Diskretne strukture UNI
izročki predavanj

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

Ljubljana, januar 2009

Kazalo

Izjavni račun

Izjava je stavek, ki je bodisi resničen bodisi neresničen.
Vsak stavek ni izjava:

- *Zapri vrata!*
- *Ta stavek ni resničen.*

Izjave

Zgledi osnovnih izjav:

- *Zunaj sije sonce.*
- *Peter sedi na vrtu.*

Zgledi sestavljenih izjav:

- *Če zunaj sije sonce, Peter sedi na vrtu.*
- *Peter sedi na vrtu in zunaj sije sonce.*
- *Ni res, da zunaj sije sonce.*

Izjave

Izjave delimo po *vsebini* na

- *resnične* (imajo vrednost 1) in
- *neresnične* (imajo vrednost 0)

ter *obliki* na

- *osnovne* (tudi *enostavne*) in
- *sestavljene*.

Izjavni vezniki

Izjave sestavljamo s pomočjo *izjavnih veznikov* (tudi *izjavnih povezav*, *logičnih veznikov*).
Izjavni vezniki so:

- *enomestni* (npr. *ne*)
- *dvomestni* (npr. *in*, *ali*, *če*. . . *potem*. . . , *niti*. . . *niti*. . .)
- *tromestni*,. . .

Izjavni vezniki

Resničnost sestavljene izjave je odvisna samo od resničnosti sestavnih delov. Zato izjavne veznike definiramo s pomočjo *resničnostnih tabel*.

- negacija $\neg$
- konjunkcija $\wedge$
- disjunkcija $\vee$
- implikacija $\Rightarrow$
- ekvivalenca $\Leftrightarrow$

Konjunkcija

Konjunkcija izjav A in B, označimo jo z $A \wedge B$, in beremo "*A in B*".

$A \wedge B$ je resnična n.t., ko sta obe izjavi A in B resnični. Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Negacija

Negacija izjave A, $\neg A$, beremo "*Ne A*".

$\neg A$ je resnična natanko tedaj, ko je A neresnična. Definirana je z naslednjo pravilnostno tabelo:

A	$\neg A$
0	1
1	0

Negacija je *enomestni* izjavni veznik.

Disjunkcija

Disjunkcija izjav A in B, označimo jo z $A \vee B$, in beremo "*A ali B*".

$A \vee B$ je resnična n.t., ko je vsaj ena od izjav A ali B resnična. Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Implikacija

Implikacija izjav A in B, označimo jo z $A \Rightarrow B$, in beremo
"*Iz A sledi B*" "*Če A potem B*" "*A implicira B*"

Izjavi A pravimo *antecedens* implikacije, izjavi B pa *konsekvens* implikacije $A \Rightarrow B$.
$A \Rightarrow B$ je neresnična samo v primeru, ko je izjava A resnična in izjava B neresnična.

Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Izjavni vezniki

Konjunkcija, disjunkcija, implikacija in ekvivalenca so *dvomestni* izjavni vezniki.

Ekvivalenca

Ekvivalenca izjav A in B, označimo jo z $A \Leftrightarrow B$, in beremo
"*A ekvivalentno B*"
"*A natanko tedaj, ko B*"
"*A , če in samo če B*".
$A \Leftrightarrow B$ je resnična n.t., ko imata obe izjavi A in B isto logično vrednost.
Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Dogovor o opuščanju oklepajev

Če ni z oklepaji drugače naznačeno, potem:

1. Negacija veže močneje kot konjunkcija, konjunkcija veže močneje kot disjunkcija, disjunkcija veže močneje kot implikacija in implikacija veže močneje kot ekvivalenca.
2. Istovrstni (dvomestni) vezniki vežejo od *leve proti desni*.

Izjavni izrazi

Osnovne izjave označujemo s črkami $p, q, r, \ldots$
Namesto o izjavah govorimo o *izjavnih izrazih*.

1. *Izjavni konstanti* 0 in 1, ki jima pravimo tudi *laž* in *resnica*, sta izjavna izraza.
2. *Izjavne spremenljivke* $p, q, r, \ldots$ so izjavni izrazi.
3. Če so $A_1, A_2, \ldots, A_n$ izjavni izrazi in je F n-mestni izjavni veznik, potem je $F(A_1, A_2, \ldots, A_n)$ izjavni izraz.

