Osnove programiranja v diskretni matematiki
Zapiski predavanj

2023/24

Povzetek

Dokument vsebuje zapiske predavanj predmeta Osnove programiranja v diskretni matematiki profesorja Taranenka v okviru študija prvega letnika magistrskega študija matematike na FNM.

Kazalo

1 Relacije

Definicija 1: Relacija R iz množice A v množico B je podmnožica kartezičnega produkta $A \times B$: $R \subseteq A \times B$. Če je $(a, b) \in R$ pišemo aRb, sicer pa $\neg(aRb)$ ali $a \not R b$. Relaciji $R \subseteq A \times A$ pravimo relacija na množici A.

Zgled 1: $\forall i \in \{1, 2, 3, 4, 5\} : R_i \subseteq \mathbb{Z} \times \mathbb{Z}$

i) $R_1 = \{(a, b);\ a \leq b\}$

ii) $R_2 = \{(a, b);\ a > b\}$

iii) $R_3 = \{(a, b);\ a = b \vee a = -b\}$

iv) $R_4 = \{(a, b);\ a = b\}$

v) $R_5 = \{(a, b);\ a + b \leq 3\}$

Zgled 2: Koliko je možnih relacij na množici z $n \in \mathbb{N}$ elementi? Odgovor: 2^{n^2}.

Definicija 2: Naj bo A poljubna množica in R relacija na njej. Relacija R je:

a) Refleksivna, če velja: $\forall a \in A : aRa$.

b) Irefleksivna, če velja: $\forall a \in A : a \not R a$.

c) Simetrična, če velja: $\forall a, b \in A : aRb \Rightarrow bRa$.

d) Asimetrična, če velja: $\forall a, b \in A : aRb \Rightarrow b \not R a$.

e) Antisimetrična, če velja: $\forall a, b \in A : aRb \wedge bRa \Rightarrow a = b$.

f) Tranzitivna, če velja: $\forall a, b, c \in A : aRb \wedge bRc \Rightarrow aRc$.

g) Intranzitivna, če velja: $\forall a, b, c \in A : aRb \wedge bRc \Rightarrow a \not R c$.

h) Sovisna, če velja: $\forall a, b \in A; a \neq b : aRb \vee bRa$.

i) Strogo sovisna, če velja: $\forall a, b \in A : aRb \vee bRa$.

Zgled 3: Oglejmo si relacije $R_i \subseteq \mathbb{Z} \times \mathbb{Z}$ iz zgleda 1 in jim določimo lastnosti, ki smo jih ravnokar definirali.

Rešitev:

i) R_1 je refleksivna, antisimetrična, tranzitivna ter strogo sovisna.

ii) R_2 je irefleksivna, asimetrična, tranzitivna ter sovisna.

iii) R_3 je refleksivna, simetrična ter tranzitivna.

iv) R_4 je refleksivna, simetrična ter tranzitivna.

v) R_5 je simetrična.

Zgled 4: Navedimo primer relacije, ki je hkrati simetrična in antisimetrična: $R = \{(x, x); x \in \mathbb{R}\}$.

2 Delna in linearna urejenost

Definicija 3: Relacija $R \subseteq A \times A$ je delna urejenost, če je refleksivna, antisimetrična in tranzitivna. Paru (A, R) pravimo delno urejena množica.

Zgled 5: Naštejmo nekaj primerov delno urejenih množic:

- (Družina podmnožic, $\subseteq$)
- $(\mathbb{R}, \leq)$
- $(\mathbb{N}, |)$

Definicija 4: Naj bo $(A, \leq)$ delno urejena množica. Elementa $a, b \in A$ sta primerljiva, če velja $a \leq b$ ali $b \leq a$, sicer sta pa neprimerljiva.

Definicija 5: Relacija $R \subseteq A \times A$ je linearna urejenost, če je delna urejenost in strogo sovisna. Paru (A, R) pravimo linearno urejena množica oz. veriga.

Opomba 1: Zgornjo definicijo lahko prebesedimo: Relacija (A, R) je linearno urejena množica $\iff$ $(A, \leq)$ je delno urejena množica in poljubni par elementov $a, b \in A$ je primerljiv.

