотоних стања графа G_{00}, а $L(S_{11})$ је доња граница монотоних стања графа G_{11}. Број парова монотоних стања графова G_{00} и G_{11} који задовољава претходне две неједнакости је $\mu(L(S))\eta(U(S))$. Сумирањем по свим монотоним стањима $S_{01,10}$, односно по свим монотоним стањима графа изоморфног са D_{n-2}, добија се израз из теореме. □

Израчунавање на основу доказане теореме може се учинити још ефикаснијим. Ако је ϕ аутоморфизам графа D_{n-2}, нека је $S'(v) = S(\phi(v))$ за све чворове v графа D_{n-2}. Тада важи $\mu(L(S'))\eta(U(S')) = \mu(L(S))\eta(U(S))$. Према томе, сума се ефикасније може израчунати груписањем монотоних стања графа D_{n-2} у класе еквиваленције и обрадом само представника класа еквиваленције.

Пример 4.3.1. *Илустроваћемо теорему 4.3.1 израчунавањем* $|\operatorname{fix}(H_4)|$ *полазећи од* $\operatorname{fix}(H_2)$ *и* $\operatorname{fix}(D_2)$. *Слика 4.5 приказује разлагање графа* H_4 *у подграфове* G_{00}, $G_{01,10}$ *и* G_{11}. *Ако су чворови подграфова поређани одозго на доле, тада је*

$$\operatorname{fix}(G_{00}) = \operatorname{fix}(G_{11}) = \{\{0,0,0\},\{0,0,1\},\{0,1,1\},\{1,1,1\}\}$$

$$\operatorname{fix}(G_{01,10}) = \{\{0,0,0,0\},\{0,0,0,1\},\{0,0,1,1\},\{0,1,0,1\},\{0,1,1,1\},\{1,1,1,1\}\}$$

Вредности $\mu(R)$ *и* $\eta(R)$, $R \in \operatorname{fix}(H_2)$ *приказане су у табели 4.3. Ове вредности искоришћене су за израчунавање* $|\operatorname{fix}(H_4)| = 28$ *(видети табелу 4.4). Два стања обојена истом бојом су еквивалентна, пошто припадају истој орбити аутоморфизама графа* D_2; *према томе, оба стања производе исте векторе* $U(S)$ *и* $V(S)$.

Табела 4.3: Вредности $\mu(R)$, $\eta(R)$, $R \in \operatorname{fix}(H_2)$ из примера 4.3.1.

R	$\mu(R)$	$\eta(R)$
000	4	1
001	3	2
011	2	3
111	1	4

Табела 4.4: Израчунавање $|\operatorname{fix}(H_4)|$.

$S \in \operatorname{fix}(D_2)$	$U(S)$	$L(S)$	$\eta(U(S))$	$\mu(L(S))$	product
0000	000	000	1	4	4
0001	001	001	2	3	6
0011	001	011	2	2	4
0101	001	011	2	2	4
0111	011	011	3	2	6
1111	111	111	4	1	4
					28

Полазећи од $|\operatorname{fix}(D_6)| = 7828354$ монотоних стања графа D_6, резулатат $|\operatorname{fix}(H_8)| = 2038188253420$ добијен је за мање од два часа. Рачунање вредности $|\operatorname{fix}(H_8)|$ помоћу теореме 4.1.2 мање је ефикасно: граф H_8 у средњем слоју има 38 чворова, па је број могућих стања тог слоја прилично велики (2^{38}). Група од 192 аутоморфизма графа H_8 разлаже скуп стања средњег слоја на 1439777920 класа еквиваленције; за сваког представника класе еквиваленције, неопходно је рекурзивном претрагом израчунати број проширења на горе и на доле.

4.4 Израчунавање r_8

Нека m_p означава величину средњег слоја графа G_p, $p \in P_8$. Вредности $|\operatorname{fix}(G_p)|$ за различите партиције одређене су на следећи начин:

- за партиције за које је $|V_p| \leqslant 84$ средњи слој одговарајућег графа G_p има највише 22 чвора, видети табелу 4.5. Ово дозвољава ефикасно рачунање вредности $|\operatorname{fix}(G_p)|$ на основу теореме 4.1.2;
- за осам партиција које имају као сабирке две јединице и за које је $|V_p| > 84$, вредност $|\operatorname{fix}(G_p)|$ израчуната је на основу теореме 4.2.1;
- партицији $(2, 2, 2, 2)$ одговара граф H_8. Вредност $|\operatorname{fix}(H_8)|$ израчуната је на основу теореме 4.3.1;
- партицији $(1, 1, 1, 1, 1, 1, 1, 1)$ одговара граф D_8, па је искоришћена већ позната вредност $|\operatorname{fix}(D_8)| = |\mathcal{D}_8| = d_8$ [40].

Узимајући у обзир вредности $|\operatorname{fix}(G_p)|$ (које су приказане у табели 4.5) на основу леме 4.1.1, добија се $r_8 = 1392195548889993358$. Резултат се поклапа са резултатом Павелског [31], који је користио исту идеју, осим што је уместо партиција посматрао појединачне пермутације. Такође, уместо графова користио је скупове битова, што је убрзало израчунавање r_8. Неколико различитих алгоритама за израчунавање броја фиксних тачака монотоних Булових функција приказани су у раду [39] у коме је такође израчунат број r_8.

Табела 4.5: Израчунавање r_8.

$p \in P$	$\lvert fix(G_p)\rvert$	$g(p)$	$\lvert V_p\rvert$	m_p	a_p
$\{5,3\}$	870	2688	32	6	4
$\{8\}$	2364	5040	36	10	4
$\{7,1\}$	3858	5760	40	10	12
$\{5,2,1\}$	21216	4032	48	10	4
$\{4,3,1\}$	25168	3360	48	10	2
$\{6,2\}$	70096	3360	52	14	4
$\{6,1,1\}$	144320	3360	56	14	4
$\{5,1,1,1\}$	531708	1344	64	14	24
$\{4,4\}$	3211276	1260	70	20	16
$\{3,3,2\}$	3607596	1120	72	18	12
$\{3,2,2,1\}$	16380370	1680	80	18	4
$\{4,2,2\}$	37834164	1260	84	22	16
$\{4,2,1,1\}$	93994196	2520	88	22	8
$\{3,2,1,1,1\}$	401622018	1120	96	22	6
$\{4,1,1,1,1\}$	424234996	420	96	22	48
$\{3,3,1,1\}$	535426780	1120	96	26	24
$\{3,1,1,1,1,1\}$	262808891710	112	128	30	120
$\{2,2,2,2\}$	2038188253420	105	136	38	192
$\{2,2,2,1,1\}$	7377670895900	420	144	38	48
$\{2,2,1,1,1,1\}$	182755441509724	210	160	42	96
$\{2,1,1,1,1,1,1\}$	101627867809333596	28	192	50	720
$\{1,1,1,1,1,1,1,1\}$	56130437228687557907788	1	256	70	40320

4.5 Процена тежине израчунавања r_9

За сваку партицију $p \in P_9$ табела 4.6 приказује величину m_p средњег слоја скупа G_p и величину a_p групе аутоморфизама скупа G_p. Вредност $|\operatorname{fix}(G_p)|$ за $m_p \leqslant 42$ може се израчунати за прихватљиво време на основу теореме 4.1.2.