Tavtologija in protislovje

Izjavni izraz je *tavtologija*, če je resničen pri vseh naborih vrednosti izjavnih spremenljivk, ki v njem nastopajo.
Izjavni izraz je *protislovje*, če je neresničen pri vseh naborih vrednosti izjavnih spremenljivk, ki v njem nastopajo.
Izjavni izraz je *nevtralen*, če ni niti tavtologija niti protislovje.

Konstrukcijsko drevo in resničnostna tabela

Vsakemu izjavnemu izrazu pripada *konstrukcijsko drevo* in *resničnostna tabela*.

Enakovredni izjavni izrazi

Izjavna izraza A in B sta *enakovredna*, če imata pri vseh naborih vrednosti izjavnih spremenljivk enako vrednost.
V tem primeru pišemo $A \sim B$.

Enakovredni izjavni izrazi

Izrek

Izjavna izraza A in B sta enakovredna natanko tedaj, ko je izraz $A \Leftrightarrow B$ tavtologija.

Naloga

Poišči izjavni izraz s predpisano resničnostno tabelo:

p	q	r	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Zakoni izjavnega računa

Nekateri pari enakovrednih izjavnih izrazov imajo posebna imena. To so *zakoni izjavnega računa*.

Disjunktivna normalna oblika

Disjunktivna normalna oblika (DNO) izjavnega izraza A je izjavni izraz A_{DNO}, za katerega velja:

- $A \sim A_{DNO}$
- A_{DNO} je disjunkcija osnovnih konjunkcij.

Osnovna konjunkcija je konjunkcija izjavnih spremenljivk in/ali njihovih negacij.
A_{DNO} *lahko* zgradimo tako, da za vsak nabor pravilnostne tabele, pri katerem je izraz A resničen, pripravimo eno osnovno konjunkcijo. V njej nastopajo v tem naboru resnične spremenljivke in negacije v tem naboru lažnih spremenljivk.

Konjunktivna normalna oblika

Konjunktivna normalna oblika (KNO) izjavnega izraza A je izjavni izraz A_{KNO}, za katerega velja:

- $A \sim A_{KNO}$
- A_{KNO} je konjunkcija osnovnih disjunkcij.

Osnovna disjunkcija je disjunkcija izjavnih spremenljivk in/ali njihovih negacij.
A_{KNO} *lahko* zgradimo tako, da za vsak nabor pravilnostne tabele, pri katerem je izraz A neresničen, pripravimo eno osnovno disjunkcijo. V njej nastopajo v tem naboru lažne spremenljivke in negacije v tem naboru resničnih spremenljivk.

Polni nabori izjavnih veznikov

Družina izjavnih veznikov $\mathcal{N}$ je *poln nabor*, če za vsak izjavni izraz A obstaja enakovreden izjavni izraz B, ki vsebuje samo veznike iz $\mathcal{N}$.
$\{\neg, \wedge, \vee\}$ je poln nabor izjavnih veznikov.

Kdaj KNO in DNO

Trditev

Vsak izjavni izraz, ki ni protislovje, ima DNO.
Vsak izjavni izraz, ki ni tavtologija, ima KNO.

Posledica

Za vsak izjavni izraz A obstaja enakovreden izjavni izraz B, ki vsebuje samo veznike $\neg$, $\wedge$, $\vee$.

Polni nabori izjavnih veznikov

Nekaj drugih polnih naborov izjavnih veznikov:

$$\{\neg, \vee\}\ , \quad \{\neg, \wedge\}, \quad \{\neg, \Rightarrow\}\ , \quad \{0, \Rightarrow\}$$

Polni nabori izjavnih veznikov

Vprašanje:
Kako v praksi pokazati, da je nabor izjavnih veznikov $\mathcal{N}$ poln?

1. Izberemo znan poln nabor izjavnih veznikov $\mathcal{Z}$.
2. Vsak veznik iz znanega nabora $\mathcal{Z}$ izrazimo samo z uporabo veznikov iz $\mathcal{N}$.

Ekskluzivna disjunkcija

Ekskluzivna disjunkcija izjavnih izrazov A in B, označimo jo z $A \veebar B$, in beremo "*A ekskluzivni ali B*".

$A \veebar B$ je resnična n.t., ko je natanko eden od izjavnih izrazov A in B resničen.

Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \veebar B$
0	0	0
0	1	1
1	0	1
1	1	0

Velja tudi $A \veebar B \sim \neg(A \Leftrightarrow B)$

Še trije izjavni vezniki

- ekskluzivna disjunkcija $\veebar$
- Shefferjev veznik $\uparrow$
- Pierce-Lukasiewiczev veznik $\downarrow$

Shefferjev veznik

Shefferjev veznik povezuje dva izraza A in B, kar označimo z $A \uparrow B$. Shefferjevemu vezniku pravimo tudi veznik NAND.
$A \uparrow B$ je neresničen n.t., ko sta oba izjavna izraza A in B resnična.
Definiran je z naslednjo pravilnostno tabelo:

A	B	$A \uparrow B$
0	0	1
0	1	1
1	0	1
1	1	0

Velja tudi $A \uparrow B \sim \neg(A \wedge B)$

Pierce-Lukasiewiczev veznik

Pierce-Lukasiewiczev veznik povezuje dva izraza A in B, kar označimo z $A \downarrow B$. Pravimo mu tudi veznik NOR.
$A \downarrow B$ je resničen n.t., ko sta oba izjavna izraza A in B neresnična.
Definiran je z naslednjo pravilnostno tabelo:

A	B	$A \downarrow B$
0	0	1
0	1	0
1	0	0
1	1	0

Velja tudi $A \downarrow B \ \sim \ \neg(A \vee B)$

Kam jih uvrstimo po prednosti

Shefferjev in Pierce-Lukasiewiczev veznik vežeta tako močno kot konjunkcija.

$$A \uparrow B \wedge C \downarrow D \uparrow E$$

pomeni isto kot

$$((((A \uparrow B) \wedge C) \downarrow D) \uparrow E$$

Kam jih uvrstimo po prednosti

Ekskluzivna disjunkcija veže tako močno kot (navadna) disjunkcija.

$$A \vee B \veebar C \vee D$$

pomeni isto kot

$$((A \vee B) \veebar C) \vee D$$

Zakoni z novimi vezniki

ekskluzivna disjunkcija	$A \veebar B \sim \neg(A \Leftrightarrow B)$
	$A \veebar B \sim B \veebar A$
	$(A \veebar B) \veebar C \sim A \veebar (B \veebar C)$
Shefferjev veznik	$A \uparrow B \sim \neg(A \wedge B)$
	$A \uparrow B \sim B \uparrow A$
Pierceov veznik	$A \downarrow B \sim \neg(A \vee B)$
	$A \downarrow B \sim B \downarrow A$

Sklepanje v izjavnem računu

Predpostavke:	1.	*Ta žival ima krila ali pa ni ptič.*
	2.	*Če je ta žival ptič, potem leže jajca.*
	3.	*Ta žival nima kril.*
Zaključek:	4.	*Torej ta žival ne leže jajc.*

Ali je ta sklep pravilen?

Pravilen sklep

Zaporedje izjavnih izrazov $A_1, A_2, \ldots, A_n, B$ je *pravilen sklep* s *predpostavkami* $A_1, A_2, \ldots, A_n$ in *zaključkom* B, če je zaključek B resničen pri vseh tistih naborih vrednosti izjavnih spremenljivk, pri katerih so resnične vse predpostavke.

Pišemo: $A_1, A_2, \ldots, A_n \models B$

in beremo:
Iz predpostavk $A_1, A_2, \ldots, A_n$ logično sledi zaključek B.

Formalizacija

ta žival ima krila	...	k
ta žival je ptič	...	p
ta žival leže jajca	...	j

1.	$k \vee \neg p$
2.	$p \Rightarrow j$
3.	$\neg k$
4.	$\neg j$

Pravilen sklep

Izrek
$A_1, A_2, \ldots, A_n \models B$ *natanko tedaj, ko*
$\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$

Nepravilen sklep

Kako pokažemo, da sklep ni pravilen?

Poiščemo *protiprimer*, tj. nabor vrednosti izjavnih spremenljivk, pri katerem so vse predpostavke resnične, zaključek pa ne.

Pravila sklepanja

$A, A \Rightarrow B \models B$	*modus ponens* (MP)
$A \Rightarrow B, \neg B \models \neg A$	*modus tollens* (MT)
$A \vee B, \neg B \models A$	*disjunktivni silogizem* (DS)
$A \Rightarrow B, B \Rightarrow C \models A \Rightarrow C$	*hipotetični silogizem* (HS)
$A, B \models A \wedge B$	*združitev* (Zd)
$A \wedge B \models A$	*poenostavitev* (Po)
$A \models A \vee B$	*pridružitev* (Pr)

Pravilom sklepanja pravimo tudi *osnovni pravilni sklepi*.