Izrek 1. *Naj bo $(A, \leq)$ delno oz. linearno urejena množica in $B \subseteq A$. Potem je zožitev relacije $\leq$ na B tudi delna oz. linearna urejenost. Oznaka: $\leq_B = \{(a, b);\ a, b \in B \wedge a \leq b\}$*

Dokaz.

1. Naj bodo $a, b, c \in B$ poljubni elementi. Ker je $a \in B$, je tudi $a \in A$ in velja $a \leq a$. Sledi, da je $a \leq_B a$.
2. Če sta $a, b \in B$, sta tudi $a, b \in A$. Denimo, da velja $a \leq_B b$ in $b \leq_B a$. Potem je tudi $a \leq b$ in $b \leq a$, torej je $a = b$.
3. Naj bo $a \leq_B b$ in $b \leq_B c$. Potem je $a \leq b$ in $b \leq c$, torej je $a \leq c$ in posledično je $a \leq_B c$
4. Ker za poljubna $a, b \in B$ velja $a \leq b \vee b \leq a$, sledi $a \leq_B b \vee b \leq_B a$.

□

Zgled 6: Naj bo $\mathcal{D} = \mathcal{P}(\mathbb{Z})$ in vzemimo za relacijo $\subseteq$. Hitro vidimo, da je $(\mathcal{D}, \subseteq)$ veriga. Naj bo $\mathcal{A} = \{\{1, 2, \ldots, n\};\ n \in \mathbb{N}\}$. Potem je $(\mathcal{A}, \subseteq_{\mathcal{A}})$ veriga v $\mathcal{D}$.

Definicija 6: Naj bo $(A, \leq)$ delno urejena množica. Element $a \in A$ je:

- minimalni element, če velja: $\forall b \in A : b \leq a \Rightarrow b = a$
- najmanjši element oz. prvi element, če velja: $\forall b \in A : a \leq b$
- maksimalni element, če velja: $\forall b \in A : a \leq b \Rightarrow b = a$
- največji element oz. zadnji element, če velja: $\forall b \in A : b \leq a$

Navedimo nekaj primerov.

Zgled 7:

$(\mathbb{N}, |)$: 1 je hkrati minimalni in prvi element, ni minimalnega in ni zadnjega elementa.

$(\mathbb{R}, \leq)$: Nima niti minimalnega, niti maksimalnega, niti prvega niti zadnjega elementa.

$(\mathbb{N} \setminus \{1\}, |)$: minimalni elementi so vsa praštevila. Nima niti prvega element niti minimalnega niti zadnjega elementa.

Izrek 2. *Naj bo $(A, \leq)$ delno urejena množica.*

1. *Če obstaja prvi ali zadnji element, je enoličen.*
2. *Če je $a \in A$ prvi (oz. zadnji) element, je tudi edini minimalni (oz. maksimalni) element.*
3. *Če je A končna, potem vedno obstaja vsaj en minimalni oz. vsaj en maksimalni element.*

Dokaz. 1. Denimo, da imamo dva različna prva elementa: $a, b \in A; a \neq b$. Ker je a prvi element je $a \leq b$ in ker je b prvi element je $b \leq a$. Posledično, ker je $\leq$ antisimetrična, je $a = b$, kar pa nas privede v protislovje.

2. Denimo, da je $a \in A$ prvi element. Naj bo $b \in A$ minimalni element. Ker je a prvi element velja $a \leq b$ in ker je b minimalni element posledično velja $b = a$.

3. To točko bomo pokazali z indukcijo na $|A|$.

$|A| = 1$: Ta primer je trivialen - trditev očitno velja v tem primeru.

$|A| = n$: Denimo, da trditev velja za množice moči $n-1$. BŠS denimo, da ima vsaka množica moči $n-1$ vsaj en minimalni element. Naj bo $a \in A$ poljuben element in označimo $\acute{A} = A \setminus \{a\}$. Po indukcijski predpostavki, ima $\acute{A}$ minimalni element $b \in \acute{A}$. Obravnavamo primere:

- Če je $a \leq b$, je a minimalni element v A.
- Če je $b \leq a$, je b minimalni tudi v A.
- Če a in b nista primerljiva je b minimalni element v A.