Размотримо партицију $p = (1, 4, 0, \ldots, 0) \in P_9$ која одговара разлагању $9 = 2+2+2+2+1$. Генерално, ако је n непарно, нека је $p = (1, (n-1)/2, 0, \ldots, 0) \in P_n$ и $H_n = G_p$. Слично као у теореми 4.3.1, може се показати да је $\operatorname{fix}(H_n)$ једнако суми унапред израчунатих израза за скуп $\operatorname{fix}(D_{n-2})$. Пошто је $|\operatorname{fix}(D_7)| = 2414682040998 \sim 2^{41}$, $|\operatorname{fix}(H_9)| = |\operatorname{fix}(G_p)|$ се такође може израчунати за прихватљиво време.

Табела 4.6: Партиције $p \in P_9$ и величине m_p и a_p редом средњег слоја и групе аутоморфизама скупа V_p.

	$p \in P_8$	m_p	a_p
1	{9}	14	6
2	{8,1}	17	4
3	{7,2}	13	12
4	{7,1,1}	18	24
5	{6,3}	23	6
6	{6,2,1}	24	4
7	{6,1,1,1}	25	12
8	{5,4}	9	8
9	{5,3,1}	12	4
10	{5,2,2}	16	16
11	{5,2,1,1}	19	8
12	{5,1,1,1,1}	26	96
13	{4,4,1}	34	16
14	{4,3,2}	18	4
15	{4,3,1,1}	19	4
16	{4,2,2,1}	39	16
17	{4,2,1,1,1}	40	24
18	{4,1,1,1,1,1}	41	240
19	{3,3,3}	42	108
20	{3,3,2,1}	33	12
21	{3,3,1,1,1}	46	72
22	{3,2,2,2}	31	24
23	{3,2,2,1,1}	34	8
24	{3,2,1,1,1,1}	41	24
25	{3,1,1,1,1,1,1}	56	720
26	{2,2,2,2,1}	66	192
27	{2,2,2,1,1,1}	69	144
28	{2,2,1,1,1,1,1}	76	480
29	{2,1,1,1,1,1,1,1}	91	5040
30	{1,1,1,1,1,1,1,1,1}	126	362880

Преосталих 6 партиција за последња два сабирка имају јединице. Да би се израчунала вредност $|\operatorname{fix}(G_p)|$, на основу теореме 4.2.1 потребно је сабрати $|\operatorname{fix}(G_q)|^2$ производа, где је партиција $q \in P_7$ добијена изостављањем последња два сабирка из одговарајуће партиције $p \in P_9$. Табела 4.7 приказује $|\operatorname{fix}(G_q)|$ за ових 6 партиција. Вредности $|\operatorname{fix}(G_p)|$ за прве две партиције могу се израчунати за прихватљиво време на основу теореме 4.2.1. Очигледно, најзахтевнија партиција за рачунање придруже-

на је графу D_9. Уколико би се успешно израчунала вредност $|\operatorname{fix}(D_9)| = d_9$, вероватно би било изводљиво израчунати број фиксних тачака за све партиције из табеле 4.7.

Табела 4.7: Преосталих 6 партиција укључених у израчунавање вредности r_9 у којима су барем два сабирка јединице.

$p \in P_9$	$\lvert fix(G_q)\rvert$	$\log_2(\lvert fix(G_q)\rvert)$
$\{3,3,1,1,1\}$	69264	16.1
$\{3,1,1,1,1,1,1\}$	2068224	21.0
$\{2,2,2,1,1,1\}$	12015832	23.5
$\{2,2,1,1,1,1,1\}$	67922470	26.0
$\{2,1,1,1,1,1,1,1\}$	2208001624	31.0
$\{1,1,1,1,1,1,1,1,1\}$	2414682040998	41.1

Глава 5

Закључак

У овом раду 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.

У поглављу 3 анализиране су Булове и инвертибилне Булове функције, када на улазне променљиве делују четири групе трансформација: група пермутација, група композиције пермутација и комплементирања, линеарна група и афина група. У случају инвертибилних Булових функција иста група трансформација делује и на улазе и на излазе.

Ако се зна циклусни индекс, број Булових, односно инвертибилних Булових функција може се директно израчунати. Међутим, експлицитни изрази за циклусне индексе до сада су били познати за само релативно мале вредности n. Оригинални допринос ове дисертације огледа се у проналажењу алгоритма за добијање експлицитног израза за циклусни индекс за битно веће вредности n за све четири групе трансформација. На основу тога добијени су и одговарајући бројеви класа еквиваленције. Специјално, у случају групе пермутација, приказан је поступак рачунања броја класа еквиваленције без претходног рачунања циклусног индекса.

У поглављу 4 решава се проблем проналажења броја класа еквиваленције монотоних Булових функција. Приказан је поступак на основу кога су (паралелно и независно од [31]) ефикасно израчунати бројеви за $n \leqslant 8$, што такође представља оригинални допринос ове дисертације.

Резултати изложени у овој дисертацији везани за Булове и инвертибилне Булове функције објављени су у радовима:

M. Živković and M. Carić, On the Number of Equivalence Classes of Boolean and

Invertible Boolean Functions, *IEEE Transactions on Information Theory*, vol. 67 (2021), 391–407.

M. Carić and M. Živković, 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* Vol. 100, Issue 114 (2016), 95–99.

Резултат везан за монотоне Булове функције објављен је у раду

M. Carić and M. Živković, „The number of nonequivalent monotone Boolean functions of 8 variables," in *IEEE Transactions on Information Theory*, 2022, doi: 10.1109/TIT.2022.3214973.

Библиографија

[1] J. A. Anderson, *Diskretna matematika sa kombinatorikom*, CET-Računarski fakultet, Prevod drugog izdanja, Beograd, 2005.

[2] L. R. Ashenhurst, *The application of counting techniques*,Technical Report,Bell Laboratories, BL-1 (11), pp. 541-602, 1952.

[3] J. Berman, P. Köhler, *Cardinalities of finite distributive lattices*, Mitt. Math. Sem. Giessen 121, pp. 103–124, 1976.

[4] Y. Borissov, M. H. Lee, S. Nikova, *On the Asymptotic Behavior of the Ratio between the Numbers of Binary Primitive and Irreducible Polynomials*, Serdica J. Computing 2, pp. 239-248, 2008.

[5] N. G. de Bruijn, *Generalization of Pólya's fundamental theorem in enumerative combinatorial analysis*, Konikl. Nederl. Akademie Van Wetenschappen, A 52(2), pp. 56-69, 1959.

[6] N. G. de Bruijn, *Pólya's Theory of Counting*, E.F. Beckenbach (Ed.), Applied Combinatorial Mathematics, Wiley, New York, pp. 144-184, 1964.

[7] M. Carić, M. Živković, *The number of nonequivalent monotone Boolean functions of 8 variables*, in IEEE Transactions on Information Theory, 2022, doi: 10.1109/TIT.2022.3214973, 2022.

[8] M. Carić, M. Živković, *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 Vol. 100, Issue 114, pp. 95-99, 2016.

[9] E. W. Weinstein, *CRC Concise Encyclopedia of Mathematics*, 2nd ed., Chapman & Hall/CRC, 2003.

[10] D. Cvetković, S. Simić, *Kombinatorika i grafovi*, treće izdanje, CET-Računarski fakultet, Beograd, 2006.

[11] D. Cvetković, *Diskretne matematičke strukture, Matematika za kompjuterske nauke*, četvrto izdanje, CET-Računarski fakultet, Beograd, 2004.

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

[13] L. E. Dickson, *History of the theory of numbers, Vol. II: Diophantine analysis*, Dover Publications, 2005.

