Diskretna matematika II - Zapiski predavanj

Amar Ustavdić

Vsebina

1 Uvod

1.1 Uporabna matematika (nekaj zgodovine)

a) Zgodovinsko (od Newtona in Leibniza):

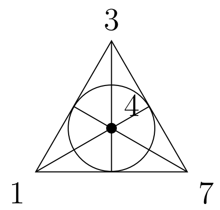
- temelji na <u>zvezno spreminjajočih se procesih</u>.
- motivirani predvsem z fizikalnimi aplikacijami.
- in študiranih z uporabo <u>analize</u> (diferencialni račun, integralni račun).

b) Z rastjo računalnikov in drugih digitalnih naprav:

- <u>diskretna matematika</u> postaja vse pomembnejša.
- diskretna matematika študira končne ali števno neskončne diskretne objekte
- Zajema številna področja matematike:
  - teorijo množic,
  - logiko,
  - kombinatoriko,
  - teorijo grafov,
  - teoretično računalništvo,
  - teorijo števil,
  - pa tudi (vsaj delno):
    - algebro,
    - operacijske raziskave,
    - terijo iger,
    - verjetnost,
    - statistiko.

Uporaba diskretne matematike v resničnem življenju (poleg računalnikov):

- organizacija sestankov,
- sestavljanje proizvodnih in šolskih urnikov,
- kriptografija,
- načrtovanje kod,
- oblikovanje prometnih, električnih in komunikacijskih omrežij,
- dodeljevanje zaposlenih na delovna mesta,
- oblikovanje glasovnih shem,
- načrtovanje poskusov (npr.: Recimo da imate kmetijo, pa želite preiskusit različna gnoila za zemljo, imate na voljo samo 3 njive, pa 7 različnih gnojil, kako jih boste zdej preiskusili katero je boljše. In potem lahko razvijete načrt kako boste to naredili na nek pošten način)



- v kemiji in biologiji (lasti bioinformatiki, v študiju sekvence DNA in filogenetiki),
- v razvedrilnih matematiki (Sudoku, Rubikova kocka, Hanoijski stolpi…)

Pri tem predmetu bomo obravnavali kombinatoriko pa teorijo grafov:

- reševanje problemov
- dokazovanje

1.2 Kaj je kombinatorika?

Kombinatorika se ukvarja z rasporejanjem predmetov v skladu s predpisanimi pravili:

- Prvič preučuje uprašanje ali je določena razporeditev sploh možna?
- Če je odgovor pritrdilen, na koliko različnih načinov?

Če so pravila preprosta (npr.: izbira nogometne ekipe iz razreda učencov je obstoj razporeditve jasen in se osredotočimo na problem štetja.)

Vendar za bolj zapletena pravila morda ne bo jasno, ali je razporeditev sploh mogoča. (npr.: Eulerjev problem časnikov.)

Včasih je podana tudi kriterijska funkcija, ki meri, kako dobra je neka razporeditev.
U tem primeru iščemo optimalne rešitve glede na kriterijsko funkcijo (npr.: poiščite tak razpored tekm nogometnega turnirja, da bo turnir trajal čim manj dni.)

1.3 Zgled kombinatoričnih problemov

1.3.1 Deranžmaji

Danih n pisem in n ovojni.
Na koliko načinov lahko pisma vstavite v ovojnice, da nobeno pismo ni v pravilnid ovojnici?

Diskusija:
Najprej se vprašamo na koliko načinov lahko damo n pisem v n ovojnic če ni nobenih omejitev? (vse je dovoljeno)

$$4 \cdot 3 \cdot 2 \cdot 1 = 4!$$
$$n! = n \cdot (n-1) \dots 1$$

Skupno število dajanja pisem v ovojnice je število vseh permutacij n objektov ki je $n!$.

Videli bomo da je delež premutacij, ki so nepravilno naslovljene, zelo blizu $\frac{1}{e}$, kjer je $e \approx 2,71828\ldots$ osnova naravnih logaritmov.

Presenetljiv rezultat na prvi pogled.

