ДИСКРЕТНЕ СТРУКТУРЕ 1

Александра Костић Матијевић **Жарко Мијајловић**

Зоран Петровић **Маја Рославцев**

Издавач: Математички факултет, Београд
Студентски трг 16, 11000 Београд

Аутори: др Александра Костић Матијевић, Математички факултет, Београд
проф. др Жарко Мијајловић, Математички факултет, Београд
проф. др Зоран Петровић, Математички факултет, Београд,
др Маја Рославцев, Математички факултет, Београд

Рецензенти: проф. др Небојша Икодиновић, Математички факултет, Београд
проф. др Зоран Пуцановић, Грађевински факултет, Београд
др Милан Банковић, Математички факултет, Београд

За издавача: проф. др Зоран Ракић, декан

Цртежи и слог: аутори

Дизајн корица: Карим Салим

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

510.3(075.8)
510.63(075.8)
511.1(075.8)

ДИСКРЕТНЕ структуре 1 / Александра Костић Матијевић ... [и др.]; [цртежи аутори]. - Београд : Математички факултет, 2025 (Београд : Донат граф). - 284 стр. : граф. прикази, табеле ; 25cm

Тираж 500. – Библиографија: стр. 284.

ISBN 978-86-7589-201-4

1. Костић Матијевић Александра, 1989- [autor][ilustrator]
a) Теорија скупова b) Математичка логика v) Теорија бројева

COBISS.SR-ID 174096905

Тираж: 500 примерака

Штампа и повез: ДОНАТ ГРАФ ДОО, Београд

© 2025. Аутори.
Сва права задржана. Ниједан део ове публикације не може бити репродукован нити смештен у систем за претраживање или трансмитовање у било ком облику (електронски, механички, фотокопирањем, смањењем или на други начин), без претходне писане дозволе аутора.

С а д р ж а ј

Предговор

Овај уџбеник базиран је на предавањима и вежбама које су аутори више година држали из предмета Дискретне структуре 1 у првом семестру студија смера Информатика на Математичком факултету у Београду. У зависности од тога како се развијала конкретна академска година, пређено је мање или више појмова који се појављују у овом уџбенику. Он је пре свега намењен студентима Информатике на Математичком факултету, али га могу користити и студенти Математике као допунски материјал за курс Увод у математичку логику или за сам увод у теорију бројева.

Књига се састоји од девет основних поглавља, затим поглавља у коме су дата решења свих задатака, као и два додатка.

Прво поглавље је посвећено основним појмовима о скуповима. Наравно, са овим појмовима читаоци су се већ срели у ранијем школовању, те је стога овде учињен покушај да се они мало пажљивије уведу него што је то било у основној и средњој школи. Наведене су аксиоме теорије скупова да би се истакло на шта је важно обратити пажњу, а свакако не зато да би се у овој књизи развијала аксиоматска теорија скупова. Овде посебно скрећемо пажњу на то како је разрешење Раселов парадокс, који нас упозорава на то да не можемо баш сваку колекцију објеката назвати скупом, а истичемо и представљање скупова Веновим дијаграмима, посебно како представити унију четири скупа Веновим дијаграмом, што читаоци вероватно нису имали прилике да виде до сада. Друго поглавље је посвећено релацијама, посебно бинарним релацијама на датом скупу. Ту се бавимо појмом релације еквиваленције, који је свакако познат читаоцима из ранијег школовања, као и појам релације парцијалног, односно делимичног уређења, који је вероватно мање познат. Важно је напоменути да се појам највећег и појам максималног елемента у неком скупу не поклапају у општем случају, баш због тога што се ради о делимичном уре ђењу. Истичемо и појам матрице релације који је посебно важан у информатици. У трећем поглављу се уводи појам функције као специјалан случај релације. Ту је битан и појам домена функције, са којим су се читаоци вероватно срели у средњој школи, ако су тамо испитивали функције користећи основе диференцијалног рачуна. Важно је да читаоци овде упознају појмове инјекције, сурјекције и бијекције, као и инверзне функције. Осим тога, веома је користан појам карактеристичне функције подскупова и њихове примене у доказивању разних скуповних идентитета.