Nepravilen sklep

Z izbiro nabora $k \sim 0$, $p \sim 0$ in $j \sim 1$ pridelamo:

$$\begin{array}{rcl} k \vee \neg p & \sim & 1 \\ p \Rightarrow j & \sim & 1 \\ \neg p & \sim & 1 \qquad \text{in} \\ \neg j & \sim & 0 \end{array}$$

Protiprimer je žival, ki

- nima kril,
- ni ptič in
- leže jajca.

Pravilnost sklepa

Pravilnost sklepa $A_1, A_2, \ldots, A_n \models B$ pokažemo tako, da sestavimo zaporedje izjavnih izrazov $C_1, C_2, \ldots, C_m$, kjer je $C_m = B$ in za $i = 1, 2, \ldots, m$ velja:

(a) C_i je ena od predpostavk ali

(b) C_i je tavtologija ali

(c) C_i je enakovreden enemu od predhodnih izrazov v zaporedju ali

(d) C_i logično sledi iz predhodnih izrazov po enem od osnovnih pravilnih sklepov.

Zgled pravilnega sklepa

Ali iz predpostavk $p \Rightarrow q, p \vee r, q \Rightarrow s, r \Rightarrow t, \neg s$ sledi t?

Pogojni sklep

Pogojni sklep (PS) uporabljamo, kadar ima zaključek sklepa obliko implikacije.

Izrek

$A_1, A_2, \ldots, A_k \models B \Rightarrow C$ *natanko tedaj, ko*
$A_1, A_2, \ldots, A_k, B \models C$.

Še en primer pravilnega sklepa

Ali iz predpostavk $p, \neg p$ sledi q?

Zgled

Pokaži, da iz predpostavk $p \Rightarrow q \vee r$ in $\neg r$ logično sledi zaključek $p \Rightarrow q$.

Sklep s protislovjem

Sklep s protislovjem (RA) lahko uporabljamo kadarkoli.

Izrek

$A_1, A_2, \ldots, A_k \models B$ *natanko tedaj, ko*
$A_1, A_2, \ldots, A_k, \neg B \models 0.$

Analiza primerov

Analizo primerov (AP) lahko uporabljamo, kadar ima ena od predpostavk obliko disjunkcije.

Izrek

$A_1, A_2, \ldots, A_k, B_1 \vee B_2 \models C$ *natanko tedaj, ko*
$A_1, A_2, \ldots, A_k, B_1 \models C$ *in*
$A_1, A_2, \ldots, A_k, B_2 \models C.$

Zgled

Pokaži, da iz $p \Rightarrow \neg(q \Rightarrow r)$, $s \wedge q \Rightarrow r$ in s sledi $\neg p$.

1.	$p \Rightarrow \neg(q \Rightarrow r)$	predpostavka
2.	$s \wedge q \Rightarrow r$	predpostavka
3.	s	predpostavka
4.1.	$\neg\neg p$	predpostavka RA
4.2.	p	$\sim$4.1
4.3.	$\neg(q \Rightarrow r)$	MP(1,4.2)
4.4.	$q \wedge \neg r$	$\sim$4.3
4.5.	q	Po(4.4)
4.6.	$\neg r$	Po(4.4)
4.7.	$s \wedge q$	Zd(3,4.5)
4.8.	r	MP(2,4.7)
4.9.	$r \wedge \neg r \sim 0$	Zd(4.8,4.6)
4.	$\neg p$	RA(4.1,4.9)

Dvojiški seštevalnik

Radi bi konstruirali vezje, ki zna sešteti dve števili v dvojiškem zapisu.

Naravno število zapisano v dvojiškem sestavu smemo interpretirati kot zaporedje ničel in enic, oziroma kot zaporedje logičnih vrednosti.

1. sumand x	23	10111
+2. sumand y	+26	+11010
rezultat z	49	110001

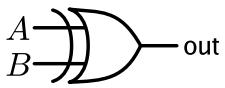
Dvojiški seštevalnik

Na posameznem mestu je potrebno, poleg vrednosti sumandov x_i in y_i, upoštevati tudi prenos p_i. Izračunamo pa, poleg ustrezne mestne vrednosti rezulata z_i tudi prenos na naslednje dvojiško mesto p_{i+1}.

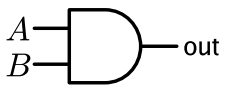
x_i	y_i	p_i	p_{i+1}	z_i
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

z_i ima vrednost 1 natanko tedaj, ko ima liho mnogo izmed x_i, y_i, p_i vrednost 1.
p_{i+1} ima vrednost 1 natanko tedaj, ko imata vsaj dva izmed x_i, y_i, p_i vrednost 1.