Iskaže se, da je število (deranžmajev) načinov napačnega naslavljanja pisem enako celemu številu, najbližjemu številu $\frac{n!}{e}$.

Domača naloga: Za $n = 4$ in $n = 5$ izračunajte število (deranžmajev) načinov razporeditev n pisem v ovojnice, tako da je vsako pismo napačno naslovljeno. Za vsak tak n izračunajte razmerje tega števila s številom $n!$.

1.3.2 Kirkumnove šolarke (na e-učilnici)

1.3.3 Eulerjevi častniki

To je pa ta zanimiv problem kjer se iskaže da ni preprosto ugotovit ali rešitev obstaja.
Opazimo da je Eulerjev problem zelo podoben Latinskemu kvadratu, samo da ni $n = 3$, ampak je $n = 6$.

Danih je 36 časnikov, ki pripadaju 6 polkom in imajo 6 činov (pri čemer vsaka kombinacija čina in polka samo enemu častniku). Ali je častnike mogoče razvrstiti v tako 6×6 formacijo tako da bo vsaki vrstici in v vsakem stolpcu natanko en častnik iz vsakega polka in natanko en častnik iz vsakega polka in natanko en častnik vsakega čina?

Problem je sestavil Euler leta 1782.
Vrejel je da je odgovor ne, kar pa je šele leta 1900 dokazal Taury.
Problem je mogoče posplošiti na n^2 častnikov, kjer je število polkov, činov, vrstic in stolpcev enako n.

$$n : 1, \textcolor{red}{2}, 3, 4, 5, \textcolor{red}{6}, 7, 8, 9, 10, 11, 12, 13, \ldots$$

Euler je pokazal rešitve za vsa števila n ki niso kongruentna 2 po modulu 4, in ugotovil da rešitev za $n \equiv 2 (\mathrm{mod}\ 4)$ ne obstaja.

$$a \equiv b (\mathrm{mod}\ k) \quad (k \in \mathbb{N}, a, b \in \mathbb{Z}) \text{ če } k | a - b$$

Euler se je glede tega motil. Trije matematiki, Bose, Shirikande in Parker so leta 1960 pokazali, da obstaja rešitev za vse n razen za 2 in 6.

Domača naloga: Rešite problem za 16 in 25 častnikov.

1.3.4 Ramseyjeva igra

Igra dveh igralcev ki zahteva list papirja in svinčnik dveh barv, npr.: rdečega pa zelenega. Izberemo 6 točk na papirju, tako da nobene 3 niso na skupni premici in igralca vzameta svinčnika in izmenjojoče z daljico povežeta dve izmed izbranih točk. In igralec ki prvi nariše trikotnik svoje barve izgubi (štejejo samo trikotniki z oglišči v izbranih točkah).

Ali se lahko igra konča z neodločenim izidom (da nihče ne izgubi)?

Diskusija:
Iskaže se, da neodločen izid ni mogoč, saj eden igralc bo prisiljen vstvariti trikotnik.

Remzi je dokazal široko posplošitev tega dejstva. Njegov izrek se včasih zapiše v obliki "Popoln nered je nemogoč."

Domača naloga: Igrajte to igro s prijatelji in preverite da nedoločen izid ni mogoč.

2 Osnovna kombinatorična načela

Če želimo prešteti neke objekte s predpisanimi lastnostmi, to lahko storimo v dveh delih:

- najprej objekte ki jih preštevamo, združimo jih v neko natančno opisano množico
- nato pa tej množici določimo moč

2.1 Definicija

Pravimo da končna množica X vsebuje n elementov, če obstaja bijekcija iz množice X v množico $\{1, 2, 3, \ldots, n\}$. U tem primeru pištemo $|x| = n$ in rečemo da je moč množice X enaka n. Prazno množico obravnavamo posebej in postavimo $|\emptyset| = 0$.

Pri določanju moči množice si pomagamo z nekaj preprostimi načeli.

2.2 Izrek (načelo vsote)

Če sta A in B končni disjunktni množici potem velja $|A \cup B| = |A| + |B|$.