Четврто поглавље, које носи назив „Бројеви" је најдуже у целој књизи, али је од посебног значаја. У почетном делу бави се математичком индукцијом, важним оруђем за доказивање у математици, којој се овде темељније приступа него што је

то случај у средњој школи. Ми у овој књизи уводимо природне бројеве, а дајемо и конструкцију целих бројева на основу природних. Појам дељивости је од централног значаја као и Еуклидов алгоритам који се овде обрађује. Имамо и примере Диофантових једначина, као и решавања конгруенција, уз посебно важну Кинеску теорему о остацима. Примене резултата овог поглавља су дата у другом додатку посвећеном RSA алгоритму у криптографији. Наредно поглавље је краће и оно је посвећено коначним и бесконачним скуповима, посебно пребројивим скуповима.

Шестим поглављем почиње изучавање формалне логике и наравно прво на реду је исказна логика. Ту имамо и појам таутологије, као исказа који је увек тачан, као и контрадикције, исказа који је увек нетачан. Појам таутологије је читаоцима свакако познат из школе, као и метод таблица. Овде показујемо и друге методе, попут метода таблоа и метода разрешења. У рачунарској литератури код нас се уобичајило да се метод разрешења назива метод резолуције, па смо ми најчешће користили тај термин, али је разрешење одличан термин на српском који означава шта заправо радимо. Следеће поглавље се бави формалним системима у којима се формализује појам доказа. Овде нам је главни пример Исказни рачун. Осмо поглавље је посвећено предикатској логици, где се уводе и квантификатори „постоји" и „за све" и која нам омогућава формирање знатно сложенијих теорија. Појам ваљане формуле, тј. формуле која је тачна у свим интерпретацијама, одговара појму таутологије (заправо су неке од ваљаних формула таутологије). Са тим појмом се читаоци нису раније сретали, а имплицитно се појављује у другим математичким курсевима. И овде се разматрају одговарајући методи за доказивање ваљаности формула. Девето поглавље је посвећено Буловим алгебрама. Заправо, Булове алгебре су могле бити уведене и раније, али је ипак одлучено да оне буду представљене на крају. Булове алгебре су наравно од великог значаја у рачунарству и читаоци ће се са њима сигурно сретати у другим курсевима. Овде посебно истичемо метод минимизација буловских израза базиран на Карноовим мапама. Грејови кодови, који су у вези и са овим појмовима, обрађују се у првом додатку.

Важан део књиге чине задаци. Добро је познато да „математика није спорт гледалаца". Задаци су неопходан део сваком математичког курса – неки воле да кажу: „На курсу српског језика пишемо саставе, а на курсу математике решавамо задатке!" У овој књизи, задаци се налазе на крају сваког од основних поглавља, док су њихова решења наведена у посебном, десетом, поглављу. Важно је да читаоци најпре сами покушају да реше задатак пре него што потраже његово решење. Тако ће од задатка имати знатно више користи, чак и ако не успеју да га реше. Наравно, уколико реше задатак, опет могу погледати и дато решење, можда нешто ново науче из њега!

За крај, аутори желе да изразе своју захвалност рецензентима др Небојши Икодиновићу, редовном професору Математичког факултета, др Зорану Пуцановићу, редовном професору Грађевинског факултета и др Милошу Банковићу, доценту Математичког факултета, као и др Славку Моцоњи, ванредном професору Математичког факултета, који је, не у својству рецензента, него у својству колеге, прегледао цео текст. Сви они су дали низ веома корисних сугестија и захваљући њима у књизи има значајно мање штампарских, али и материјалних грешака него

што би иначе било! Свакако, за све преостале грешке, одговорност преузимају аутори на себе.