□

Izrek 3. *Naj bo $(A, \leq)$ linearno urejena množica.*

i) $a \in A$ je prvi element $\iff$ a je minimalni element

ii) $a \in A$ je zadnji element $\iff$ a je maksimalni element

Dokaz. i) Denimo, da je $a \in A$ prvi element. Potem je, po prejšnjem izreku, a edini minimalni element. Obratno, denimo da je a minimalni element. Ker je $\leq$ strogo sovisna, velja $\forall b \in A : b \leq a \vee a \leq b$. Denimo, da je $b \leq a$. Ker je a minimalni element, sledi $b = a$. Torej $\forall b \in A : a \leq b$ oz. a je prvi element.

ii) Naj bo $a \in A$ zadnji element. Potem po prejšnjem izreku velja, da je a edini maksimalni element. Denimo sedaj, da je a maksimalni element. Zaradi stroge sovisnosti $\leq$ je $\forall b \in A : a \leq b \vee b \leq a$. Denimo, da za nek $b \in A$ velja $a \leq b$. Ker je a maksimalni element je potem $b = a$. Sledi torej, da $\forall b \in A$ velja $b \leq a$, torej je a zadnji element.

□

Posledica 1. *Naj bo $(A, \leq)$ linearno urejena množica. Če obstaja prvi (ali zadnji) element, je enoličen.*

Posledica 2. *Vsaka končna linearno urejena množica vsebuje natanko en prvi in natanko en zadnji element.*

Od zdaj naprej se bomo pretežno ukvarjali s končnimi množicami. Kadar bomo rekli, da je množica urejena, bomo s tem mislili linearno urejenost.

Definicija 7: Naj bo $(A, \leq)$ linearno urejena množica in A končna. Tak $(A, \leq)$ imenujemo abeceda. Beseda dolžine n nad $(A, \leq)$ je n-terica $b = (b_1, b_2, \ldots, b_n) = b_1 b_2 \ldots b_n$, kjer je $b_i \in A \ \forall i \in \{1, 2, \ldots, n\}$.

Definicija 8: Naj bo a beseda dolžine n in b beseda dolžine $m; n \leq m$ nad abecedo $(A, \leq)$. Potem je $a \leq_{LEX} b$, če velja:

- $\forall i \in \{1, 2, \ldots n\} : a_i = b_i$, ali
- $\exists j \in \{1, 2, \ldots, n\} : \forall i \in \{1, 2, \ldots, j-1\} a_i = b_i \ \& \ a_j \leq b_j$

Očitno je leksikografska urejenost besed $\leq_{LEX}$ linearna urejenost.

3 Generiranje kombinatoričnih objektov

Naj bo A neka končna množica. Pogosto potrebujemo učinkovite algoritme za generiranje:

- Vseh podmnožic množice A
- Vseh podmnožic dolžine k množice A
- Vseh permutacij elementov množice A

V vseh primerih bomo obravnavali ureditev, ki jo naravno porodi leksikografska ureditev ter ureditev najmanjše spremembe. Pri tem bomo govorili o naslednjih operacijah:

Rangiranje: $Rang : S \to \{0, 1, \ldots, |S| - 1\}$ je bijekcija, ki vsakemu objektu $s \in S$ določi njegov položaj v ureditvi. Velja torej: $a \leq b \iff Rang(a) \leq Rang(b)$

Derangiranje: $Derang : \{0, 1, \ldots, |S| - 1\} \to S$ je bijektivni inverz preslikave $Rang$, ki vsaki poziciji v ureditvi $i \in \{0, 1, \ldots, |S| - 1\}$ določi pripadajoč objekt. Velja: $\forall a \in S, \forall r \in \{0, 1, \ldots |S| - 1\} : Rang(a) = r \iff Derang(r) = a$

Naslednik: $Naslednik : S \to S \cup \{nedefinirano\}$ je preslikava s predpisom $\forall s \in S : Naslednik(s) = \begin{cases} Derang(Rang(s) + 1) & ; \ rang(s) < |S| - 1 \\ nedefinirano & ; \text{ sicer} \end{cases}$ Velja: $\forall s \in S : Naslednik(s) = t \neq nedefinirano \iff Rang(t) = Rang(s) + 1$

