

Diskretna matematika

©2000 Željko Vrba

Ovo su auditorne vježbe iz diskretne matematike rađene na FER-u, koje je godine 1997./98. održala asistentica Andrea Aglič. Ovo je samo sažetak neophodne teorije za pismeni ispit. Za konkretne zadatke ipak treba pogledati zadatke rađene na auditorima, a za usmeni također treba pogledati dodatno gradivo jer su izostavljene relacije, operator diferencije i još neke stvari.

1	Skupovi	3
2	Logika i predikatni račun	3
2.1	Operacije među sudovima	3
2.2	Svojstva algebre sudova	4
2.3	Algebra predikata	4
3	Booleove algebre	5
3.1	Definicija i svojstva	5
3.2	Booleove funkcije	5
4	Teorija brojeva	6
4.1	Djeljivost	6
4.2	Prosti brojevi	6
4.3	Kongruencije	6
5	Kombinatorika	7
5.1	Permutacije, varijacije i kombinacije	7
5.2	Formula uključivanja-isključivanja	9
5.3	Dirichletov princip	9
5.4	Funkcije izvodnice	9
6	Rekurzivne relacije	10
6.1	Homogene RR	10
6.2	Nehomogene RR	10
7	Algebarske strukture	11
7.1	Grupe	11
7.2	Simetrične grupe	12
7.3	Prsteni i polja	12
8	SNBR stroj	13

1 Skupovi

Skup je bilo koja množina elemenata. Element je osnovni pojam i ne definira se. Operacije nad skupovima su presjek, unija, razlika, komplement te simetrična diferencija ($A \triangle B = (A \setminus B) \cup (B \setminus A)$)

Definicija 1 Za neprazne skupove $A_1, \dots, A_n \neq \emptyset$ definiramo *Kartezijev produkt*:

$$A_1 \times A_2 \times \dots \times A_n$$

kao skup svih uređenih n -torki (a_1, \dots, a_n) tako da je $a_k \in A_k, k = 1 \dots n$. Ponekad se koristi oznaka $\prod_{i=1}^n A_i$. Svaku n -torku možemo shvatiti kao funkciju $f : \{1, \dots, n\} \rightarrow \bigcup_{i=1}^n A_i$ i $f(k) \in A_k$. Tada je Kartezijev produkt skup svih takvih funkcija.

Definicija 2 A je *konačan* ako postoji prirodan broj $n \in \mathbb{N}$ i *bijekcija* $f : \{1, 2, \dots, n\} \rightarrow A$. n je *kardinalni broj* broja skupa A (broj elemenata u skupu) i pišemo $n = |A|$. A je *beskonačan* ako nije konačan.

A je beskonačan ako i samo ako postoji bijekcija sa \mathbb{N} na neki njegov pravi podskup.

A je *prebrojivo konačan* ako se njegovi elementi mogu poredati u niz što je ekvivalentno s postojanjem bijekcije $f : \mathbb{N} \rightarrow A$. To su tzv. *diskretni skupovi*, npr. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$. Njihov kardinalni broj je \aleph_0 .

Elementi *neprebrojivo beskonačnog* skupa se ne mogu poredati u niz, npr. \mathbb{R} i \mathbb{C} . Njihov kardinalni broj se označava sa c (kontinuum).

2 Logika i predikatni račun

Definicija 3 Pod *sudom* podrazumijevamo afirmativnu rečenicu ako je istinita ili lažna. Sudove označavamo velikim slovima, a istinitost sa $\tau A = \top$ ili $\tau A = \perp$.

2.1 Operacije među sudovima

- Unarne operacije: postoji samo jedna: negacija. Njezina je tablica istinitosti:

A	$\neg A$
\top	\perp
\perp	\top

- Binarne operacije: od ukupno 16 različitih binarnih operacije ovdje će biti navedene samo najvažnije:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$A \nabla B$
\top	\top	\top	\top	\top	\top	\perp
\top	\perp	\perp	\top	\perp	\perp	\top
\perp	\top	\perp	\top	\top	\perp	\top
\perp	\perp	\perp	\perp	\top	\top	\perp

Definicija 4 Za dvije formule sudova A i B se kaže da su *logički istovrijedne* ili jednake ako za bilo koju kombinaciju vrijednosti istinitosti njihovih varijabli sudova, poprimaju istu vrijednost istinitosti.

Da bi se izbjeglo suvišno pisanje zagrada uvodi se *prioritet operatora*: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$.