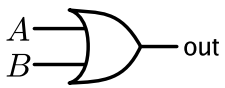
Logična vrata



$A \veebar B$



$A \wedge B$



$A \vee B$

Predikatni račun

Predpostavki:	*Vsi študentje računalništva znajo logično sklepati.*
	Škrat Kuzma ne zna logično sklepati.
Zaključek:	*Škrat Kuzma ni študent računalništva.*

Spremenljivke in formule

V predikatnem računu bomo za spremenjlivke uporabljali črke $x, y, z, \ldots$
V predikate lahko, namesto konstant, vstavljamo tudi spremeljivke.
Na ta način pridelamo *formule*. Formule niso nujno izjave.

Področje pogovora in predikati

Področje pogovora je neprazna *množica* iz katere izbiramo *individualne konstante*.
Predikati so logične *funkcije*, ki za svoje argumente lahko dobijo individualne konstante iz področja pogovora.
Če v predikate vstavljamo (individualne) konstante, dobimo *izjave*.

Kvantifikatorja

Poznamo dva kvantifikatorja:

$\forall$	univerzalni kvantifikator
$\exists$	eksistenčni kvantifikator

Kako iz formule naredimo izjavo?

Možna sta dva pristopa.

1. Namesto spremenljivke vstavimo konstanto.
2. Formulo zapremo s kvantifikatorji.

Izjavne formule

- *spremenljivke* $x, y, z, \ldots,$
- *konstante* $a, b, c, \ldots,$
- *predikati* $P, Q, R, \ldots,$
- izjavni vezniki $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \ldots,$
- *kvantifikatorja* $\forall$ in $\exists$ ter
- oklepaja (in) .

Spremenljivkam in konstantam pravimo tudi *termi*.
Atomi predikatnega računa so, na primer,

$$P(x), P(a), Q(x, y), Q(a, x), \ldots$$

Atome dobimo tako, da terme vstavimo v predikate.

Zgled

Dvomestni predikat $P(x, y)$ naj pomeni *x pozna y-ona.*
Na katere načine lahko formulo $P(x, y)$ spremeniš v izjavo?

Izjavne formule

Izjavne formule so definirane induktivno:

1. Atomi so izjavne formule
2. Če sta W in V izjavni formuli in je x spremenljivka, potem so tudi

$$\neg(W), (W) \wedge (V), (W) \vee (V), (W) \Rightarrow (V), (W) \Leftrightarrow (V), \ldots$$

$$\exists x\,(W) \quad \text{in} \quad \forall x\,(W)$$

izjavne formule.

Doseg kvantifikatorjev

Doseg kvantifikatorja je *najmanjši možen*: najmanjša izjavna formula, ki jo preberemo desno od kvantifikatorja (skupaj z njegovo spremenljivko).
Kvantifikator *veže* svojo spremenljivko in proste spremenljivke z istim imenom v svojem dosegu.
Formulo brez prostih spremenljivk imenujemo, če imamo izbrano interpretacijo, *izjava*, ali *izjavna shema*, če interpretacija ni določena.

Pomen kvantifikatorjev

Naj bo W formula. Z $W(x/a)$ označimo formulo, ki jo dobimo tako, da v formuli W vse proste vstope spremenljivke x nadomestimo z a.

W	$P(x) \vee \exists x\, Q(x,y) \wedge R(b,x)$
$W(x/a)$	$P(a) \vee \exists x\, Q(x,y) \wedge R(b,a)$

Interpretacija izjavne formule

Interpretacija $\mathcal{I}$ izjavne formule W je sestavljena iz neprazne množice $\mathcal{D}$, ki ji pravimo *področje pogovora* interpretacije.
Poleg tega

- vsakemu predikatu ustreza $0/1$ logična funkcija v $\mathcal{D}$ (0-mestnemu predikatu ustreza izjava oziroma njena logična vrednost)
- vsaki konstanti določimo vrednost v $\mathcal{D}$ (ponavadi je implicitno določena že z imenom konstante)
- vsaki prosti spremenljivki v W določimo vrednost v $\mathcal{D}$, pri tem vsem prostim spremenljivkam z istim imenom določimo *isto* vrednost iz $\mathcal{D}$.