3.1 Določanje vseh podmnožic

Brez škode za splošnost recimo, da je $A = \{1, 2, \ldots, n\} = [n]$ in $\mathcal{A} = \mathcal{P}(A)$. Potem lahko vsaki podmnožici $T \in \mathcal{A}$ določimo t. i. karakteristični vektor $\chi(T)$ dolžine n s predpisom $\chi(T) = (X_{n-1}, \ldots, X_1, X_0); X_i = \begin{cases} 0 & ; \ n-i \notin T \\ 1 & ; \ n-i \in T \end{cases}$.

3.1.1 Urejenost porojena z leksikografsko

Definicija 9: Naj bo $A = [n]$. Leksikografska urejenost $\mathcal{A} = \mathcal{P}(A)$ je tista urejenost, ki je porojena z leksikografsko ureditvijo pripadajočih karakterističnih vektorjev $\chi(T); T \in \mathcal{A}$.

Zgled 8: Poglejmo si leksikografsko ureditev od $\mathcal{P}(\{1, 2, 3\})$.

T	$\chi(T)$	$Rang(T)$
$\emptyset$	000	0
$\{3\}$	001	1
$\{2\}$	010	2
$\{2, 3\}$	011	3
$\{1\}$	100	4
$\{1, 3\}$	101	5
$\{1, 2\}$	110	6
$\{1, 2, 3\}$	111	7

Opazimo, da leksikografska ureditev $\mathcal{A}$ sovpada z naraščujočo ureditvijo binarno predstavljenih pripadajočih rangov. Navedimo sedaj algoritme za $Rang$, $Derang$ in $Naslednik$ za podmnožice:

- Za $Rang$:

Data: $n \in \mathbb{N}$ in podmnožica $T \in \mathcal{P}([n])$
Result: $r = Rang(T)$
$r = 0$
for $i \in \{n, n-1, \ldots, 1\}$ **do**
  if $i \in T$ **then**
    $r = r + 2^{n-i}$
  end
end
return r

Algoritem 1: Algoritem $LexRangPodmnožice(n, T)$

- Za $Derang$:

Data: $n \in \mathbb{N}$ in rang $r \in \{0, 1, \ldots, n-1\}$
Result: množica $T \in \mathcal{P}([n])$, za katero je $Rang(T) = r$
$T = \emptyset$
for $i \in \{n, n-1, \ldots, 1\}$ **do**
  if $r \mod 2 \equiv 1$ **then**
    $T = T \cup \{i\}$
    $r = \lfloor \frac{r}{2} \rfloor$
  end
end
return T

Algoritem 2: Algoritem $LexDerangPodmnožice(n, r)$

Data: $n \in \mathbb{N}$ in podmnožica $T \in \mathcal{P}([n])$
Result: množica Nas, ki je naslednik množice T
$Nas = nedefinirano$
$r = LexRangPodmnožice(n, T)$

- Za $Naslednik$:

if $r < 2^n - 1$ **then**
  $Nas = LexDerangPodmnožice(n, r + 1)$
end
return Nas

Algoritem 3: Algoritem $LexNaslednikPodmnožice(n, T)$

V leksikografski ureditvi podmnožic se nam lahko zgodi, da sta dve zaporedni podmnožici zelo različni. To se zgodi v zgledu 3.1.1 na sredini tabele, kjer podmnožici $\{2, 3\}$ sledi njen komplement $\{1\}$. To nas motivira, da začnemo študirati ureditve v katerih se dva zaporedna elementa medseboj čim manj razlikujeta.

3.1.2 Ureditev z najmanjšo spremembo

Za začetek naredimo en primer na znani množici $\{1, 2, 3\}$.