Definicija 5 Formula A algebre sudova se zove *identički istina* ili *tautologija* ako poprima isključivo vrijednost \top za sve vrijednosti istinitosti sudova od kojih je izgrađena. Analogno se definira *identički neistinita* formula.

Npr. $A \wedge \neg A$ je identički neistinita, a $A \vee \neg A$ je tautologija

2.2 Svojstva algebre sudova

- | | |
|--|--|
| 1. $A \wedge A \equiv A$ | 10. $\neg(A \vee B) \equiv \neg A \wedge \neg B$ |
| 2. $A \vee A \equiv A$ | 11. $A \vee \perp \equiv A$ |
| 3. $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ | 12. $A \wedge \top \equiv A$ |
| 4. $(A \vee B) \vee C \equiv A \vee (B \vee C)$ | 13. $A \vee \top \equiv \top$ |
| 5. $A \wedge B \equiv B \wedge A$ | 14. $A \wedge \perp \equiv \perp$ |
| 6. $A \vee B \equiv B \vee A$ | 15. $A \vee \neg A \equiv \top$ |
| 7. $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ | 16. $A \wedge \neg A \equiv \perp$ |
| 8. $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ | 17. $\neg(\neg A) \equiv A$ |
| 9. $\neg(A \wedge B) \equiv \neg A \vee \neg B$ | |

Ako je neka formula A algebre sudova dana svojom tablicom istinitosti, lako je sagraditi njoj jednaku formulu algebre sudova koja će imati oblik disjunktije blokova od kojih je svaki konjunkcija varijabli od A ili njihovih negacija (*perfektna disjunktivna forma*) ili koja će imati oblik konjunkcije blokova od kojih je svaki disjunktija varijabli od A ili njihovih negacija (*perfektna konjunktivna forma*). Pri građenju disjunktivne forme gledamo samo retke gdje je $A = \top$, a kod konjunktivne forme samo retke gdje je $A = \perp$.

Definicija 6 Skup operacija algebre sudova s kojima se može izgraditi formula s proizvoljno zadanim tokom vrijednosti istinitosti zove se *sustav izvodnica* algebre sudova. Sustav izvodnica algebre sudova sa svojstvom da nijedan njegov pravi podskup nije sustav izvodnica, dakle minimalni sustav izvodnica zove se *baza algebre sudova*

Npr. jedan sustav izvodnica je $\{\neg, \wedge, \vee\}$, a baza je npr. $\{\neg, \wedge\}$. Jedna od tročlanih baza je $\{\vee, \Leftrightarrow, \underline{\vee}\}$. Postoje i jednočlane baze: $\{\uparrow\}$ (Shefferova operacija, NI) te $\{\downarrow\}$ (Lukasiewiczova operacija, NILI).

2.3 Algebra predikata

Definicija 7 Rečenica koja sadrži jednu ili više varijabli i koja za konkretne vrijednosti iz zadanog skupa D (domene) postaje sud zove se *predikat*.

Univerzalni kvantifikator: $\forall x P(x)$ je sud ako je $P(x)$ jednomjesni predikat (smanjuje broj varijabli za jedan). Također i kvantifikator egzistencije: $\exists x P(x)$.

Teorem 1 (*Negiranje kvantifikatora*) Ovaj teorem kaže kako se negiraju predikati koji sadrže kvantifikatore:

$$\neg(\forall x)P(x) \equiv (\exists x)(\neg P(x))$$

$$\neg(\exists x)P(x) \equiv (\forall x)(\neg P(x))$$

3 Booleove algebre

3.1 Definicija i svojstva

Definicija 8 Apstraktna Booleova algebra je neprazan skup B zajedno s dvije binarne operacije $+, \cdot : B \times B \rightarrow B$, jednom unarnom operacijom $\bar{} : B \rightarrow B$ i dvije konstante $0, 1 \in B$ tako da $\forall x, y, z \in B$ vrijedi:

- | | |
|--|--------------------------|
| 1. $x + y = y + x$ | 6. $x + 0 = x$ |
| 2. $x \cdot y = y \cdot x$ | 7. $x \cdot \bar{x} = 0$ |
| 3. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ | 8. $x + \bar{x} = 1$ |
| 4. $x + (y \cdot z) = (x + y) \cdot (x + z)$ | 9. $0 \neq 1$ |
| 5. $x \cdot 1 = x$ | |

Iz ovih svojstava slijedi asocijativnost:

$$(x + y) + z = x + (y + z)$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Još neka svojstva (za dokaz pogledati vježbe):