У Београду, маја 2025. године

Аутори

Глава 1

Скупови

1.1 Формирање скупова

Појам скупа је интуитивно врло јасан, мада се прецизно описује тек аксиомама теорије скупова, које ће бити изложене у наставку. Раселов[1] парадокс нас брзо може убедити зашто није тако једноставно описати нешто што је скуп.

Наиме, нека је S сачињен од елемената x за које важи $x \notin x$. Да ли је $S \in S$? Ако јесте, онда према томе како смо дефинисали S важи $S \notin S$, што је немогуће. С друге стране, ако није $S \in S$, онда S испуњава својство елемента од S, што је такође немогуће. Дакле, S није скуп.

Основна релација међу скуповима је већ поменута релација припадности. Скуп x припада скупу y записујемо као $x \in y$ и кажемо да је x елемент скупа y. Наравно, овде ћемо подразумевати да су читаоци упознати, као што и јесу, са основним појмовима теорије скупова.

Наведимо сада аксиоме теорије скупова.

Аксиоме теорије скупова:

A1 (Аксиома екстензионалности или Аксиома обухватности) Два скупа су једнака ако имају исте елементе.

Поента ове аксиоме је да је скуп потпуно одређен елементима који се налазе у њему, није битан њихов поредак нити чињеница да је неки елемент можда наведен више пута.

A2 (Аксиома празног скупа) Постоји скуп који нема ниједан елемент. Означаваћемо га са $\emptyset$.

Аксиома празног скупа нам гарантује да постоји бар један скуп – празан скуп. На основу прве аксиоме празан скуп је јединствен.

[1] Bertrand Russell (1872-1970), британски филозоф и математичар

Глава 2

Релације

2.1 Основни појмови и особине

Први и најпознатији примери релација су релације $\leq$, $=$, $\subseteq$, и тако даље. Неформално речено, појам релације бави се остваривањем веза између неких елемената скупова које посматрамо. Математичка дефиниција гласи овако:

Дефиниција 2.1 Нека су A и B скупови. *Релација* ρ са скупа A у скуп B је сваки подскуп од $A \times B$. Дакле, $\rho \subseteq A \times B$. Ако је $A = B$ онда кажемо да је ρ *бинарна релација* на скупу A.

За $(a, b) \in \rho$ користимо и запис $a \,\rho\, b$.

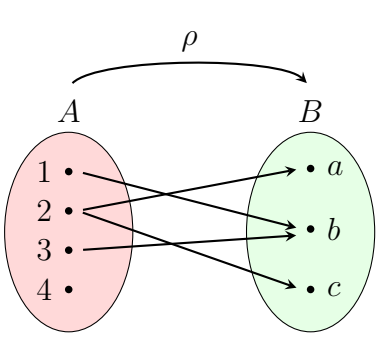
Уколико су A и B коначни скупови, релацију $\rho \subseteq A \times B$ можемо представити у форми дијаграма који се формира на следећи начин:

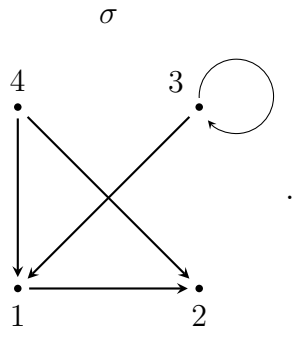
- елементима скупа A и скупа B придружимо тачке у равни,
- уколико је $(a, b) \in \rho$, тада од тачке придружене елементу $a \in A$ полази усмерена стрелица ка тачки која је придружена елементу b.