Zgled 9: Zapiši karakteristične vektorje podmnožice množice $\{1, 2, 3\}$ tako, da se dva zaporedna razlikujeta v natanko enem mestu:

$$000 \leq 001 \leq 011 \leq 010 \leq 110 \leq 100 \leq 101 \leq 111$$

Definicija 10: Naj bo $A = \{1, 2, \ldots, n\}$ za nek $n \in \mathbb{N}$ in $\mathcal{A} = \mathcal{P}(A)$. Spomnimo se, da je za $T_1, T_2 \in \mathcal{A}$ simetrična razlika množic $T_1 \triangle T_2 = (T_1 \cup T_2) \setminus (T_1 \cap T_2)$. Potem količino $d(T_1, T_2) = |T_1 \triangle T_2|$ imenujemo Hemmingova razdalja med T_1 in T_2. Za $T_1 \neq T_2$ je $d(T_1, T_2) \geq 1$.

Opomba 2: Opazimo, da je $d(T_1, T_2)$ ravno enaka številu bitov, v katerih se $\chi(T_1)$ in $\chi(T_2)$ razlikujeta.

Definicija 11: Vsako ureditev vseh binarnih nizov dolžine n v kateri se dva zaporedna elementa razlikujeta v natanko enem bitu imenujemo Grayeva koda. Ena izmed njih je t. i. zrcaljena Grayeva koda. Označimo:
G^n = ureditev vseh binarnih nizov dolžine n v zrcaljeni Grayevi kodi,
$G^n = (G_0^n, G_1^n, \ldots, G_{2^n-1}^n)$. Zrcaljena Grayeva koda je definirana rekurzivno na naslednji način:

Data: Dolžina binarnih nizov $n_0 \in \mathbb{N}$
Result: Zrcaljena Grayeva koda G^{n_0}
$G_1 = (0, 1)$
for $n \in \{2, 3, \ldots, n_0\}$ **do**
  $G^n = (0G_0^{n-1}, 0G_1^{n-1}, \ldots, 0G_{2^{n-1}-1}^{n-1}, 1G_{2^{n-1}-1}^{n-1}, \ldots, 1G_1^{n-1}, 1G_0^{n-1})$
end
return G^{n_0}

Algoritem 4: Algoritem za zrcaljeno Grayevo kodo za bin. nize dolžine n_0.

Zgled 10: S tabelo prikažimo izvedbo algoritma 4 za $n_0 = 3$.

0	00	000
1	01	001
	11	011
	10	010
		110
		111
		101
		100

Izrek 4. *$\forall n \in \mathbb{N}$ je G^n Grayeva koda.*

Dokaz. Dokaz bomo izvedli z indukcijo po n.

$(n = 1)$: $G_1 = (0, 1)$, kar je očitno Grayeva koda.

$(n > 1)$: Denimo, da je G^k Grayeva koda $\forall k \in \{1, 2, \ldots, n-1\}$ in gledamo G_i^n ter G_{i+1}^n.

i) Denimo, da je $i \leq i + 1 \leq 2^{n-1} - 1$. Potem sta prva bita od G_i^n in G_{i+1}^n enaka in edina možna razlika se lahko pojavi pri gledanju zadnjih $(n-1)$ bitov. Torej $G_i^n = 0G_i^{n-1}$ in $G_{i+1}^n = 0G_{i+1}^{n-1}$ in edina razlika se lahko pojavi pri primerjanju G_i^{n-1} in G_{i+1}^{n-1}. Ta sta pa po indukcijski predpostavki razlikujeta v natanko 1 bitu.

ii) Denimo, da je $2^{n-1} - 1 < i < 2^n - 1$. Potem je $G_i^n = 1G_{i+1}^{n-1}$ in $G_{i+1}^n = 1G_i^{n-1}$ in edina razlika nastopi pri primerjavi G_i^{n-1} in G_{i+1}^{n-1}. Ta se pa po predpostavki razlikujeta v natanko 1 bitu.

iii) Denimo, da je $i = 2^{n-1} - 1$. Potem je $G_i^n = 0G_{2^{n-1}-1}^{n-1}$ in $G_{i+1}^n = 1G_{2^{n-1}-1}^{n-1}$ in G_i^n ter G_{i+1}^n se posledično razlikujeta v natanko enem bitu.

Torej $\forall i \in \{0, 1, \ldots, 2^n - 2\}$ velja, da se G_i^n in G_{i+1}^n razlikujeta v natanko enem bitu.

Potem je pa tudi G^n Grayeva koda. □