- | | |
|---|---|
| 1. ako je $x + y = 1$ i $x \cdot y = 0$ tada je $y = \bar{x}$ | 3. $\overline{(\bar{x})} = x$ |
| 2. de Morganovi zakoni: | 4. ako je $y + x = z + x$ i $y + \bar{x} = z + \bar{x}$ tada je $y = z$ |
| • $\overline{x + y} = \bar{x} \cdot \bar{y}$ | |
| • $\overline{x \cdot y} = \bar{x} + \bar{y}$ | |

3.2 Booleove funkcije

Definicija 9 Booleova funkcija od n varijabli je $F : \{0, 1\}^n \rightarrow \{0, 1\}$. Ukupan broj različitih Booleovih funkcija od n varijabli iznosi 2^{2^n} . Skup svih Booleovih funkcija n varijabli označavamo sa B_n .

Teorem 2 Neka je $F : \{0, 1\}^n \rightarrow \{0, 1\}$ Booleova funkcija i neka je $J = \{(j_1, j_2, \dots, j_n) \in \{0, 1\}^n \mid F(j_1, \dots, j_n) = 1\}$ (skup svih n -torki za koje je $F = 1$). Tada je

$$F(x_1, \dots, x_n) = \sum_{(j_1, \dots, j_n) \in J} (x_1^{j_1} \cdot x_2^{j_2} \dots x_n^{j_n})$$

Analogno, neka je $K = \{(k_1, \dots, k_n) \in \{0, 1\}^n \mid F(k_1, \dots, k_n) = 0\}$ skup svih n -torki za koje je $F = 0$. Tada je

$$F(x_1, \dots, x_n) = \prod_{(k_1, \dots, k_n) \in K} (\bar{x}_1^{k_1} + \bar{x}_2^{k_2} + \dots + \bar{x}_n^{k_n})$$

gdje je:

$$x_i^0 = \overline{x_i}$$

$$x_i^1 = x_i$$

4 Teorija brojeva

4.1 Djeljivost

Kažemo da a dijeli b (b je djeljiv sa a) i pišemo $a|b$ ako i samo ako $(\exists k \in \mathbb{Z})(b = ka)$. Definiramo najveću zajedničku mjeru i najmanji zajednički višekratnik za dva ili više brojeva. Za svaka dva broja a i b vrijedi:

$$\text{nzv}(a, b) = \frac{ab}{\text{Nzm}(a, b)}$$

Teorem 3 (*O dijeljenju*) Neka je $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Tada postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \{0, 1, \dots, b-1\}$ tako da je

$$a = bq + r$$

q nazivamo *kvocijent*, a r *ostatak*.

4.2 Prosti brojevi

Definicija 10 Broj $p \in \mathbb{N}$, $p > 1$ je *prost* ako su mu 1 i p jedini djelitelji (tj. ako ima samo *trivijalne djelitelje*). Ako nije prost, onda je *složen*. 1 nije ni prost ni složen. Dobar algoritam za nalaženje svih prostih brojeva do nekog n je *Eratostenovo sito*.

Teorem 4 Osnovni teorem aritmetike: $\forall n \in \mathbb{N}, n > 1$ postoji *jedinstveni* rastav na proste faktore:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

gdje je $p_1 < p_2 < \dots < p_k$ i svi p_i su prosti.

Teorem 5 (*Euklidov*) Skup svih prostih brojeva je beskonačan, tj. ne postoji najveći prost broj.

Teorem 6 $\forall n \in \mathbb{N}$ postoji n uzastopnih složenih brojeva: to su brojevi $2|a_1 = (n+1)! + 2$, $3|a_2 = (n+1)! + 3, \dots, a_n = (n+1)|(n+1)! + (n+1)$.

4.3 Kongruencije

Definicija 11 Pišemo $a \equiv b \pmod{m}$ (a i b cijeli, m pozitivan), ako i samo ako $m|(a-b)$, tj. a i b daju isti ostatak pri dijeljenju sa m . Relacija "biti kongruentan" je *relacija ekvivalencije*.

Teorem 7 Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, te $k, n \in \mathbb{N}$ tada je

- | | |
|--------------------------------------|------------------------------|
| 1. $a \pm c \equiv b \pm d \pmod{m}$ | 3. $ka \equiv kb \pmod{m}$ |
| 2. $ac \equiv bd \pmod{m}$ | 4. $a^n \equiv b^n \pmod{m}$ |

Teorem 8 Ako je $ka \equiv kb \pmod{m}$ i ako je $\text{Nzm}(k, m) = 1$ tada je $a \equiv b \pmod{m}$. Općenitije vrijedi,

$$ka \equiv kb \pmod{m} \Rightarrow a \equiv b \pmod{\frac{m}{\text{Nzm}(k, m)}}$$

Iz ovoga direktno slijedi ova činjenica: Neka je $P(x)$ polinom sa cjelobrojnim koeficijentima, te neka je $a \equiv b \pmod{m}$. Tada je i $P(a) \equiv P(b) \pmod{m}$

Definicija 12 Eulerova funkcija $\phi(m)$ se definira kao broj brojeva $\leq m$ i relativno prosti sa m .