[14] P. Erdös, J. Lehner, *The distribution of the number of summands in the partitions of a positive integer*, Duke Mathematical Journal, 8(2), pp. 335-345, 1941.

[15] H. Fripertinger, *Cycle Indices of Linear, Affine, and Projective Groups*, Linear Algebra and its Applications Vol. 263, pp. 133-156, 1997.

[16] Gallian, J. A, *Contemporary abstract algebra*, Boston, MA: Brooks/Cole Cengage Learning, 2013.

[17] M. A. Harrison, *Counting theorems and their applications to switching theory*, Chapter 4 in A. Mukhopadyay, ed., Recent Developments in Switching Functions, Academic Press, New York, pp. 85-120, 1971.

[18] X. Hou, *Lectures on Finite Fields*, Grad. Stud. Math., vol. 190, Amer. Math. Soc., Providence, RI, 2018.

[19] V. Jovović, G. Kilibarda, *On the number of Boolean functions in the Post classes F*, Discr. Math. Applic. 9 (6): pp. 593–605, 1999.

[20] C. S. Lorens, *Invertible Boolean functions*, Tech. Rep. 21, Space General Corporation Report, El Monte, California, Research Memorandum, 1962.

[21] C. S. Lorens, *Invertible Boolean functions*, IEEE Trans. Electron. Comput. vol. EC-13, pp. 529-541, 1964.

[22] M. A. Harrison, *The number of transitivity sets of boolean functions*, J. Soc. Ind. Appl. Math. Vol. 11, No. 3, pp. 806-828, 1963.

[23] M. A. Harrison, *On the classification of Boolean functions by the general linear and affine groups*, Journal of the Society for Industrial and Applied Mathematics, Vol. 12, No. 2, pp. 285-299, 1964.

[24] M. A. Harrison, *Counting theorems and their applications to switching theory*, Chapter 4 in A. Mukhopadyay, ed., *Recent Developments in Switching Functions*, Academic Press, New York, pp. 85-120, 1971.

[25] R. A. Horn, C. R. Johnson,*Matrix Analysis*, Cambridge UNiversity Press, 1999

[26] P. D. Lax, *Linear Algebra*, John Wiley & Sons, Inc. New York, QA184.L396, 1996

[27] R. Lidl, H. Niederreiter, *Finite fields*, 2nd Edition, Cambridge University Press, 1997.

[28] L. Chuchang, H. Shoben, *A mechanical algorithm of equivalent classification for free distributive lattices*, in Chinese Journal of Computers, Issue 02 (in Chinese), 1985.

[29] L. Chuchang, H. Shoben, *A note on computation of the numbers of equivalent classes for the free distributive lattices*, in Journal of Wuhan University (Natural Science Edition), Issue 01, pp. 13-17 (in Chinese), 1986.

[30] The On-Line Encyclopedia of Integer Sequences, published electronically at: http://oeis.org, 2010.

[31] B. Pawelski, *On the number of inequivalent monotone Boollean functions of 8 variables*, arXiv:2108.13997v1 [math.CO] 31 Aug 2021.

[32] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen*, Acta Math. 68, pp. 145-253, 1937.

[33] A. E. Primenko, *Equivalence classes of invertible Boolean functions*, Cybernetics 20(6), pp. 771-776, 1984.

[34] J. H. Redfield, *The Theory of Group-Reduced Distributions*, *Amer. J. Math.*, pp. 433-455, 1927.

[35] J. J. Rotman, *Advanced Modern Algebra*, Providence, RI, USA:American Mathematical Soc., vol. 114, 2010.

[36] D. Slepian, *On the number of symmetry types of Boolean functions of n variables*, Canadian journal of mathematics, vol 5, pp. 185-193, 1953.

[37] T. Stephen, T. Yusun, *Counting inequivalent monotone Boolean functions*, Discrete Applied Mathematics 167, pp. 15–24, 2014.

[38] Stinson DR, *Cryptography, theory and practice*, CRC press series on discrete mathematics and its applications, 2nd edn. Chapman & Hall/CRC, Boca Raton 2002

[39] A.Szepietowski, *Fixes of permutations acting on monotone Boolean functions*, arXiv:2205.03868v1 [math.CO] 8 May 2022.

[40] D. Wiedemann, *A computation of the eighth Dedekind number*, *Order* 8 (1), pp. 5-6, 1991.

[41] Y. Zhang, G. Yang, W.N.N. Hung, J. Zhang, *Computing affine equivalence classes of Boolean functions by group isomorphism*, *IEEE Trans. on Computers*, Vol. 65, no. 12, pp. 3606-3616, 2016.

[42] M. Živković, M. Carić, *On the Number of Equivalence Classes of Boolean and Invertible Boolean Functions*, IEEE Transactions on Information Theory, vol. 67, pp. 391-407, 2021.

[43] M. Živković, *Algoritmi*, prvo izdanje, Matematički fakultet, Beograd, 2000.

Биографија аутора

Марко Царић рођен је 22. маја 1973. године. Завршио је Математичку гимназију у Београду 1991. године. Основне студије Математичког факултета Универзитета у Београду, на смеру Вероватноћа и статистика завршио је 2002. године са просечном оценом 8.36. Магистарске студије на Математичком факултету Универзитета у Београду, на смеру Рачунарство завршио је 2010. године одбраном магистарског рада под насловом „Проналажење колизија код криптографских хеш функција“. Докторске студије на Математичком факултету, студијски програм Информатика уписао је 2015. године. Положио је све испите предвиђене планом и програмом докторских студија са просечном оценом 9.83.