S pomočjo matematične indukcije načelo vsote posplošimo na končno unijo paroma disjunktnih končnih množic.

Če so $A_1, A_2, \ldots, A_n$ končne in paroma disjunktne množice (tj. $A_i \cap A_j = \emptyset$ za $i \neq j$), potem velja naslednje

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

oziroma

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i|$$

2.3 Zgled

Od mesta X do mesta Y lahko pridemo z letalom, vlakom ali avtobusom. Med X in Y je 12 različnih letalskih poletov, 5 različnih vlakov in 10 različnih avtobusov. Koliko različnih množic imamo, da pridemo iz X v Y?

Izberemo lahko le en način prevoza.
In za vsak način imamo izbiro: $12 + 5 + 10 = 27$

2.4 Izrek (načelo enakosti)

Če obstaja bijekcija med dvema končnima množicama A in B, potem je $|A| = |B|$.

2.5 Zgled

Naj bo X množica z n elementi:
Koliko podmnožic premore X?

Naloga sprašuje po moči potenčne množice $P(X)$ množice X. (2^X)
Rešimo jo tako da poiščemo bijekcijo med množico $P(X)$ in množico vseh narejenih n-teric z elementi iz množice $\{0, 1\}$
Označimo elemente množice X z $X_1, X_2, \ldots, X_n$.
Poljubni množici $Y \in P(X)$ priredimo $\chi(Y) = (Y_1, Y_2, \ldots, Y_n) \in \{0, 1\}^n$ za katerega je

$$y_i = \begin{cases} 1; & \text{če } x_i \in Y \\ 0; & \text{sicer} \end{cases}$$

Na ta način smo definirali preslikavo

$$\chi : P(X) \to \{0, 1\}^n$$

Ta preslikava je bijektivna. Zato je

$$|P(X)| = |\{0, 1\}^n| = 2^n$$

2.6 Načelo dvojnega preštevanja

Če isto množico preštejemo na dva različna načina, potem sta odgovora enaka.

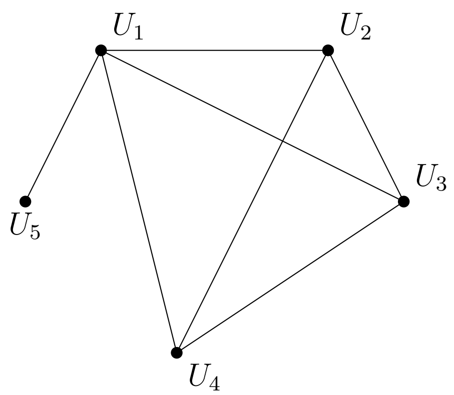
Učasih se imenuje tudi "računovodsko načelo".

Načelo je analogno iskanju vsote vseh elentov v matriki tako, da seštejete vsote vseh vrstic, nato pa raun preverite tako da seštejete vsoto stolpcev.

2.7 Zgled (uporabe načela dvojnega preštevanja)

2.7.1 Lema (lema o rokovanju)

Na kongresu je število vseh vdeležencev ki se rokojejo liho mnogokrat, sodo.



$U_1 : U_2, U_3, U_4, U_5$	$x_1 = 4$	$y = 7$ (skupno število rokovanj)
$U_2 : U_1, U_3, U_4$	$x_2 = 3$	
$U_3 : U_2, U_1, U_4$	$x_3 = 3$	
$U_4 : U_1, U_2, U_3$	$x_4 = 3$	
$U_5 : U_1$	$x_5 = 1$	

2.7.2 Dokaz

Naj bodo od $U_1, \ldots, U_n$ udeleženci kongresa. Načelo dvojnega preštevanja bomo uporabili na množici urejenih parov (U_1, U_j), za katere se udeleženca U_i in U_j rokojeta. Naj bo x_i število udeležencev s katerimi se je U_i rokoval in y skupno število rokovanj.

Po eni strani je to število parov enako:

$$\sum_{i=1}^{n} x_i$$

saj je za vsak U_i število izbir enako x_i.

Po drugi strani pa vsako rokovanje poredi natanko dva para:

$$(U_i, U_j) \text{ in } (U_j, U_i)$$

skupno število parov je tako $2y$.