Пример 2.2 Нека су скупови $A = \{1, 2, 3, 4\}$ и $B = \{a, b, c\}$. Релације

$$\rho = \{(1, b), (2, a), (2, c), (3, b)\} \subseteq A \times B \text{ и } \sigma = \{(1, 2), (3, 1), (3, 3), (4, 1), (4, 2)\} \subseteq A^2$$

помоћу дијаграма представљамо на следећи начин:





Глава 3

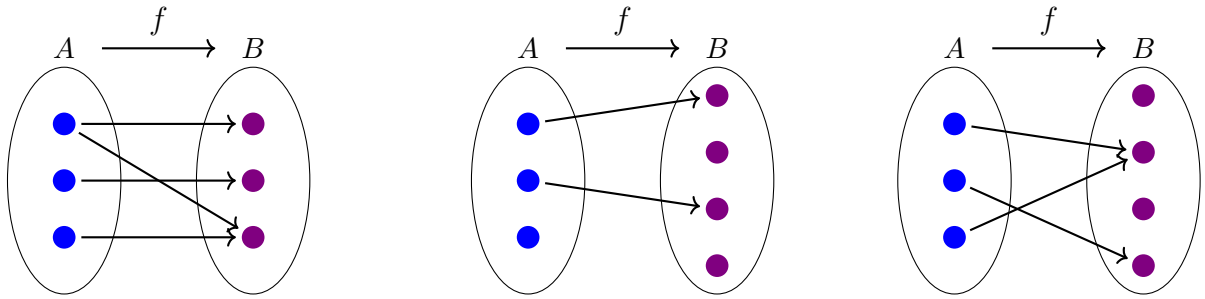
Функције

3.1 Основни појмови и особине

Нека су дати скупови A и B. Функцију из A у B замишљамо као додељивање елементима скупа A елементе скупа B, на неки начин. Увешћемо функцију преко појма релације и лако се можемо уверити да се та дефиниција поклапа са нашом интуицијом.

Дефиниција 3.1 Нека је $f \subseteq A \times B$ релација. Кажемо да је f функција ако за свако $a \in \mathrm{Dom}(f)$ постоји тачно једно $b \in B$ тако да $(a, b) \in f$.

Ако је $f \subseteq A \times B$ функција, уместо $(a, b) \in f$ пишемо $b = f(a)$. Ако је $\mathrm{Dom}(f) = A$, пишемо $f \colon A \to B$ и кажемо да је f функција из A у B. Скуп A тада називамо *домен* функције f, а скуп B *кодомен*.



није функција из A у B — није функција из A у B — функција из A у B

Уколико $f \colon A \to B$ и ако је $C \subseteq A$, онда можемо дефинисати *рестрикцију* функције f на подскуп C са

$$f|_C := \{(x, y) \in f : x \in C\}.$$

Тада $f|_C \colon C \to B$ и $f|_C(c) = f(c)$ за све $c \in C$.

Ако је $f \colon A \to B$ функција, знамо да је f^{-1} инверзна релација. Занима нас под којим условима је f^{-1} такође и функција. Како је

$$\begin{aligned} \mathrm{Dom}(f^{-1}) = \mathrm{Im}(f) &= \{b \in B \mid \text{постоји } a \in A \text{ тако да } (a, b) \in f\} \\ &= \{b \in B \mid \text{постоји } a \in A \text{ тако да } f(a) = b\}, \end{aligned}$$

Глава 4

Бројеви

Прве аксиоме теорије природних бројева увели су Пеано[1] и Дедекинд[2] крајем 19. века. Докажимо за почетак пар тврђења која ће нам касније бити потребна.

Тврђење 4.1 а) Не постоји скуп x такав да је $x \in x$.

б) Не постоје скупови x и y такви да $x \in y$ и $y \in x$.

Доказ. а) Претпоставимо да је $x \in x$ за неки x. Посматрајмо скуп $A = \{x\}$. Из $x \in x$ и $x \in A$ следи да је $A \cap x \neq \emptyset$. Према аксиоми регуларности, постоји $a \in A$ тако да $A \cap a = \emptyset$. С друге стране, једини елемент у A је x. На основу аксиоме регуларности добили смо контрадикцију.