Прилози

Табела 1: $Z_n(S'_n)$

n	$Z_n(S'_n)$
1	f_1^2
2	$\frac{1}{2}\left(f_1^4 + f_1^2 f_2\right)$
3	$\frac{1}{6}\left(f_1^8 + 3f_1^4 f_2^2 + 2f_1^2 f_3^2\right)$
4	$\frac{1}{24}\left(f_1^{16} + 6f_1^8 f_2^4 + 3f_1^4 f_2^6 + 8f_1^4 f_3^4 + 6f_1^2 f_2 f_4^3\right)$
5	$\frac{1}{120}\left(f_1^{32} + 10f_1^{16} f_2^8 + 15f_1^8 f_2^{12} + 20f_1^8 f_3^8 + 30f_1^4 f_2^2 f_4^6 + 20f_1^4 f_2^2 f_3^4 f_6^2 + 24f_1^2 f_5^6\right)$
6	$\frac{1}{720}\left(f_1^{64} + 15f_1^{32} f_2^{16} + 45f_1^{16} f_2^{24} + 40f_1^{16} f_3^{16} + 15f_1^8 f_2^{28} + 90f_1^8 f_2^4 f_4^{12} + 120f_1^8 f_2^4 f_3^8 f_6^4 + 40f_1^4 f_3^{20} f_1^4 + 90f_2^6 f_4^{12} + 144f_1^4 f_5^{12} + 120f_1^2 f_2 f_3^2 f_6^9\right)$
7	$\frac{1}{5040}\left(f_1^{128} + 21f_1^{64} f_2^{32} + 105f_1^{32} f_2^{48} + 70f_1^{32} f_3^{32} + 105f_1^{16} f_2^{56} + 210f_1^{16} f_2^8 f_4^{24} + 420f_1^{16} f_2^8 f_3^{16} f_6^8 + 280f_1^8 f_3^{40} + 630f_1^8 f_2^{12} f_4^{24} + 504f_1^8 f_5^{24} + 210f_1^8 f_2^{12} f_3^8 f_6^{12} + 840f_1^4 f_2^2 f_3^4 f_6^{18} + 504f_1^4 f_2^2 f_5^{12} f_{10}^6 + 420f_1^4 f_2^2 f_3^4 f_4^6 f_6^2 f_{12}^6 + 720f_1^2 f_7^{18}\right)$
8	$\frac{1}{40320}\left(f_1^{256} + 28f_1^{128} f_2^{64} + 210f_1^{64} f_2^{96} + 112f_1^{64} f_3^{64} + 420f_1^{32} f_2^{112} + 420f_1^{32} f_2^{16} f_4^{48} + 1120f_1^{32} f_2^{16} f_3^{32} f_6^{16} + 105f_1^{16} f_2^{120} + 1120f_1^{16} f_3^{80} + 2520f_1^{16} f_2^{24} f_4^{48} + 1344f_1^{16} f_5^{48} + 1680f_1^{16} f_2^{24} f_3^{16} f_6^{24} + 1260f_1^8 f_2^{28} f_4^{48} + 3360f_1^8 f_2^4 f_3^8 f_6^{36} + 1120f_1^8 f_2^4 f_3^{40} f_6^{20} + 4032f_1^8 f_2^4 f_5^{24} f_{10}^{12} + 3360f_1^8 f_2^4 f_3^8 f_4^{12} f_6^4 f_{12}^{12} + 1260f_1^4 f_2^6 f_4^{60} + 3360f_1^4 f_2^6 f_3^4 f_6^{38} + 5760f_1^4 f_7^{36} + 2688f_1^4 f_3^4 f_5^{12} f_{15}^{12} + 5040f_1^2 f_2 f_4^3 f_8^{30}\right)$
9	$\frac{1}{362880}\left(f_1^{512} + 36f_1^{256} f_2^{128} + 378f_1^{128} f_2^{192} + 168f_1^{128} f_3^{128} + 1260f_1^{64} f_2^{224} + 756f_1^{64} f_2^{32} f_4^{96} + 2520f_1^{64} f_2^{32} f_3^{64} f_6^{32} + 945f_1^{32} f_2^{240} + 3360f_1^{32} f_3^{160} + 7560f_1^{32} f_2^{48} f_4^{96} + 3024f_1^{32} f_5^{96} + 7560f_1^{32} f_2^{48} f_3^{32} f_6^{48} + 11340f_1^{16} f_2^{56} f_4^{96} + 10080f_1^{16} f_2^8 f_3^{16} f_6^{72} + 2520f_1^{16} f_2^{56} f_3^{16} f_6^{56} + 10080f_1^{16} f_2^8 f_3^{80} f_6^{40} + 18144f_1^{16} f_2^8 f_5^{48} f_{10}^{24} + 15120f_1^{16} f_2^8 f_3^{16} f_4^{24} f_6^8 f_{12}^{24} + 2240f_1^8 f_3^{168} + 11340f_1^8 f_2^{12} f_4^{120} + 30240f_1^8 f_2^{12} f_3^8 f_6^{76} + 25920f_1^8 f_7^{72} + 9072f_1^8 f_2^{12} f_5^{24} f_{10}^{36} + 15120f_1^8 f_2^{12} f_3^8 f_4^{24} f_6^{12} f_{12}^{24} + 24192f_1^8 f_3^8 f_5^{24} f_{15}^{24} + 20160f_1^4 f_2^2 f_3^{20} f_6^{74} + 45360f_1^4 f_2^2 f_4^6 f_8^{60} + 25920f_1^4 f_2^2 f_7^{36} f_{14}^{18} + 18144f_1^4 f_2^2 f_4^6 f_5^{12} f_{10}^6 f_{20}^{18} + 40320f_1^2 f_3^2 f_9^{56}\right)$
10	$\frac{1}{3628800}\left(f_1^{1024} + 45f_1^{512} f_2^{256} + 630f_1^{256} f_2^{384} + 240f_1^{256} f_3^{256} + 3150f_1^{128} f_2^{448} + 1260f_1^{128} f_2^{64} f_4^{192} + 5040f_1^{128} f_2^{64} f_3^{128} f_6^{64} + 4725f_1^{64} f_2^{480} + 8400f_1^{64} f_3^{320} + 18900f_1^{64} f_2^{96} f_4^{192} + 6048f_1^{64} f_5^{192} + 25200f_1^{64} f_2^{96} f_3^{64} f_6^{96} + 945f_1^{32} f_2^{496} + 56700f_1^{32} f_2^{112} f_4^{192} + 25200f_1^{32} f_2^{16} f_3^{32} f_6^{144} + 25200f_1^{32} f_2^{112} f_3^{32} f_6^{112} + 50400f_1^{32} f_2^{16} f_3^{160} f_6^{80} + 60480f_1^{32} f_2^{16} f_5^{96} f_{10}^{48} + 50400f_1^{32} f_2^{16} f_3^{32} f_4^{48} f_6^{16} f_{12}^{48} + 22400f_1^{16} f_3^{336} + 56700f_1^{16} f_2^{24} f_4^{240} + 18900f_1^{16} f_2^{120} f_4^{192} + 151200f_1^{16} f_2^{24} f_3^{16} f_6^{152} + 86400f_1^{16} f_7^{144} + 25200f_1^{16} f_2^{24} f_3^{80} f_6^{120} + 90720f_1^{16} f_2^{24} f_5^{48} f_{10}^{72} + 151200f_1^{16} f_2^{24} f_3^{16} f_4^{48} f_6^{24} f_{12}^{48} + 120960f_1^{16} f_3^{16} f_5^{48} f_{15}^{48} + 56700f_1^8 f_2^{28} f_4^{240} + 75600f_1^8 f_2^{28} f_3^8 f_6^{156} + 201600f_1^8 f_2^4 f_3^{40} f_6^{148} + 226800f_1^8 f_2^4 f_4^{12} f_8^{120} + 50400f_1^8 f_2^4 f_3^4 f_6^{12} f_{12}^{60} + 259200f_1^8 f_2^4 f_7^{72} f_{14}^{36} + 181440f_1^8 f_2^4 f_4^{12} f_5^{24} f_{10}^{12} f_{20}^{36} + 120960f_1^8 f_2^4 f_3^8 f_5^{24} f_6^4 f_{10}^{12} f_{15}^{24} f_{30}^{12} + 72576f_1^4 f_5^{204} + 226800f_1^4 f_2^6 f_4^{12} f_8^{120} + 403200f_1^4 f_3^4 f_9^{112} + 151200f_1^4 f_2^6 f_3^4 f_4^{12} f_6^{38} f_{12}^{60} + 172800f_1^4 f_3^4 f_7^{36} f_{21}^{36} + 362880f_1^2 f_2 f_5^6 f_{10}^{99}\right)$