Torej velja:

$$\sum_{i=1}^{n} x_i = 2y$$

$$4 + 3 + 3 + 3 + 1 = 14$$

Če pa je vsota n celih števil sodo število lihih sumandov sodo.

Načelo se navadno uporablja za štetje urejenih parov.

2.7.3 Izrek

Naj bosta $A = \{a_1, \ldots, a_m\}$ in $B = \{b_1, \ldots, b_n\}$ množici in naj bo $S \subseteq A \times B$.
Naj bo za vse $i = 1, \ldots, n$ element a_i prva koordinata x_i parov množice S, medtem ko je za vse $j = 1, \ldots, n$ element b_j druga koordinata y_j parov množice S. Tedaj velja:

$$|S| = \sum_{i=1}^{m} x_i = \sum_{j=1}^{n} y_j$$

2.7.4 Zgled

$$A = \{1, 2, 3\} \; B = \{u, v\}$$

$$A \times B = \{(1, u), (1, v), (2, u), (2, v), (3, u), (3, v)\}$$

$$S = \{(1, u), (1, v), (2, u), (3, v)\}$$

$(1, u)$	$(1, v)$
$(2, u)$	
	$(3, v)$

2.7.5 Posebni primer

x_i je konstanta, npr. x in tudi y_i je konstanta, npr. y, potem je:

$$|S| = m \cdot n = n \cdot y$$

2.8 Načelo produkta

Poseben primer načela dvojnega preštevanja je:

2.8.1 Izrek

Če sta A in B končni množici, potem velja:

$$|A \times B| = |A| \cdot |B|$$

2.8.2 Dokaz

Uporabimo prejšnji izrek z množicama A in B kot v izreku, $S = A \times B$ in $x_i = |B|$ za vse $i = 1, \ldots, n$. Torej velja:

$$|A \times B| = |S| = m \cdot |B| = |A| \cdot |B|$$

S pmočjo matematične indukcije načelo produkta posplošimo na kartezični produkt poljubnega števila množic $A_1, \ldots, A_n$:

$$|A_1 \times ... \times A_n| = |A_1| \ldots |A_n| = \prod_{i=i}^{n} |A_i|$$

2.8.3 Zgled

Koliko je vseh različnih 8-bitnih nizov? Iskani nizi so elementi množice $\{0,1\}^8$.
Vsakega izmed bitov lahko izrazimo na dva načina (0 ali 1) od DOPOLNI po načelu produkta sledi, da DOPOLNI natanko:

$$|\{0,1\}|^8 = 2^8 = 256 \quad \text{(8-bitnih nizov)}$$

2.8.4 Zgled

Študentska restavracija streže 3 vrste predjedi (P), 6 glavnih jedi (G) in 5 sladic (S). Koliko različnih kosil si lahko sestavi študent? Kosilo opišemo kot element množice:

$$P \times G \times S$$

različnih kosil pa je potem: $3 \cdot 6 \cdot 5 = 90$.

2.9 Dirichletovo načelo (načelo golobnjaka)

Predpostavimo, da je jata golobov priletela v golobnjak. Če je več golobov kot je hišic v golobnjaku, potem bomo vsaj v eni hišici našli vsaj dva goloba.

2.9.1 Izrek (Dirichletovo načelo)

Če $n+1$ ali več predmetov razporedimo v n škatli, potem imamo vsaj v eni škatli vsaj dva predmeta.

2.9.2 Dokaz

S protislovjem. Recimo, da je v vsaki škatli največ en predmet.

Potem zaključimo da je vseh predmetov največ n, kar je v protislovju s predpostavko, da imamo vsaj $n+1$ predmetov.