Pomen kvantifikatorjev

Formula $\forall x\, W$ je *resnična* v interpretaciji $\mathcal{I}$, če je za vsak element področja pogovora $d \in \mathcal{D}$ resnična formula $W(x/d)$. Sicer je $\forall x\, W$ neresnična.

Formula $\exists x\, W$ je *resnična* v interpretaciji $\mathcal{I}$, če v področju pogovora obstaja $d \in \mathcal{D}$, za katerega je formula $W(x/d)$ resnična. Sicer je $\exists x\, W$ neresnična.

Enakovredne izjavne formule

Izjavni formuli W in V sta *enakovredni*, če imata isto logično vrednost v vseh možnih interpretacijah.
V tem primeru pišemo $W \sim V$.

Zgled

Formuli $\neg\forall x\, W$ *in* $\exists x\, \neg W$ *sta enakovredni.*

Enakovredne izjavne formule

Izjavna formula W je *splošno veljavna*, če je resnična v vsaki interpretaciji.
Izjavna formula V je *neizpolnljiva*, če je neresnična v vsaki interpretaciji.

Zakoni predikatnega računa

So nekateri pomembni pari enakovrednih izjavnih formul:

$$\neg\forall x\, W \sim \exists x\, \neg W$$
$$\neg\exists x\, W \sim \forall x\, \neg W$$

$$\forall x \forall y\, W \sim \forall y \forall x\, W$$
$$\exists x \exists y\, W \sim \exists y \exists x\, W$$

$$\forall x\, (W \wedge V) \sim \forall x\, W \wedge \forall x\, V$$
$$\exists x\, (W \vee V) \sim \exists x\, W \vee \exists x\, V$$

Preimenovanje spremenljivk

Formula

$$\forall x\,(P(w) \Rightarrow P(x))$$

je enakovredna formuli

$$\forall y\,(P(w) \Rightarrow P(y))$$

in ni enakovredna formuli

$$\forall w\,(P(w) \Rightarrow P(w)).$$

Preimenovanje spremenljivk

Želja: če je W formula, potem imen prostih spremenljivk ne smemo spreminjati, če zelimo pridelati enakovredno formulo. Vezane spremenljivke lahko preimenujemo tako, da ista spremenljivka (tj. spremenljivka z istim imenom)

- *ne nastopa pri več kvantifikatorjih*
- *ni hkrati vezana in prosta.*

Preimenovanje spremenljivk

Trditev

Če se y ne pojavi v W, potem veljata enakovrednosti:

$$\begin{aligned} \forall x\, W &\sim \forall y\,(W(x/y)) \\ \exists x\, W &\sim \exists y\,(W(x/y)) \end{aligned}$$

Zakoni predikatnega računa z omejitvami

Če se x ne pojavi (prosto) v formuli C, potem veljajo naslednje enakovredosti:

$$\forall x\,(C \vee W) \sim C \vee \forall x\, W$$
$$\exists x\,(C \vee W) \sim C \vee \exists x\, W$$

$$\forall x\,(C \wedge W) \sim C \wedge \forall x\, W$$
$$\exists x\,(C \wedge W) \sim C \wedge \exists x\, W$$

Prenexna normalna oblika

Naj bo W izjavna formula. *Prenexna normalna oblika* izjavne formule W je izjavna formula W_{PNO}, za katero velja:

- W_{PNO} je enakovredna W in
- W_{PNO} ima vse kvantifikatorje na začetku.

Prenexna normalna oblika

$$\forall x\, A(x) \vee \exists x\, B(x) \Rightarrow C(x) \wedge \exists x\, C(x)$$

Prenexna normalna oblika

Kako do prenexne normalne oblike?

1. Preimenuj vezane spremenljivke v formuli tako, da nobena dva kvantifikatorja ne uporabljata spremenljivke z istim imenom in so imena prostih spremenljivk drugačna od imen vezanih spremenljivk.
2. premakni kvantifikatorje proti levi, pri tem pa, če je potrebno, nadomesti $\Rightarrow$ in $\Leftrightarrow$ z logičnimi vezniki $\neg, \wedge, \vee$.

Sklepanje v predikatnem računu

Predpostavke:	*Vsak pes ima rad ljudi ali sovraži mačke.*
	Fido je pes.
	Fido ima rad mačke.
Zaključek:	*Obstaja pes, ki ima rad ljudi.*

Kaj, če interpretacija ni določena.

Pokaži, da je izjavna formula

$$\neg\exists y \forall x (P(x,y) \Leftrightarrow \neg P(x,x))$$

splošno veljavna.