Ako je p prost tada je

$$\phi(p) = p - 1$$

Ako su m i n relativno prosti ($\text{Nzm}(m, n) = 1$) tada je

$$\phi(mn) = \phi(m)\phi(n)$$

Ako m ima rastav na proste faktore $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ tada se $\phi(m)$ može računati po slijedećoj formuli:

$$\phi(m) = m(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_n})$$

Teorem 9 (Euler) Ako su a i m relativno prosti tada vrijedi:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Specijalan slučaj ovog teorema je *mali Fermatov teorem*: ako je p prost, tada je $\text{Nzm}(a, p) = 1$ i vrijedi $a^{p-1} \equiv 1 \pmod{p}$

5 Kombinatorika

Teorem 10 (*O uzastopnom prebrojavanju*) Ako se prvi dio posla može učiniti na n_1 načina, drugi na n_2 načina, itd. . . , r -ti dio na n_r načina, tada se čitav posao može učiniti na $n_1 n_2 \dots n_r$ načina.

Oznake koje će se ovdje koristiti za permutacije, varijacije i kombinacije (C, V, P) su nestandardne i ne treba ih znati.

5.1 Permutacije, varijacije i kombinacije

Definicija 13 Permutacija bez ponavljanja je svaka uređena n -torka od n -članog skupa sa različitim elementima. Broj svih permutacija od n elemenata je

$$P_n = n!$$

Primjer 5.1 Ispiši sve permutacije skupa 1, 2, 3. Ima ih $3! = 6$: 123, 132, 213, 231, 312, 321.

Definicija 14 Permutacija sa ponavljanjem od n elemenata je permutacija n elemenata koji nisu svi različiti i od kojih je 1. vrste n_1 , 2. vrste n_2 , . . . , k -te vrste n_k pri čemu je

$$n_1 + n_2 + \dots + n_k = n$$

Broj takvih permutacija iznosi

$$P_n^{n_1, \dots, n_k} = \frac{n!}{n_1! n_2! \dots n_k!}$$

Primjer 5.2 Koliko se različitih riječi može napraviti od riječi “matematika”? Imamo 3 slova A, 2 slova M, 2 slova T te po jedno E, K, I. Broj različitih riječi je

$$\frac{10!}{3!2!2!} = 151200$$

Definicija 15 Kombinacije bez ponavljanja od n elemenata r -tog razreda ($r \leq n$) je svaka *neuređena* r -torka (r -člani podskup) od n -članog skupa sa različitim elementima. Broj svih kombinacija je

$$C_n^r = \frac{n(n-1) \dots (n-r+1)}{r!} = \frac{n!}{r!(n-r)!} = \binom{n}{r}$$

Primjer 5.3 Na koliko se načina u razredu od 30 učenika može odabrati 3 predstavnika: $\binom{30}{3} = 4060$.

Definicija 16 Kombinacija s ponavljanjem od n elemenata r -tog razreda je svaka *neuređena* r -torka ne nužno različitih elemenata od n -članog skupa s različitim elementima (npr. “loto r od n” s vraćanjem kuglica u bubanj nakon svakog izvlačenja):

$$\overline{C}_n^r = \binom{n+r-1}{r}$$

Primjer 5.4 Broj načina na koji se može 5 istih nagrada podijeliti među 30 ljudi ako a) svaki čovjek može dobiti 1 nagradu: $C_{30}^5 = \binom{30}{5} = 142506$, b) svaki čovjek može dobiti proizvoljno mnogo nagrada (ipak, najviše 5 jer ih samo toliko ima): $\overline{C}_{30}^5 = \binom{34}{5} = 278256$

Definicija 17 Varijacije bez ponavljanja r -tog razreda ($r \leq n$) je svaka *uređena* r -torka od n -članog skupa s različitim elementima. Broj svih takvih je

$$V_n^r = n(n-1)(n-2) \dots (n-r+1)$$

Primjer 5.5 Na koliko se načina može 6 putnika rasporediti u autobus sa 15 sjedala: $V_{15}^6 = 3603600$. Primijetiti da za $n = r$ imamo permutacije.