2.9.3 Zgled

i. Vsaki množici z več kot 12 osebami obstajata dve , ki imata rojstni dan v istem mescu. (škatle predstavljajo mesece)

ii. V vsaki množici z več kot 366 osebami obstajata dve, ki imata rojstni dan, na isti dan. (škatle predstavljajo dneve)

iii. Za vsako naravno število n obstaja večkratnik tega števila katerega lahko zapišemo samo s pomočjo cifer 0 in 1.

n	
1	1
2	10
3	111
4	100
6	1110

Naj bo n naravno število. Poglejmo si naslednje zaporedje naravnih števil:

$$1, 11, 111, \ldots, \underbrace{111\ldots1}_{n}$$

p	p mod 6
1	1
11	5
111	3
1111	1
11111	5
111111	3

Če je kakšno izmed njih deljivo z n je problem rešen. V nasprotnem primeru da vsako izmed teh števil pri deljenju z n enega od $n-1$ možnih ostankov $1, \ldots, n-1$. Kar je v zaporedju n števil, po **Dirichletovom načelu** obstajata dve števili v zaporedju, na primer:

$$\underbrace{11\ldots1}_{k} \text{ in } \underbrace{11\ldots1}_{l}, \qquad k < l$$

ki data isti ostanek pri deljenju z n. Potem pa je njuna razlika:

$$\underbrace{11\ldots1}_{l-k}\underbrace{0\ldots0}_{k}$$

deljiva z n.

iv. V skupini dveh ali več ljudi lahko vedno najdemo dva, ki imata v tej skupini enako število prijateljev. (predpostavimo, da je relacija prijateljstva simetrična: x je prijatelj z y natanko tedaj, ko je y prijatelj z x). Recimo, da skupino sestavlja n ljudi: Razporedimo, ljudi v prostoru glede na to koliko prijateljev imajo.

Število prostorov = številu ljudi (in ne moremo na začetku uporabiti Dirichletovega načela), vendar pa opazimo da je vsaj eden od prostorov vedno prazen, če prostor $n-1$ ni prazen, potem obstaja oseba x, ki ima $n-1$ prijateljev, torej je vsaka oseba prijatelj z osebo x in zato ne obstaja oseba, ki ima 0 prijateljev. Torej je n oseb razporejenih v $n-1$ prostorov. Po Dirichletovem načelu obstajata vsaj dve osebi, ki se nahajata v istem prostoru, in imata torej enako število prijateljev.

2.10 Izrek (posplošeno Dirichletovo načelo)

Če m predmetov razporedimo v n škatel in velja da je:

$$m > k \cdot n$$

potem imamo vsaj v eni škatli vsaj $k+1$ predmetov.

OPOMBA: Neenakost je najboljša možna. Če je $m = k \cdot n$, lahko vsaka od n škatel vsebuje natanko k objektov.

2.10.1 Zgled

i.

$$\begin{array}{cl} \heartsuit & 1, \ldots, 13 \\ \diamondsuit & 1, \ldots, 13 \\ \clubsuit & 1, \ldots, 13 \\ \spadesuit & 1, \ldots, 13 \end{array}$$

Najmanj koliko kart moramo izvleči iz standardnega kompleta 52 kart, da bodo med izvlečenimi kartami gotovo štiri karte iste barve (4 $\heartsuit$ ali 4 $\diamondsuit$ ali 4 $\clubsuit$ ali 4 $\spadesuit$)?

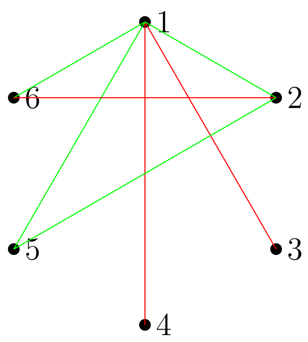
$$\begin{aligned} \text{predmeti} &= \text{karte} \quad k+1 = 4 \\ \text{škatle} &= \text{barve} \quad k = 3 \end{aligned}$$

Predpostavimo da imamo 4 škatle, vsako rezerviramo z posamezno barvo. Ko karto izvlečemo, jo damo v pripadajočo škatlo. Iz posplošenega Drirchletovega načela vidimo, da je dovolj izvleči:

$$13 \quad (= 3 \cdot 4 + 1)$$

kart, da bodo med izvlečenimi kartami gotovo štiri iste barve.

ii. V množici šestih oseb vedno obstajajo tri osebe ki se poznajo med sabo, ali pa obstajajo tri osebe, ki se ne poznajo med sabo.