Napačno sklepanje v predikatnem računu

$$\forall x \exists y\, P(x,y) \quad \models \quad \exists y \forall x\, P(x,y)$$

Kako torej sklepamo?

1. Izberemo interpretacijo, če slučajno ni določena.
2. Izjavne formule preoblikujemo tako, da kvantifikatorji nastopajo na začetku. Preimenovanje spremenljivk in prenexna normalna oblika.
3. Odpravimo kvantifikatorje. Formule smemo prilagoditi.
4. Sklepamo kot v izjavnem računu.
5. Uvedemo kvantifikatorje nazaj.
6. Upoštevamo interpretacijo.

Napačno sklepanje v predikatnem računu

$$\exists x\, P(x) \wedge \exists x\, Q(x) \quad \models \quad \exists x\, (P(x) \wedge Q(x))$$

Omejeni kvantifikatorji

Gre za *način zapisa*.

$N(x)$	...	x je naravno število, pripada $\mathbb{N}$.
$P(x)$	...	x lahko pišemo kot produkt praštevil.
$S(x)$	...	x je sodo število.

Omejeni kvantifikatorji

Vsako naravno število lahko pišemo kot produkt praštevil.

$$\forall x\,(N(x) \Rightarrow P(x)) \quad \overset{\text{def}}{\sim} \quad \forall x \in \mathbb{N}\,(P(x))$$

Obstaja sodo naravno število.

$$\exists x\,(N(x) \wedge S(x)) \quad \overset{\text{def}}{\sim} \quad \exists x \in \mathbb{N}\,(S(x))$$

Omejeni kvantifikatorji in negacija

Obnašanje je ravno takšno, kot pričakujemo.

$$\neg\forall x \in A\,(P(x)) \;\sim\; \exists x \in A\,\neg(P(x))$$

$$\neg\exists x \in A\,(P(x)) \;\sim\; \forall x \in A\,\neg(P(x))$$

Teorija množic

relacija pripadnosti $\ldots x \in A$
x *pripada* A.
podajanje množic

- z naštevanjem elementov $A = \{0, 1, 2\}$
- z neko izjavno formulo $A = \{x \,;\, \varphi(x)\}$
  Velja: $x \in A \Leftrightarrow \varphi(x)$

Operacije z množicami

- *unija* $A \cup B = \{x \,;\, x \in A \vee x \in B\}$
- *presek* $A \cap B = \{x \,;\, x \in A \wedge x \in B\}$
- *razlika* $A \setminus B = \{x \,;\, x \in A \wedge x \notin B\}$
- *simetrična razlika* $A + B = \{x \,;\, x \in A \veebar x \in B\}$

Enakost in vsebovanost

Množici A in B sta *enaki*,

$$A = B \iff \forall x\,(x \in A \Leftrightarrow x \in B)$$

Množica A je *podmnožica* množice B,

$$A \subseteq B \iff \forall x\,(x \in A \Rightarrow x \in B)$$

relacija *inkluzije*
Množica A je *prava podmnožica* množice B,

$$A \subset B \iff A \subseteq B \;\wedge\; A \neq B$$

relacija *stroge inkluzije*

Lastnosti operacij

- $A = B \iff A \subseteq B \wedge B \subseteq A$
- $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$
- $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$
- $A \cap B \subseteq A \subseteq A \cup B$

Pravimo, da sta množici A in B *disjunktni*, če je $A \cap B = \emptyset$.

Potenčna množica

Potenčna množica množice A, $\mathcal{P}A$, je množica vseh podmnožic množice A.

$$\mathcal{P}A = \{B \; ; \; B \subseteq A\}$$

Tako $\emptyset$ kot A pripadata potenčni množici $\mathcal{P}A$.

$$\mathcal{P}\emptyset = \{\emptyset\} \qquad \mathcal{P}\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$$

$$\mathcal{P}\{1, 2, 3\}$$

Lastnosti komplementa

- $(A^c)^c = A$
- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$
- $A \setminus B = A \cap B^c$
- $A \subseteq B \Rightarrow B^c \subseteq A^c$
- $A \cap B = \emptyset \iff A \subseteq B^c \iff B \subseteq A^c$

Univerzalna množica in komplement

Univerzalna množica, označimo jo z S, ustreza področju pogovora v predikatnem računu. Z univerzalno množico se izognemo Russellovi antinomiji.
Vse obravnavane množice so vsebovane v univerzalni množici S.
Komplement množice A, označimo ga z A^c, definiramo kot

$$A^c = S \setminus A$$

Enakosti z množicami

Pokažimo, da velja

$$A \cup (A \cap B) = A$$

Sistem enačb

Reši sistem enačb z množicami.