б) Нека је $x \in y$ и $y \in x$, за неке x и y. Нека је $A = \{x, y\}$. Како је $x \in A$ и $x \in y$, следи да је $A \cap y \neq \emptyset$. Такође, из $y \in A$ и $y \in x$ следи да $A \cap x \neq \emptyset$. Једини елементи у A су x и y, па опет добијамо противречност са аксиомом регуларности. □

Напомена 4.2 Посебно, сада знамо да не постоји скуп који садржи све скупове пошто би такав скуп садржао сам себе као свој елемент, а видимо да то није могуће.

Тврђење 4.3 Ако је $x \cup \{x\} = y \cup \{y\}$, онда је $x = y$.

Доказ. Претпоставимо супротно: нека је $x \neq y$. Како је

$$x \in x \cup \{x\} = y \cup \{y\},$$

то је $x \in y$ или $x \in \{y\}$, односно, $x \in y$ или $x = y$. Због претпоставке, мора бити $x \in y$. С друге стране из $y \in y \cup \{y\} = x \cup \{x\}$ следи да је $y \in x$ или $y = x$. Дакле, $y \in x$. Закључили смо да је $x \in y$ и $y \in x$. Због тврђења 4.1б, ово је контрадикција. □

Приликом увођења Пеанових аксиома водило се рачуна о томе да се формира што је могуће мањи скуп правила (аксиома) којим би се формално описао скуп природних бројева, важан и на интуитивном нивоу свима добро познат објекат.

[1] Giuseppe Peano (1858-1932), италијански математичар

[2] Julius Wilhelm Richard Dedekind (1831-1916), немачки математичар

Глава 5

Коначни и бесконачни скупови

5.1 Коначни и пребројиви скупови

Пре него што уведемо дефиницију коначних и бесконачних скупова докажимо следеће тврђење које ће нам обезбедити коректност поменутих дефиниција. Како ћемо у овом поглављу у више наврата помињати скуп $\{1, 2, \ldots, n\}$, краће ћемо га означавати са $\mathbb{N}_n$.

Тврђење 5.1 Нека су $m, n \geqslant 1$ природни бројеви. Ако је $f : \mathbb{N}_m \to \mathbb{N}_n$ инјекција, тада је $m \leqslant n$.

Доказ. Нека је $\Phi(m)$ исказ: „ако је $f : \mathbb{N}_m \to \mathbb{N}_n$ инјекција, тада је $m \leqslant n$". Применом математичке индукције по m покажимо да својство $\Phi(m)$ важи за све природне бројеве $m \geqslant 1$.

Ако је $m = 1$, тада је $m \leqslant n$, за било које $n \geqslant 1$, па $\Phi(1)$ тривијално важи. Претпоставимо да је тачно $\Phi(m)$ и докажимо да тада важи и $\Phi(m+1)$. Нека је $f : \mathbb{N}_{m+1} \to \mathbb{N}_n$ инјекција. Означимо са $b = f(m+1)$. Тада је функција $g : \mathbb{N}_m \to \mathbb{N}_n \setminus \{b\}$ дефинисана са $g(x) = f(x)$ инјекција. Није тешко уверити се да је и функција $h : \mathbb{N}_n \setminus \{b\} \to \mathbb{N}_{n-1}$ дефинисана са

$$h(x) = \begin{cases} x, & x < b \\ x - 1, & x > b \end{cases}$$

такође инјекција. Како су g и h инјекције, на основу примера 3.9, композиција $h \circ g : f : \mathbb{N}_m \to \mathbb{N}_{n-1}$ је такође инјекција. Према томе, на основу индуктивне претпоставке следи да је $m \leqslant n - 1$. Из последњег закључујемо да је $m + 1 \leqslant n$, па важи $\Phi(m + 1)$. □

Дефиниција 5.2 Непразан скуп X је *коначан* ако постоји природан број n такав да постоји бијекција $f : X \to \mathbb{N}_n$. Тада кажемо да X има n елемената и пишемо $|X| = n$. Ако скуп није коначан, кажемо да је *бесконачан*.