Definicija 18 Varijacije s ponavljanjem n elemenata r -tog razreda je svaka *uređena* r -torka ne nužno različitih elemenata n -članog skupa s različitim elementima. Broj svih iznosi

$$\overline{V}_n^r = n^r$$

Primjer 5.6 Broj mogućih ishoda bacanja 8 različitih kocaka: $\overline{V}_6^8 = 6^8$.

Umjesto pamćenja ovih formula, zadatke je bolje rješavati logički. Npr. u posljednjem primjeru s bacanjem kocaka: Svaka kocka može dati 6 različitih ishoda. Budući da imamo 8 kocaka to je ukupan broj različitih ishoda (prema teoremu o uzastopnom prebrojavanju) $6 * 6 * \dots * 6 = 6^8$.

Pri složenijim zadacima ove formule su ipak korisne, ali treba paziti da li je bitan poredak (tada koristimo varijacije/permutacije) ili nije bitan (kombinacije) te da li su dozvoljena ponavljanja. Također treba napomenuti da neki autori ne razlikuju permutacije i varijacije te upotrebljavaju samo jedan pojam (permutacije).

5.2 Formula uključivanja-isključivanja

Za kardinalni broj unije dva skupa vrijedi:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Teorem 11 Formula uključivanja-isključivanja je poopćenje prethodnog rezultata:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |A_1 \cap A_2 \dots \cap A_n|$$

Teorem 12 Neka je S konačan skup uz $|S| < \infty$ i neka su A_1, A_2, \dots, A_n neki njegovi podskupovi, $\overline{A_i} = S \setminus A_i$. Tada vrijedi:

$$|\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}| = |S| - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| - \dots + (-1)^n |A_1 \cap A_2 \dots \cap A_n|$$

U obje gornje formule se u prvoj sumi sumira po svim skupovima A_i , u drugoj sumi po svim 2-kombinacijama, trećoj po svim 3-kombinacijama itd. . . . Npr. druga suma je u slučaju $n = 3$:

$$\sum_{1 \leq i < j \leq n} |A_i \cap A_j| = |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|$$

Teorem 13 Broj svih *surjekcija* sa $|X| = n$ u $|Y| = m$ je

$$|\text{Sur}(X, Y)| = \sum_{r=0}^m (-1)^r \binom{m}{r} (m-r)^n$$

Dokaz je pomoću formule uključivanja-isključivanja.

5.3 Dirichletov princip

Teorem 14 (*Dirichletov princip*) Neka je n predmeta smješteno u m kutija, $n > m$. Onda postoji kutija s barem 2 predmeta.

Teorem 15 (*Poopćeni Dirichletov princip*) Ako je n predmeta smješteno u m kutija, onda postoji kutija koja sadrži barem

$$\left\lfloor \frac{n-1}{m} \right\rfloor + 1$$

predmeta.

5.4 Funkcije izvodnice

Definicija 19 Funkcija izvodnica niza $\{a_n\}$ je

$$f(x) = a_0 + a_1 x + \dots + a_n x^n = \sum_{n=0}^{\infty} a_n x^n$$

Teorem 16 (*Poopćeni binomni teorem*) Neka je $|x| < 1$, $\alpha \in \mathbb{R}$. Tada je

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k$$

gdje je $\binom{\alpha}{k}$ *poopćeni binomni koeficijent* definiran sa:

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-k+1)}{k!}$$

U brojniku je točno k faktora.

6 Rekurzivne relacije

6.1 Homogene RR

Linearna rekurzivna relacija s konstantnim koeficijentima je oblika:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_r a_{n-r}$$

$c_i \in \mathbb{R}$. r je *red* rekurzivne relacije za $c_r \neq 0$. Rješenje se pretpostavlja u obliku $a_n = x^n$, a nakon sređivanja se dobije *karakteristična jednadžba* rekurzivne relacije:

$$x^r - c_1 x^{r-1} - c_2 x^{r-2} - \dots - c_r = 0$$

Rješavanjem ove jednadžbe dobivamo tzv. karakteristične korijene $x_1 \dots x_r$. Imamo dva slučaja:

1. Svi korijeni su različiti. Tada je opće rješenje oblika

$$a_n = \lambda_1 x_1^n + \lambda_2 x_2^n + \dots + \lambda_r x_r^n$$

2. Neka su x_1, \dots, x_t svi različiti i neka su pripadne kratnosti k_1, \dots, k_t . Partikularno rješenje koje odgovara korijenu x_i je

$$a_n^{(i)} = (\lambda_1^{(i)} + \lambda_2^{(i)} n + \dots + \lambda_{k_i}^{(i)} n^{k_i-1}) x_i^n$$