Табела 2: $U_n(S'_n)$

n	$U_n(S'_n)$
1	4
2	12
3	80
4	3984
5	37333248
6	25626412338274304
7	675163429731859743281756900876615 68
8	28718276100524850099040137377589208476698098298976367465294111 52822140928
9	36948324321931760084804963068248032762615294432491718006429150 09791576440497577843422364150646385515592057329361947025589086393 803097273611247288320
10	49539603584168758480194697717951519334710564895896896294485802 78817589170127062016282573005524945990357719535241976068287537012 2162752698710461662660934059888660169186367283516790360554283709 73173355364551517732389570098778743078711676854923840445599961007 93240808456013220403927177138879503391019499 52

n	број цифара	првих 10 цифара	последњих 10 цифара
10	302	4953960358	9101949952
11	609	8096091387	9988921344
12	1225	2180345287	1455334400
13	2457	1751637212	7853867008
14	4922	1364710731	8023431168
15	9853	1082426226	2274886656
16	19715	9575825887	9021408256
17	39443	1128556104	2152309760
18	78898	2516762987	3845659648
19	157810	2134381540	5071135744
20	315635	2770822705	7817590784
21	631286	8894525773	5920624640
22	1262591	1837243952	4797814784
23	2525201	1649576304	2207606784
24	5050422	2931082251	7359756288
25	10100866	2132169236	6736451584
26	20201755	2712162313	3467180032
27	40403535	1098718953	7726454784
28	80807095	4694593494	9141382144
29	161614218	2317068161	977035264
30	323228465	1582323159	8609016832
31	646456960	2142341745	1894662144
32	1292913952	1179367868	4055357440
33	2585827937	1109063442	6609006592

Табела 3: $U_n(G_n)$

n	$U_n(G_n)$
1	3
2	6
3	22
4	402
5	1228158
6	400507806843728
7	52747143205765300401727403072 5792
8	11218076601767519586965281984173341005925142853855481024470471657123840
9	72164695941272968915634693492671938997117624255160085872467227965434796621908173076713086669511137012532701111814714310142634744787330002626912256
10	48378519125164803203315134490187030600303286031149312787583791785328019239540891229811987263397524710917730613279530479674889403590218084017915411587209217942141146793017943332876520130184925618515382516448167702195222923978525740245378908630676179330029928029851949150824420513845475723945124560896

n	број цифара	првих 10 цифара	последњих 10 цифара
10	299	4837851912	5124560896
11	606	3953169623	5342686208
12	1221	5323108612	750578688
13	2453	2138229019	1343455232
14	4917	8329533272	4552316928
15	9848	3303302691	3095042048
16	19711	1461155073	2680714240
17	39437	8610199770	5539312640
18	78892	9600688886	305708032
19	157804	4071009712	7233422336
20	315629	2642462449	5842946048
21	631280	4241240393	7344691200
22	1262584	4380330926	7257129984
23	2525194	1966448193	742640640
24	5050415	1747061164	9936671744
25	10100858	6354359498	8437796864
26	20201747	4041436781	9259187200
27	40403526	8186094118	4533050368
28	80807087	1748872360	3056640000
29	161614209	4315875770	9895513088
30	323228456	1473653279	5694676992
31	646456950	9976056151	5984594944
32	1292913942	2745929800	2205485056

Табела 4: $U_n(\mathrm{GL}_n)$

n	$U_n(\mathrm{GL}_n)$
1	4
2	8
3	20
4	92
5	2744
6	950998216
7	2076795963681989019155896
8	216512170075309461756067687622554211596928456405221697796 16
9	191646255185337958276617411086954001801914056155896384831129555049566838350922731598983647558266842305063557950356166083563022288 32
10	490583031681057712802385964184337722935202951986879226362999223701293422774643359126449205510752879532323128230123441456130314489524693644509400515146782406559276357130984160509363119708042014060756590172463568353089610932023748669112007835883389590192684939351717155567658637040

n	број цифара	првих 10 цифара	последњих 10 цифара
10	279	4905830316	7658637040
11	581	4207365905	6572193664
12	1191	1621278206	9330775296
13	2416	5046879208	2793767272
14	4874	4101701154	4104127792
15	9797	9089842394	9140513216
16	19652	5991437479	68327744
17	39371	1397463015	8191174216
18	78817	1632615069	1255183584
19	157719	1914071374	8381355576
20	315533	9039728539	3320916320
21	631174	2771144219	127424288
22	1262467	1431647594	3849171584
23	2525064	8402718102	5818113536
24	5050273	2546108234	2336345472
25	10100703	8225091972	2961040320
26	20201579	1208031732	9812269296
27	40403344	1466976913	9423820352
28	80806889	4871278129	9770368640
29	161613996	4838068238	9015843840
30	323228227	1719411692	1467008448
31	646456705	3129719385	8924464888

Табела 5: $U_n(\mathrm{AGL}(n))$

n	$U_n(\mathrm{AGL}(n))$
1	3
2	5
3	10
4	32
5	382
6	15768919
7	16224999167506438730294
8	845750664356679069781095560310816167041836398101030151 18
9	37430909215886319975901838102920717810428460679428092304280082579018500064631097026597863697259931801933484260185559925420090026
10	47908499187603292265858004314876730755390913279968674449511642939579436034123162518369322883615259300043087073397364756587432595352994037781113003857592676537237044775962710960690298997198405370570217712314109935763875520593037300308736448393009590287767878962772505462573563 6

n	број цифара	првих 10 цифара	последњих 10 цифара
10	276	4790849918	4625735636
11	578	2054377883	2319137590
12	1187	3958198745	4399802540
13	2412	6160741221	9267197860
14	4870	2503479708	8164662120
15	9793	2773999754	4318369670
16	19647	9142208068	7797494578
17	39366	1066179669	1556775942
18	78811	6227932240	2843918576
19	157713	3650801419	2921525334
20	315527	8620956935	5464109194
21	631168	1321384534	6380185388
22	1262460	3413313853	2376167938
23	2525058	1001682055	9442791822
24	5050266	1517598769	3850662760
25	10100696	2451268426	5174999328
26	20201571	1800107556	9459030448
27	40403336	1092982972	2205058216
28	80806881	1814692515	1922641604
29	161613987	9011604335	7273576092
30	323228218	1601326923	6000148420
31	646456696	1457389158	792141128

Табела 6: $V_n(S'_n)$

n	$V_n(S'_n)$
1	2
2	7
3	1172
4	36325278240
5	1827297478706355168798634830633 6
6	2447664586919061807550798405385060995056953516804366382059507218 4452353976388161536 0
7	1518095247396149934396561893437671802632484211979653211919046057 2419587843882495858528287600864911303830870768143309448109933903 4671518287392649956419149356667671350869456395141802513832187897 09596490606182400
8	5276597828377707101367890406517408260932514587414557669716521611 6877815555488359331784236239083574487580007591939126392761504001 8821216278774202023997397079366824661489931236149172145693732111 5003924305620092278668775086984681215549370125014517000731969158 5121394921465596217271765454069675365920014984558985618461211811 0722871947349006968239825032973991355317680321485829624176524898 6666164958696461300204071805602521076844115062550144859238782331 0658677339242863017557115060510166825933209600000 0
9	2640674186057734420991930928315688562870683196704918129080678559 5207919579157820374379500499800694343931935665638585660056771001 4711080138640649077160404172738505092500185193919142842736546598 0322259719527963963017018081392784395765197637618931124840513448 6464649524304424873096846336593869765529329153737879398307495299 0710361271944889122793368550058901512007397664533157286038662914 5652477807342113170881758146654835228711419604133228326470608445 5234725637339730861912511010904750121966886667998077807262166444 0855318152480776920392080852178579766887332338861885660254769972 1455950314400375882402318803277582933395768107346528702683280953 7781813786493896438530257922744141156357711162050661213209508862 6377113807622856129578420710344181832189204911264827583469568519 1676343780054159603877237634095410762777710784700411489926524851 7156168427686364450408622817282651956321382848649241836424750480 0661684726454045647372343309018751738150295146135226912754254972 7818772970022094457947312392115780436373203535202115844856315831 5772461447566153105732547034758874469385351519604787474193765667 3533964435465856256595927257366771432995467331495494942720000000 0000