Глава 6

Исказна логика

6.1 Увод

Исказ је реченица која је или тачна или нетачна. Тачне исказе формално ћемо означавати са 1 а нетачне са 0. У наставку наводимо пар примера тачних и нетачних исказа.

„*Не постоје* $a, b \in \mathbb{Z}$ *такви да је* $\sqrt{2} = \frac{a}{b}$.” (Тачан.)

„*Број 1 је решење квадратне једначине* $x^2 - x + 3 = 0$.” (Нетачан.)

„*Земља је највећа планета у Сунчевом систему.*” (Нетачан.)

„$2 + 3 > 4$.” (Тачан.)

Од исказа се могу формирати сложени искази. Основна особина сложеног исказа је то да је његова истинитосна вредност потпуно одређена истинитосном вредношћу исказа који фигуришу у њему. Сложени искази се формирају уз помоћ исказних операција. Издвајамо шест операција које одговарају везницима говорног језика.

Дефиниција 6.1 *Конјункција* исказа p и q је исказ $p \wedge q$ („p и q”). Тачан је ако су тачни и p и q. У свим осталим случајевима је нетачан.

Дефиниција 6.2 *Дисјункција* исказа p и q је исказ $p \vee q$ („p или q”). Нетачан је ако су нетачни и p и q. У свим осталим случајевима је тачан.

Дефиниција 6.3 *Импликација* исказа p и q је исказ $p \Rightarrow q$ („p повлачи q”). Нетачан је ако је тачан p и нетачан q. У свим осталим случајевима је тачан.

Исказ $p \Rightarrow q$ још читамо и: „ако p онда q”, „из p следи q”, „p имплицира q”, „p је довољан услов за q”, „q је потребан услов за p”, „p само ако q”.

Дефиниција 6.4 *Еквиваленција* исказа p и q је исказ $p \Leftrightarrow q$ („p ако и само ако q”). Тачан је ако p и q имају једнаке истинитосне вредности – оба су тачна или су оба нетачна. У осталим случајевима је нетачан.

Глава 7

Формални системи

7.1 Основни појмови

Формални систем (*формална теорија*) $\mathcal{S}$ је уређена четворка $\mathcal{S} = (\mathcal{A}, For, Ax, Rules)$, при чему:

1. *Азбука* $\mathcal{A}$ је највише пребројив скуп симбола. *Реч* је коначан низ симбола из дате азбуке.

2. Неки подскуп скупа свих речи је скуп *формула* For. При том је дат и поступак помоћу ког се одређује да ли је нека реч формула или не.

3. *Скуп аксиома* Ax је неки подскуп скупа свих формула.

4. Дат је коначан скуп правила извођења $Rules$. Ако су $A_1, A_2, \ldots, A_{n-1}, A_n$ било које формуле, тада *правило извођења* α (дужине n) одлучује да ли из формула $A_1, A_2, \ldots, A_{n-1}$ следи формула A_n. У потврдном случају пишемо

$$\alpha : \frac{A_1, A_2, \ldots, A_{n-1}}{A_n}.$$

   Кажемо и да је A_n директна последица формула $A_1, A_2, \ldots, A_{n-1}$.

Дефиниција 7.1 Коначни низ формула $A_1, A_2, \ldots, A_n$ неког формалног система је *извођење* или *доказ* ако за сваку формулу A_i важи да је или аксиома или је директна последица неких претходних формула тог низа (по неком правилу извођења).

Дефиниција 7.2 Формула A је теорема ако постоји извођење $A_1, A_2, \ldots, A_n$ тако да је $A_n = A$. Пишемо $\vdash A$.