U zagradi je polinom $k_i - 1$ -tog stupnja u varijabli n . Opće rješenje rekurzivne relacije dano je sa:

$$a_n = a_n^{(1)} + a_n^{(2)} + \dots + a_n^{(t)}$$

Napomena: Ako su x_1 i x_2 par konjugirano-kompleksnih rješenja

$$x_1 = r(\cos(\phi) + i \sin(\phi))$$

$$x_2 = r(\cos(\phi) - i \sin(\phi))$$

onda u bazi za opće rješenje umjesto x_1^n i x_2^n možemo uzeti $r^n \cos(n\phi)$ i $r^n \sin(n\phi)$.

6.2 Nehomogene RR

Linearna nehomogena rekurzivna relacija r -tog reda s konstantnim koeficijentima je oblika

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_r a_{n-r} + f(n)$$

$f(n)$	part.rj.
const.	A
Cn	$A_1n + A_0$
Cn^2	$A_2n^2 + A_1n + A_0$
C^n	AC^n
nC^n	$(A_1n + A_0)C^n$

uz $n \geq r$ i $f : N \rightarrow R$ bilo kakva funkcija.

Rješenje je zbroj općeg rješenja pripadne homogene jednačbe i partikularnog rješenja nehomogene. Za $f(n)$ treba tražiti partikularno rješenje u obliku:

Primjedba: U slučaju da $f(n)$ sadrži član Cx^n gdje je x korijen karakteristične jednačbe, odgovarajuće partikularno rješenje treba još pomnožiti s n^k pri čemu je k najmanja potencija za koju niti jedan pribrojnik u novom partikularnom rješenju nije rješenje homogene jednačbe.

Ako je $f(n)$ suma ovakvih članova, onda se partikularno rješenje traži za svaki član posebno.

Postupak rješavanja rekursivnih relacija vrlo je sličan rješavanju linearnih diferencijalnih jednačbi s konstantnim koeficijentima. Na kraju treba spomenuti da se rekursivne relacije mogu rješavati i pomoću funkcija izvodnica.

7 Algebarske strukture

7.1 Grupe

Definicija 20 Uređeni par (G, \bullet) koji se sastoji od nepraznog skupa G i binarne operacije $\bullet : G \times G \rightarrow G$ nazivamo *grupa* ako su ispunjeni slijedeći uvjeti:

1. Binarne operacije je asocijativna, tj. $(a \bullet b) \bullet c = a \bullet (b \bullet c), \forall a, b, c \in G$
2. Postoji i jednoznačno je određen neutralni element $e \in G$ sa svojstvom $e \bullet a = a \bullet e = a, \forall a \in G$
3. Svaki element je invertibilan, i njegov inverz a^{-1} je jedinstven te vrijedi $a \bullet a^{-1} = a^{-1} \bullet a = e$

Ako je operacija \bullet komutativna, riječ je o *komutativnoj* ili *Abelovoj* grupi. Ako je G konačan skup, onda je $|G|$ *red grupe*.

Teorem 17 Neka je $a \in (G, \bullet)$. Tada je:

$$\begin{aligned} a^m a^n &= a^{m+n} \\ (a^m)^n &= a^{mn} \end{aligned}$$

Definicija 21 Neka je $n, k \in N$ tako da vrijedi: 1) $a^n = e$ i 2) $a^k = e \Rightarrow k \geq n$. Tada se n naziva *red elementa* a i označava se sa $|a| = n$. Neutralni element e je uvijek reda 1.

Definicija 22 Neka je $H \subseteq G$ i (G, \bullet) grupa. Ako je (H, \bullet) također grupa, onda je (H, \bullet) podgrupa od G i pišemo $H \leq G$.

Definicija 23 Podgrupa $\{a^k | k \in Z\} \leq G$ (ovdje dopuštamo cijele brojeve, pri tome je a^{-1} inverz elementa a , a npr. $a^{-3} = a^{-1} \bullet a^{-1} \bullet a^{-1}$) zove se *podgrupa generirana* elementom a i označava se s $\langle a \rangle$. Ovo je ujedno i najmanja podgrupa od G koja sadrži a . a se zove *generator podgrupe*.

Definicija 24 Za grupu (G, \bullet) kažemo da je *ciklička grupa* ako postoji $a \in G$ takav da je $G = \langle a \rangle$. a je generator grupe. Ciklička grupa je uvijek komutativna jer je svaki $x \in G$ oblika $x = a^k$, i vrijedi propozicija.