Табела 7: $V_n(S'_n)$

n	$V_n(S'_n)$
10	411486242717575703640311689249502074144033119524897527938576669708300506654419501101370925002140202102004327518019805123590319616308760643301053643813406392723013201132049474654101188657366316842534489433699814655244296367661215597272061411575755133739689937603117768307359430884521242453456737396721543257726885738355882086043468864617831742495088112740700976780544733195167479947979307875344243919239486769674453220722034115594597721739865337136237232783745420048750076111003601327760166716652578266312925695957985735932899033358268465284380745581260937896911887315110465112785903628861850883646675456918983583655625858804644657126572525445637193897990261076289247605361750450938338120766451941245252001615693023258665070332103651076049264733501306953990544489792590785820324491608092053258963848975184482590321344478473532287417963054582666748503388045375586768796070863798041382502674236319426998458650717310763059955050368757276842987668538199896854809516619463696269143712873828074001146716668504617947900740822894745030529159221154135394675585100351157409547201738482090467997875494460464765446092319066817060516128579067113337441468485180584907216968019768900698958877593342406794924197943951579010270191978966931499988973595689593747444388857062749796425830622274906852411582898262949657275396550622260618431854210038569349817738354121826890975792554794018656659796296250712064246315620742327926148825028762766743365650014809054201316266511388877503629926960911969786503745518786861578970235125137408690379262186156110714832300113958445183361374895632952690860641622286311917091306780069135499307279658448726785600455689160784484471650981630136565045966782147211872523856176542583971931416023858009730253327386131651452642173740152240272684868870599113717182049459964912316075149288802031652492429620300823224143314076188802646669853253640575491566421167188259994340189394572224154589626967831441692510738988330443680292020479240146825251887668367979702503569068843641159620820397373369799464025506435049357338176155307968790633312001740333596273691100324926270516313830938856364146071849466685974848897306405833193127053992949352770131510141135742769362726115431043965745590513617382826047830895084018180946874232261294584032580841321970605203105406703847520649548051551813987155037894881221627765013430288386383287918951248777886889821774615973144091842502974647494925936029520010543236335987133680627205969617198068622587490537423659076913674873847016348543343662543503828285738943292779612409859348157250312089166814466692251476009988715574519214469782439384026366251352331259571195152879258173440000000000000000000

n	број цифара	првих 10 цифара	последњих 10 цифара
10	2627	4114862427	0000000000
11	5880	1049795063	0000000000
12	13003	1587646520	0000000000
13	28484	3290418747	0000000000
14	61915	1588471133	0000000000
15	133710	5317439265	0000000000
16	287168	1179393167	0000000000
17	613813	1863951032	0000000000
18	1306562	3406544315	0000000000
19	2770976	3769853709	0000000000
20	5857633	2761541679	0000000000
21	12346602	2562746290	0000000000
22	25955848	2849687196	0000000000
23	54436954	2278420247	0000000000
24	113924391	2133771053	0000000000
25	237949713	1277495638	0000000000
26	496101249	6187971910	0000000000
27	1032606106	7039012220	0000000000

Табела 8: $V_n(G_n)$

n	$V_n(G_n)$
1	1
2	2
3	52
4	142090700
5	178447019405011236406818161 60
6	597574362040786574109081641939713303967095726938163536107580850746762438460938 24
7	926571806272064168943214046287641481098928352038362556102933384547093984611969197220897447550494268961409449462152528285776005071532226159798384649365038150756391193832099360403268370959565678719148097536
8	805144932308610092371809449236665078877641996370629527239459474439663933646978139217899112534844581414489861937547704967674316434968896909750674475093684508311194857009782770003011248081667377303152594375963613396753440413764510869042243560695412010976497774391620592073150399856015851785960543262317741074012609137608803048625240864588986189385348144718856291494232389720029875144657172444459702631192412195708138265901471221636212591424381668867751183561225505884419679652847943035691991040 0
9	100733725969609619941403615124347250475718810909458851969935552960235288921958238122480394362643029571273558294824926986910900121578628592926272993911897343726541554451059415404946457953089369976892842084044035454445575004302383261306672577626461976643121667727087113588046543490777346015433370702091803504483788709622570308823117044406556241366786979256253054579797566664614119973340822314369481739546745500608872905602019849447438747226375952690488876693783539357701759480647782291039964395744708669893475800432400990216239745396261880087912119195882938262316617897911837367132594223268381533261594772631947239126147008474858354926038520263716831374168604027787907133907985899615037223905721440311702524908024345622534234505330286865940150709724593652713748602596707690303092538274074396044726332939289148821624184476886263691658307625963981480195147194856453723002080853430244164805314969537956278605488965240755299099272178924087823257363679992945822000802372852735879997268793694223090279903732283089286536590721971621105944653426487313338163726963597870590492929414028748555049836560247778934457087945212304624691556104836461895405799053721600 0

Табела 9: $V_n(G_n)$

n	$V_n(G_n)$
	39242386123426027645140808987570006765750228836526634973390261622266817727510404691826908588613529405785019637872677337988883935576320709543328632718411101600934333909230182137880438676582938846829842513437253442310742985502358970381933346898627770780533784637748505430923407638980983968110727061912683797619522641978824814419123541318686651467808543466634843519262765235440013880536967074903892890857647587745137521812632953223666927503572972978233073742660279674576520992384914017989883581844952181116402555157411820754364958127577480938762481170475587252587431786681275035026415859497660168491808657235326610409313448513075300761476254705864307345371153460276501155904405121335395222861923713123753089920193605644785547927208935271034710547766697949924378819368291766985133404651719017536725653161765904260543073124680266688226871138139559428677591209844356410682640751493435300660310827363158680629151399980423301618256523629291723581788683607419243486496762582043190931557404232545400854855387898830531581738825117029368459321343252952964878843059890387397909734346393967342101539999443976749344203077178423096905071515241545895822126901348381723615200176917297759688319790286445350928781708215536780816145626744832135954567099776602945792783477187875512160831616833092338571042874883992772527691845850015373528546852504756730197085360494676042363386074826527516293871289917394576565950032779028880650322352093874206804821059299029873392907810525941980231297974722172788040488342156479800702763457829933941208169233329268504643944433500892107687733513569865924727460593783211212865735136576824882170308337865744257553926724217943777784011056538670994788391783229258552950322193861433533433518560208278322990384347141951966794416360077184262994039393895610031367101669401233232649866743495874218859454180115574220440684790103827973166255689781548586488851811894175243427520090807262605690213950872092041656106080115420419812041147649181177422739715314840044883401165152438143765509793302900563952405137576719066726183857786665293528328091732955294366440843019060684725499978910114535510102758780781854765226318389672286194226490285851787255454072968164694839485851930632103764518670791834254611816931557919535411085897467778303616817154408272708298059328018517218584610237917794670047176539259396771709450142031497860494594522905981411980616266351851240281842218956956341748901869248722444348489277382915149643982073844588583662328053260005818498712428149436914324152731491412644569133566287133272239802806184433609754199361395291320776652265537925573291712347088083535527172319326673279295362048195811820437504000000

n	број цифара	првих 10 цифара	последњих 10 цифара
10	2621	3924238612	7504000000
11	5873	2502906472	6800000000
12	12995	9463110690	0000000000
13	28476	4903106015	0000000000
14	61906	5917516104	0000000000
15	133701	4952251226	0000000000
16	287158	2745988702	0000000000
17	613803	1084962296	0000000000
18	1306551	4957174409	0000000000
19	2770965	1371464790	0000000000
20	5857621	2511607525	0000000000
21	12346589	5827010433	0000000000
22	25955835	1619859629	0000000000
23	54436940	3237829912	0000000000
24	113924376	7580677610	0000000000
25	237949698	1134644057	0000000000
26	496101234	1374005778	0000000000
27	1032606090	3907436718	0000000000