Дефиниција 7.3 Формула A је *последица скупа формула* Γ ако постоји низ формула $A_1, A_2, \ldots, A_n$ тако да је $A_n = A$ и ако за сваку формулу A_i важи да је или аксиома или једна од формула скупа Γ или је директна последица неких претходних формула тог низа (по неком правилу извођења). Пишемо $\Gamma \vdash A$.

Глава 8

Предикатска логика

8.1 Језик предикатске логике

Уколико посматрамо исказе

„За сваки цео број x постоји цео број y такав да је $x + y = 5$"

„За сваки елемент у скупу X постоји елемент у скупу Y који га дели."

увидећемо да их не можемо изразити језиком исказне логике. Такође, уколико бисмо желели да формализујемо неку математичку теорију (нпр. да формалним језиком запишемо Пеанове аксиоме) исказна логика не би била довољна. Разлог лежи у томе што се исказна логика бави тиме како су једноставни искази повезани логичким везницима, док само значење тих једноставних исказа није битно. Да би се превазишла ова препрека уведена је предикатска логика која је значајно изражајнија од исказне логике. Главна разлика предикатске логике у односу на исказну јесте увођење универзалне и егзистенционалне квантификације. Додатно, води се рачуна и о самој семантици (значењу) исказа увођењем функцијских и релацијских структура.

Елементи језика предикатске логике су:

- скуп променљивих *Var* (променљиве ћемо обично означавати са $x, y, z, \dots$);
- логички везници: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$;
- квантификатори $\forall$ и $\exists$;
- интерпункцијски знаци (зарез, лева и десна заграда): , ( ) ;
- знак једнакости $=$;
- скуп функцијских (или операцијских) симбола *Fun* (обично ћемо их означавати са $f, g, h, \dots$);
- скуп релацијских (или предикатских) симбола *Rel* (обично ћемо их означавати са $p, q, r, \dots$);
- скуп константи *Const* (обично ћемо их означавати са $a, b, c, \dots$).

Релацијски и функцијски симболи имају своју *дужину* која је природан број $n > 0$ и која се назива и *арност* релације или функције. Означавамо је са ar.

Глава 9

Булове алгебре

9.1 Дефиниција и примери Булових алгебри

Булове алгебре увео је Џорџ Бул[1] средином XIX века са идејом да логику и њене законитости преведе на језик алгебре. Првобитни назив за теорију Булових алгебри био је управо алгебра логике. Временом су Булове алгебре примењене на широк спектар дисциплина, од теорије скупова до статистике, при чему је најважнија област примене рачунарство и информатика. У овом поглављу даћемо дефиницију, основна својства и најпознатије примере Булових алгебри.

Дефиниција 9.1 Алгебарска структура $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$, где је $B \neq \emptyset$, $0, 1 \in B$, $\curlyvee$ и $\curlywedge$ су бинарне а $'$ је унарна операција на скупу B, је *Булова алгебра* уколико су задовољене следеће аксиоме:

A1: $x \curlyvee y = y \curlyvee x$,

A2: $x \curlywedge y = y \curlywedge x$,

A3: $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$,

A4: $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$,

A5: $x \curlyvee 0 = x$,

A6: $x \curlywedge 1 = x$,

A7: $x \curlyvee x' = 1$,

A8: $x \curlywedge x' = 0$,

A9: $0 \neq 1$.

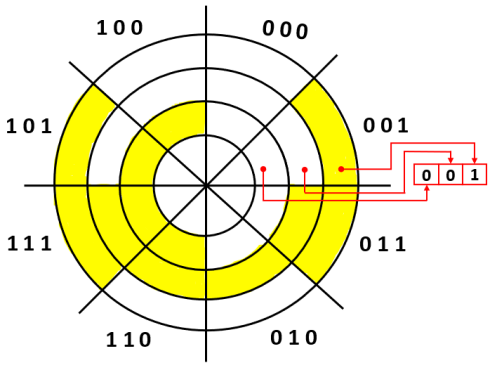
за свако $x, y, z \in B$.