Teorem 18 (*Lagrange*)

1. Red *elementa* je uvijek djelitelj reda grupe.
2. Red *podgrupe* je uvijek djelitelj reda grupe.

Primjer 7.1 Neka je $Z_n = \{0, 1, 2, 3, \dots, n-1\}$ $(Z_n, +_n)$ je Abelova grupa. Zbrajanje je definirano $(\text{mod } n)$.

7.2 Simetrične grupe

Definicija 25 Neka je X konačan skup. Permutacija skupa X je svako bijektivno preslikavanje $\alpha : X \rightarrow X$.

Neka je $|X| = n$, $X = \{1, 2, \dots, n\}$. Tada permutaciju možemo zapisati pomoću sheme, npr.:

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

Svaka permutacija se može napisati preko ciklusa (u ovom primjeru imamo 3 ciklusa).

Definicija 26 Permutacija skupa $S = \{1, 2, \dots, n\}$ u kojoj za elemente $\{b_1, b_2, \dots, b_k\} \subseteq S$ vrijedi $b_1 \rightarrow b_2 \rightarrow b_3 \dots b_{k-1} \rightarrow b_k \rightarrow b_1$, a svi ostali se preslikavaju u sami sebe, tj. $x \rightarrow x$ se zove *ciklus* i označava se (b_1, b_2, \dots, b_k) .

Teorem 19 Skup svih permutacija skupa $\{1, 2, \dots, n\}$ čini grupu uz standardnu operaciju kompozicije i tu grupu zovemo *simetrična grupa* nad n elemenata. Označava se sa S_n . Red grupe je $n!$, a red pojedinog elementa je najmanji zajednički višekratnik duljina njegovih ciklusa (svaka permutacija može se na jednoznačan način prikazati kao produkt disjunktnih ciklusa).

7.3 Prsteni i polja

Definicija 27 Uređenu trojku $(P, +, \bullet)$, gdje je P neprazan skup s dvije binarne operacije $+, \bullet : P \times P \rightarrow P$ zovemo *prsten* ako su ispunjeni slijedeći uvjeti:

1. $(P, +)$ je Abelova grupa
2. operacija množenja je asocijativna
3. vrijedi distributivnost: $a(b + c) = ab + ac$

Uz uvjet da postoji neutralan element za množenje (za zbrajanje već postoji jer je $(P, +)$ grupa) tako da je $xe = ex = x$ tada je P *prsten s jedinicom*, a ako je množenje komutativno, tada je i prsten komutativan. Npr. $(Z, +, \cdot)$ (skup cijelih brojeva) je komutativan prsten s jedinicom. Nije grupa s obzirom na množenje jer nema inverz za svaki element (npr. 2 nema svoj inverz u skupu Z).

Definicija 28 Uređenu trojku $(P, +, \bullet)$ koja se sastoji od nepraznog skupa P i dvije binarne operacije zovemo *polje* ako su ispunjeni uvjeti:

1. $(P, +)$ je Abelova grupa
2. $(P \setminus \{0\}, \bullet)$ je Abelova grupa (iz ovoga slijedi da svaki element ima multiplikativni inverz)
3. distributivnost

Npr. $(R, +, \cdot)$ je polje. I ovdje se, analogno kao kod grupa, definiraju *potprsten* i *potpolje*.

Definicija 29 Neka je R prsten. Ako postoji $n \in \mathbb{N}$ takav da je $\forall a \in R \quad na = a + a + \dots + a = 0$, onda najmanji takav n zovemo *karakteristikom prstena*. Ako takav n ne postoji, kažemo da je prsten karakteristike 0.

Definicija 30 Bilo koje *konačno* polje nazivamo *Galoisovo polje*. Konačna polja su uvijek reda p^n , p prost, n bilo kakav. Takva polja se označavaju $GF(p^n)$. Ona su uvijek karakteristike p .

Primjer 7.2 Konstrukcija polja s točno p^n elemenata. Uzmemo sve polinome stupnja $< n$ s koeficijentima iz prstena $(Z_p, +_p, \cdot_p)$. Elemente zbrajamo tako da ih zbrojimo kao što normalno zbrajamo polinome, a koeficijente rezultata zatim uzmemo \pmod{p} . Za množenje treba naći polinom stupnja n koji je *ireducibilan* nad Z_p (neka je to $Q(t)$). Dva polinoma prvo pomnožimo obično, zatim koeficijente uzmemo \pmod{p} , a zatim gledamo ostatak pri dijeljenju s $Q(t)$. Taj ostatak je rezultat množenja dva polinoma u polju.