Табела 10: $V_n(\mathrm{GL}_n)$

n	$V_n(\mathrm{GL}_n)$
1	2
2	2
3	10
4	52246
5	2631645209645100680144
6	3122420813859255942865111133846073604322601781283387320137132349 78712
7	1436373021963471088286228730014233953881153604941874111297310947 9380501248438614858055780777590843369729785783414473254052215660 1147682663346499784772168400980116274561463153898384620708 16
8	2999175551333938142449818345504089591339094361041780135109042435 2005935408570677281944779101252802445753936764533667633524010565 3562322784650797285198597633256714777503750173888398351210460811 4229039259930644681454151047771319290933667105204996976945379120 0180218494467009568116632390326013876296881683901560415329357329 5850802688677280174858834736056999735792939052276519396778444591 2989987739676323835462154760069036663343180949867919951897604292 0305003099624933468656
9	7104377018952410667814205621135656611953807712475317870702472173 5463313779082238537930282423791422098865305312425607614214836916 2514356896535038902120049684933593659424958357822840996725381419 2108600819683134717999507645294401725200098423275976849263195978 7053935391456111219583850951853095623638424601537024254343840901 8520353879210238808543854687323050504170144249214715551724721421 2490029541083315340922105275127528600315569075312038173210181641 2165165809512047781462891221267260551131403503250548741299176179 5807977230974897594087075169172237888977847849897397215039948188 1118452635585031605336506118870139931827732156937370094617453517 8947738815342755828523187256336357471379175830203200753588975503 4664799421304898247505406849956446445223367044013221381845864302 9471745951545847250936169642343869725401009559434421462848365911 2315322927610865492310388319184618156714877162704356241471596257 0666005631101843286900725074465997052535257338149139011299578185 8217340167008391915650694407078259439309697513557626149194227822 5960589546236304345856147989782218871216027934053466075619086067 3248283724362278792163545448244

Табела 11: $V_n(\mathrm{GL}_n)$

n	$V_n(\mathrm{GL}_n)$
	40352952047240754580173204304575391258384744657990676316341346
	85939372552339999943803548698647347436783191606705466470226022 83
	15061918090261520422971648592464234979336054508709462701702608 87
	62157045315797813551772204396033576720110935121661751762738236 98
	70004466854709626826909878995261637329631438332804479573686576 52
	22734569868523589661991709111710037910721807405999504358676839 87
	49780898137996357859971849408350862630536639905498399986756537 25
	94695770935052490811222909859552213096878848786765666544634992 93
	15111118112323278343701228896982689470081143327038344470843346 31
	32532999400104490124335710567426693131495534140531484505296608 29
	69243613495024891447047977135018048112209779777183183432732944 63
	65162875197818997062126756006445916557796670910311915750994383 21
	95291294764337672759874581762175024937170827631449865634782850 44
	78246343622905981494594693326909174660647981340759995016010572 92
	12725757751713668864635595462657030616673787644694747208766333 02
	95625643507223116517533016387577263433942878576045577402157632 09
	15151141332587504055479525726966608873301092559382979900963084 33
	30764422076639677028127947165015990552696294985943309926408761 90
	91147442439712721692205025471542006269894656458283374528520827 96
	06416115961751870535149231561054253760020012456618679935359239 38
10	05862612665073253080040582216431658791717508904203250349016948 04
	43728802339363403697160968921065318583158372142843846374067437 65
	88164411744353945825010690247325001323678656723857024473485879 41
	52881803144226522761920965103265270030290329185563063397383206 42
	25917128563114827644877020081316134606269231219230883457671135 74
	29866977987693595939771227540265227270617259442225282134858501 24
	55415239857456977701514559943861595436351704597818049727727176 13
	29937527990944469262906519917580517259955073832569004056007205 47
	82057132024102757390195184845295633999742043539420993121581038 17
	47179451017694739970546614347817510803573619923150577900243905 54
	99075997950487102326044178315648017443497145505665743068430848 31
	25843629016185601866783881144017913543229293785056875519787852 74
	17153995051474368102438009547492926081588070383319777877865384 21
	05695267117122918632339410709063860801515754041689947495575685 40
	74976880846822979253434834616464793653619148930686294950448138 24
	33636718896131036432603092960672894683218840773808319570264794 42
	16256282639580197943369254188121728510208876842633815035696764 06
	70955717147431088913227720576777460329031553894021267947055584 75
	19240652714036218411739406980719535372642482551626342662904398 81
	67362712012881184455526772887947462082458999766585787055938926 20
	0147794436580815474552

n	број цифара	првих 10 цифара	последњих 10 цифара
10	2581	4035295204	556274552
11	5823	2835138562	1711309456
12	12934	8778460400	2514365872
13	28403	2731546928	5468862764
14	61820	1434914895	5093195336
15	133600	3749890897	8800780244
16	287041	4617088394	7968498528
17	613669	2858043513	4986107452
18	1306400	1433497724	9474881392
19	2770794	3031772726	6324155232
20	5857430	2939306698	6366481984
21	12346377	2487586979	5154199188
22	25955600	1730357318	6353803904
23	54436681	5911920703	2908073808
24	113924093	1610072865	3548122880
25	237949388	1901067799	0713797456
26	496100897	1227647445	9349521944

Табела 12: $V_n(AGL_n)$

n	$V_n(AGL_n)$
1	1
2	1
3	4
4	302
5	2569966041123963092
6	7623097690086074079260525229364625238314362739096568515312475786 4
7	8766925182882513966590751525965783409919150420787805855086126391 2234504696438118649313555277121383225892125476929696389550785555 3188386908204901473878725895316404384316228470586133104
8	4576378709921170261306485512548964830534506776491974083113162895 5087181714737971926795622407917484200674341986898296559942643074 5792118506852412849729305470667594570165634422121146541561779731 3916484570994726010389819287752020161919094244475332436922760187 3447213962999125312178273355492317285644454540295371746399879033 8005413615981738509216600422072967645280863434558442606389215899 9987690212024912463050778962678230286830044851161778968014665909 34522276904039712
9	2710104758816684977651293037847769398480914196958663128167141789 8354840766556640067264664620892113532587167859049075170217451826 5729658850301757393692035554860532249231322615746628187837746207 8898849799988988768768122728460083665924109811125174274163511649 5915960461218304145654240017644155740218515244116601659524475441 6854993392643065951745550036362858010929162692724119396867645805 8353435341339286867773118678062544311481240574644814686407902408 4270156142338423438262793302288679450645364501905751323676206917 1610588993579350020118298089460045569033453841242296619948614221 7294689175540989072931481974367030726607010312274516125162050510 7771249505860349434668960370694169809491963580864959023135510093 7897077688479091345056885561368337574922773746310253321096589609 4653562630038741637342145511762990069068720128277040317918117827 0297392708082184542696924136177354499912062787082402416950233530 6004526298922866053993599472258705810064135461178303618784837419 6807764365146810829301972475916580632995130813937183626576119780 4168381173843020485581429782258064328979166734993368978867958637 9007969738246901078252482 0