Naj bo a poljubno izbrana oseba iz množice.
Razdelimo naslednjih 5 oseb v dva prostora.

Ker je $5 > 2 \cdot 2$, po Dirichletovem načelu obstaja en prostor z vsaj 3 osebami.

Predpostavimo najprej, da so v prvem prostoru osebe b, c, d. Če se kakšni dve izmed teh oseb poznata med seboj, na primer b in c potem je $\{a, b, c\}$ podmnožica teh oseb ki se med seboj poznajo. V nasprotnem primeru pa se nobeni dve osebi iz podmnožice $\{b, c, d\}$ ne poznata. Primer, ko se ti osebi nahajajo v drugem prostoru, obravnavamo podobno.

3 Elementarna kombinatorika

3.1 Izbori

3.1.1 Zgled

Pri igri loto se v bobnu nahaja 39 kroglic, oštevilčenih s števili $1, \ldots, 39$. Organizator igre iz bobna zaporedoma šestkrat izvleče po eno kroglico. Na koliko načinov lahko to stori?

Odgovor je odvisen od razlage besede "način":

- ali naj kroglico, ki smo jo v posameznem koraku izvlekli vržemo v boben ali ne, in
- ali je vrstni red izblečenih kroglic pomemben ali ne.

Dve osnovni lastnosti pri izbiri sta:

1. <u>ponavljanje</u>:
   - izbori s ponavljanjem
   - izbori brez ponavljanja
2. <u>izbori</u>:
   - urejeni izbori (varijacija)
   - neurejeni izbori (kombinacija)

3.2 Vrejeni izbori s ponavljanjem

(izvlečene kroglice, v boben <u>vračamo</u>, in vrstni red je <u>pomemben</u>)

$$\underbrace{(1, 2, 1, 3, 12, 5)}_{\text{k - terica}}$$

3.2.1 Definicija

Naj bo N končna množica in $k \in \mathbb{N}$. Potem bomo urejeni k-terici $(a_1, \ldots, a_k)$ elementi množice N rečemo <u>urejen izbor reda k na množici N</u>. (lahko bi tukaj dodali da je <u>s ponavljanjem</u>, ampak samo če želimo to poudariti, sicer bomo to izpustili)

Množico vseh takih izborov označimo z $\overline{V}(N, k)$.

3.2.2 Zgled

Recimo da imamo množico $N = \{a, b, c\}$ in je $k = 4$, potem lahko en tak izbor predstavimo kot (a, c, c, b), in tak izbor lahko predstavimo tudi z funkcijo katera slika iz množice $1, \ldots, k$ v N, brez kakršnih koli omejitev.

$$(a, b, c, d) \equiv \boxed{\begin{array}{l} 1 \to a \\ 2 \to c \\ 3 \to c \\ 4 \to b \end{array}}$$

Opomba

Vzamemo k-terico $(a_1, \ldots, a_k)$ elementa množice N lahko razumemo tudi kot funkcijo ki slika iz množice $\{1, \ldots, k\}$ v množico N.

Ker množica $\overline{V}(N, k)$ vsebuje vse svoje n-terice.

Od tod iz načela produkta sledi:

3.2.3 Trditev

Naj bo N poljubna množica z n elementi in $k \in \mathbb{N}$. Tedaj je v množici $\overline{V}(N, k)$ natanko n^k izborov.

$$|\overline{V}(N, k)| = |N^k| = |N|^k = n^k$$

3.2.4 Zgled

Vsak vikend v februarju lahko obiščemo enega od 3 kinematografov. Koliko različnih zaporedij obiskov je možnih, pri čemer so ponovni obiski seveda dovoljeni?

Torej, imamo $K = \{K_1, K_2, K_3\}$ (kinematografov) in 4 vikenda, torej eden primer takega zaporedja obiskov bi bil npr. (K_2, K_1, K_1, K_3)

$$|\overline{V}(K, 4)| = |K|^4 = 3^4 = 81$$