[1] George Boole (1815-1864), енглески математичар и филозоф

Додатак А

Грејови кодови

Грејове кодове је први пут описао Френк Грej[1] (по коме су касније ови кодови и добили име) који је 1953. патентирао[2] њихову употребу за декодирајуће дискове (тзв. декодере). Декодер представља точак са концентричним тракама и проводном четком која може да очита број трака под одређеним углом. Идеја је била да се сваком од 2^n различитих углова придружи јединствен n-битни бинарни број (видети слику А.1).



Слика А.1: Декодер који користи 3-битни бинарни код

На слици А.1 можемо приметити да се бинарне репрезентације суседних углова разликују у једном биту на одређеној позицији. Ова особина представља главну карактеристику Грејових кодова и чини их погодним за употребу у детекцији грешака и контроли позиција ротационих елемената. У случају декодера, уколико код суседних углова дође до „нагле" промене броја трака, тј. уколико се бинарне репрезентације суседних углова разликују у битовима на више различитих позиција то ће указати на потенцијалну грешку. Грејови кодови данас имају значајну примену и у теорији графова, као и у дизајну логичких кола (погледати секцију 9.6).

Означимо са $\mathcal{B}_n$ скуп свих бинарних низова дужине n. Приметимо да је $|\mathcal{B}_n| = 2^n$. У наставку дајемо формалну дефиницију Грејових кодова.

[1]Frank Gray (1887-1969), амерички физичар и истраживач
[2]Патент "Pulse Code Communication"

Додатак Б

RSA **алгоритам**

Криптографија је наука чији је основни задатак развој процедура којима се чува тајност порука, тј. обезбеђује се да поруке буду читљиве само онима којима су намењене. Прецизније, уколико порука треба да стигне од пошиљаоца до примаоца преко несигурног комуникационог канала, задатак криптографије је да онемогући да приликом доставе порука буде прочитана и од стране трећег лица, тзв. противника. Идеја је да се оригинална порука процесом шифровања учини непрепознатљивом за све сем за пошиљаоца и примаоца. Прималац касније уз помоћ кључа процедуром дешифровања долази до оригиналне поруке. Шифровање и дешифровање подразумева примену специјално одабраних математичких функција. Одабир погодних функција темељи се на резултатима теорије бројева, стога теорија бројева представља срж модерне криптографије.

Са развојем интернет технологија расте и значај криптографије као научне дисциплине. Данас се криптографија користи за обезбеђивање сигурне комуникације путем интернета, као и за пружање аутентичности у дигиталним комуникацијама генерисањем тзв. дигиталног потписа. У овом поглављу биће представљен један од најпознатијих и најпоузданијих алгоритама за безбедно слање података, тзв. RSA алгоритам.

RSA (Rives-Shamir-Adleman) алгоритам за криптовање изумели су Рон Ривест, Ади Шамир и Лен Адлеман 1977. године, па је овај алгоритам добио назив по почетним словима презимена његових аутора. RSA алгоритам је први и најчешће коришћени алгоритам за шифровање који користи јавни кључ. Пошиљалац поруку шифрује применом јавног кључа а прималац добијену поруку дешифрује уз помоћ приватног кључа, док остали добијају бесмислени текст. Јавност кључа за шифровање значи да било ко може шифровати поруку уз помоћ тог кључа, међутим, дешифровање може извршити само онај ко поседује приватни кључ. У наставку ћемо описати процес генерисања јавног и приватног кључа и даћемо поступак шифровања и дешифровања у RSA криптосистему.

Генерисање јавног и приватног кључа састоји се из следећих корака:

корак 1: бирају се два велика проста броја p и q и рачуна се производ $n = pq$;

корак 2: рачуна се $\varphi(n)$, где је φ Ојлерова функција;