Табела 13: $V_n(AGL_n)$

n	$V_n(AGL_n)$
	384835739586265130807621043248895561775062033252627146876729456767457700274848937452350127207253908508140483920149483396778324427663724985372085974666260330642924289070181378087485028936966778007225543575078349282474937060697242747396003881621528886626909923596066042991894024943151428810475632013686492962642418733372902709695690654363309852322684965169821473891645431045874287452578523721517371784006116089764437757742932952871847000120807317472407300671911740215408543680758974200218952644221932092138624123873816602814029005378438214203818025083619254424131721945613237679723071994791459095414706284277600587033799566319607210664425687496601233434914507360915919637852173921678350231010279013947912564432978818720814764143711096235195691868468199073711157793410510567788578447119976031740356652739042012293589730249942281994862348998485783634009309718068379489657026748479298293448987122655663458782509875017616412514395925285737490934424820710553829706779178223333655073347923008815912866551781497489658640082946670454316822780214687718511868616740119846179250763353135167622809963749279772407313792054274726788724294485966554804169148717956399421664591558972718690844385625370835804330285956860796093400051931834845348959616170198176818552538027641882491250407380379343655276342825169977487328116322372379443765115238561739379005720840347781089156814710554446247174676185666894637120622831561900113736128483311444993097008183432345133394399729437132982793750232325997345648658668639574487043371877637585757182282628260755207943648796114892443330895611353431010944632145592270009367666764557916223911276694889869809540672764492564459884825210055774762146441921373619450530955880519853665445735531979424146029385693804264117507425500335446184324761087991715693688626379532934360176885654854002471281642518116996844940513002449482021763491512696635401315898440497320662694944910212533912744425504844482225289445427335492893684934381982990077871919730206178649628272465351058989106233901591063296754625338744432997610866576503484422122293337497013515715451160070465597071884645675510572737935691389770070592943321674670240832634955445089978019069343694928517649259314082168343960374284236620886997429678470858248812684128224326716607038002697399916623366584577723887981790333508309048230333443464644938620151264320023052211994800435974944905568418613554160908742313752067063025714773283046921340102959705161095999874812794250917157918849561395683427627623490246002174677796536628860790308725555650072217794086373472528955254186360148424362708468417613049936727723023469901950373013096

n	број цифара	првих 10 цифара	последњих 10 цифара
10	2575	3848357395	5373013096
11	5816	6759497076	1388898128
12	12927	5232370138	6510709872
13	28395	4070322109	2019236076
14	61811	5345474538	0337949752
15	133591	3492358045	1887072228
16	287032	1074999662	4654857232
17	613659	1663600276	5129944956
18	1306389	2086013736	6765878752
19	2770783	1102952492	6608829104
20	5857418	2673283869	5968073120
21	12346364	5656117945	8673738084
22	25955586	9835942582	8084733936
23	54436667	8401344620	3990364880
24	113924078	5720127892	6974739456
25	237949373	1688487393	7418378832
26	496100881	2725924920	7259532696

Изворни кôд 5.1: Директно рачунање $U_n(S'_n)$

```
n = 20; (*the value of n is chosen here*)
e = Table[2, {n}];(*the sequence e*)
Do[DD = Divisors[k];
e[[k]] = (2^k - Sum[DD[[j]] e[[DD[[j]]]], {j, 1, Length[DD] -
k, {k, 2, n}]
PP = IntegerPartitions[n];
npp = Length[PP];(*the list of partitions of n*)
(*decompositions of n corresponding to partitions*)
P = Table[0, {i, npp}, {j, n}];
Do[Do[P[[ipp, PP[[ipp, i]]]]++, {i, Length[PP[[ipp]]]}], {ipp,
Un = 0;
Do[(*the main loop through all partitions of n*)PPP = PP[[p]];
np = Length[PPP];
(*current partition*)
divsets = {};
nd = 1; br = 0;
Do[(*k is the index of the current Partition element*)
DD = Divisors[PPP[[k]]];
AppendTo[divsets, DD];
```

```
nd *= Length[DD], {k, 1, np}];
(*divsets is the list of the sets of divisors of cycle lengths
sigma*)
Descartes = Tuples[divsets];
(*nd is the length of Descartes*)
Do[(*loop through Descartes product*)product = Descartes[[id]]
npr = Length[product];
lcm = 1; prx = 1; pry = 1;
Do[lcm = LCM[lcm, product[[ipr]]];
prx *= product[[ipr]];
pry *= e[[product[[ipr]]]], {ipr, npr}];
br += prx*pry/lcm, {id, nd}];
denominatorr = Product[i^P[[p, i]] P[[p, i]]!, {i, n}];
Un += (2^br)/denominatorr,
{p, npp}];
Print[{"U_n=", Un}];
```

Изворни кôд 5.2: Директно рачунање $V_n(S'_n)$

```
n = 20; (* the value of n is chosen here *)
e = Table[2, {n}]; (*the sequence e*)
Do[
DD = Divisors[k];
e[[k]] = (2^k - Sum[DD[[j]] e[[DD[[j]]]], {j, 1, Length[DD] -
k, {k, 2, n}]
PP = IntegerPartitions[n];
npp = Length[PP]; (*the list of partitions of n*)
(*the maximum length of a cycle in sigma'*)
mlcm = Apply[Max, Table[Apply[LCM, PP[[p]]], {p, npp}]];
(*decompositions of n corresponding to partitions*)
P = Table[0, {i, npp}, {j, n}];
Do[Do[P[[ipp, PP[[ipp, i]]]]++, {i, Length[PP[[ipp]]]}], {ipp,
EmptyList = Table[0, {j, mlcm}]; (*used to initialize spec(sig
Vn = 0; Do[(*the main loop through all partitions of n*)
PPP = PP[[p]]; np = Length[PPP]; (*current partition*)
Spec = EmptyList; (*initialization of spec(sigma')*)
divsets = {};
nd = 1;
Do[(*k is the index of the current Partition element*)
```

```
DD = Divisors[PPP[[k]]];
AppendTo[divsets, DD];
nd *= Length[DD], {k, 1, np}];
(*divsets is the list of the sets of divisors of cycle lengths
sigma*)
Descartes = Tuples[divsets]; (* nd is the length of Descartes
Do[ (*loop through Descartes product *)
product = Descartes[[id]];
npr = Length[product];
lcm = 1; prx = 1; pry = 1;
(* Theorem 2 *)
Do[
lcm = LCM[lcm, product[[ipr]]];
prx *= product[[ipr]];
pry *= e[[product[[ipr]]]], {ipr, npr}];
Spec[[lcm]] += prx*pry/lcm, {id, nd}];
(* Theorem 1 *)
numerator = Product[i^Spec[[i]] Spec[[i]]!, {i, Length[Spec]}]
denominatorr = Product[i^P[[p, i]] P[[p, i]]!, {i, n}];
sum = numerator/denominatorr^2;
Vn += sum, {p, npp}]
Print[{"V_n=", Vn}]
```

Прилог 1.

Изјава о ауторству

Потписани-а _____

број индекса _____

Изјављујем

да је докторска дисертација под насловом

_____

_____

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, _____

_____

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора _____

Број индекса _____

Студијски програм _____

Наслов рада _____

Ментор _____

Потписани/а _____

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, _____

_____

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

_____

_____

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, _____

_____