8 SNBR stroj

Primjer 8.1 Ima li za zadani $n \in \mathbb{N}$ broj $\sqrt{2}$ igdje n uzastopnih petica iza decimalne točke? Neka je $f(n) = 1$ ako ima, inače $f(n) = 0$. Kako izračunati f ako je n jako velik? Nije poznato da li je f izračunljiva, ali se pretpostavlja da nije.

Pojam izračunljive funkcije može se točno uvesti pomoću stroja s neograničenim brojem registara (SNBR). SNBR stroj sastoji se od beskonačne trake koja sadrži registre R_1, R_2, \dots od kojih svaki sadrži prirodan broj ili 0. Registre označavamo velikim slovom R , a sadržaj registra malim slovom. Tako registar R_1 sadrži vrijednost r_1 . Svako stanje na traci u nekom trenutku se naziva *konfiguracija*. Sadržaj registara u početnom trenutku je zadan, a mijenja se pomoću programa. *Program* je konačan niz instrukcija, a svaka od njih ima jedan od slijedećih oblika:

1. Nul instrukcija $Z(n)$. Postavlja n -ti registar na 0: $R_n \leftarrow 0$
2. Instrukcija sljedbe $S(n)$. Uvećava R_n za 1: $R_n \leftarrow r_n + 1$
3. Instrukcija transfera: $T(m, n)$: $R_n \leftarrow r_m$. Dozvoljena je instrukcija $T(n, n)$ koja ne mijenja stanje na traci.
4. Instrukcija uvjetnog skoka $J(m, n, q)$. Ako je $r_m = r_n$ onda stroj prelazi na izvršavanje q -te instrukcije u programu P , a inače prelazi na slijedeću instrukciju. Instrukcija $J(n, n, q)$ je bezuvjetan skok.

1, 2 i 3 su *aritmetičke* instrukcije. One nisu nezavisne: transfer se može opisati pomoću preostale 3 instrukcije:

I1: $Z(n)$
 I2: $J(m, n, 5)$
 I3: $S(n)$
 I4: $J(n, n, 2)$

Zaustavljanje programa P od s instrukcija je moguće realizirati na tri načina:

1. Ako je posljednja s -ta instrukcija aritmetička
2. Ako je I_k instrukcija skoka $J(m, n, q)$ uz $r_m = r_n$ i $q > s$.
3. $I_s = J(m, n, q)$, $r_m \neq r_n$

Moguće je da za neku početnu konfiguraciju izvedba programa P upadne u petlju tako da se nikad ne završi. To označavamo sa $P(a_1, a_2, \dots) \uparrow$. Ako izvršenje programa na početnoj konfiguraciji završava u konačno mnogo koraka, to označavamo sa $P(a_1, a_2, \dots) \downarrow$

Definicija 31 Neka su P i Q programi duljina s i t . *Spoj* ili *konkatenacija* programa P i Q se označava s PQ koji se sastoji od instrukcija $\underbrace{I_1, \dots, I_s}_P, \underbrace{I_{s+1}, \dots, I_{s+t}}_Q$ uz izmjenu svih naredbi u P

$J(m, n, q)$, $q > s + 1$ u $J(m, n, s + 1)$ te izmjenu svih naredbi u Q $J(m, n, q)$ u $J(m, n, q + s)$.

Definicija 32 Neka je zadana funkcija $f : D(f) \rightarrow N_0$ pri čemu je $D(f) \subseteq N_0^n$ (uređena n -torka). Neka je P program, (a_1, \dots, a_n) iz domene, $b \in N_0$.

1. Kažemo da proračun $P(a_1, \dots, a_n)$ *konvergira* prema b ako $P(a_1, \dots, a_n) \downarrow$ i u konačnoj konfiguraciji se b nalazi u R1.
2. Kažemo da P *izračunava* f ako za sve (a_1, \dots, a_n) i za svaki b vrijedi $P(a_1, \dots, a_n) \downarrow b$ (konvergira prema b) $\Leftrightarrow (a_1, \dots, a_n \in D(f) \text{ i } f(a_1, \dots, a_n) = b)$.
3. $f : D(f) \rightarrow N_0$ je *SNBR izračunljiva* ako postoji program P koji izračunava f .

Teorem 20 Slijedeće funkcije su SNBR izračunljive:

1. nul-funkcija
2. funkcija sljedbe
3. funkcija projekcije
4. zbrajanje

Izračunljivost funkcije se može dokazati tako da se napravi program koji izračunava f .