$$X \cup A = A \setminus X$$
$$X \cup A = X$$

Reševanje sistemov enačb z eno neznano množico

Reši sistem enačb z množicami.

$$A \cap X = B \setminus X$$
$$C \cup X = X \setminus A$$

Reševanje sistemov enačb z eno neznano množico

Trditev
$A \cup B = \emptyset \iff A = \emptyset \wedge B = \emptyset$

Trditev
$A + B = \emptyset \iff A = B$

Reševanje sistemov enačb z eno neznano množico

Družine množic

Naj bo $\mathcal{A} = \{A, B, C, \ldots\}$ *družina množic*.
Unija družine $\mathcal{A}$ je množica

$$\bigcup \mathcal{A} = \{x \,;\, \exists X\, (X \in \mathcal{A} \wedge x \in X)\}$$

Presek družine $\mathcal{A}$ je množica

$$\bigcap \mathcal{A} = \{x \,;\, \forall X\, (X \in \mathcal{A} \Rightarrow x \in X)\}$$

Pokritje in razbitje

Družina množic $\mathcal{A} = \{A_i \,;\, i \in \mathcal{I}\}$ je *pokritje* množice B, če je $B = \bigcup_{i \in \mathcal{I}} A_i$.
Družina množic $\mathcal{A} = \{A_i \,;\, i \in \mathcal{I}\}$ je *razbitje* množice B, če je

- $\mathcal{A}$ pokritje množice B
- elementi $\mathcal{A}$ so neprazni in
- elementi $\mathcal{A}$ so paroma disjunktni .

Družine množic

Ponavadi uporabljamo *indeksno obliko*, z $\mathcal{I}$ označimo indeksno množico.

$$\mathcal{A} = \{A_i \,;\, i \in \mathcal{I}\}$$

Potem je

$$\bigcup \mathcal{A} = \bigcup_{i \in \mathcal{I}} A_i = \{x \,;\, \exists i\, (i \in \mathcal{I} \wedge x \in A_i)\}$$

$$\bigcap \mathcal{A} = \bigcap_{i \in \mathcal{I}} A_i = \{x \,;\, \forall i\, (i \in \mathcal{I} \Rightarrow x \in A_i)\}$$

Urejeni pari

Urejeni par s *prvo komponento (koordinato)* a in *drugo komponento (koordinato)* b označimo z (a, b) in definiramo kot

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Trditev
(osnovna lastnost urejenih parov)

$$(a, b) = (c, d) \iff a = c \text{ in } b = d$$

Kartezični produkt

Kartezični produkt množic A in B je množica vseh urejenih parov

$$A \times B = \{(a, b) \; ; \; a \in A \wedge b \in B\}$$

Lastnosti kartezičnega produkta

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $(A \cup B) \times C = (A \times C) \cup (B \times C)$
- $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

Kartezični produkt

$(a_1, a_2, \ldots, a_n)$ je urejena n-terica.
Definicijo kartezičnega produkta lahko razširimo na več faktorjev.

Lastnosti kartezičnega produkta

- $A \times B = \emptyset \iff A = \emptyset \vee B = \emptyset$
- $A \subseteq C \wedge B \subseteq D \implies A \times B \subseteq C \times D$
- $A \times B \subseteq C \times D \;\wedge\; A \times B \neq \emptyset \implies A \subseteq C \wedge B \subseteq D$
- A končna z m elementi in B končna z n elementi $\implies$ $A \times B$ končna z $m \cdot n$ elementi.

Relacije

Množica R je *(dvomestna) relacija*, če je vsak njen element urejen par.

$$R \text{ je relacija.} \iff \forall x \in R\, \exists u, v \,:\, x = (u, v)$$

Množica R je *(dvomestna) relacija v množici* A, če je $R \subseteq A \times A$.

Domena in zaloga vrednosti

Naj bo R relacija v A.

$\mathcal{D}_R = \{x \,;\, \exists y : xRy\}$ *domena* ali *definicijsko območje* relacije R.

$\mathcal{Z}_R = \{y \,;\, \exists x : xRy\}$ *zaloga vrednosti* relacije R.

Zgledi

1. $A = \{a, b, c, d\}$ $\quad R = \{(a, b), (b, c), (c, d), (c, a)\}$
2. $A = \mathbb{N}$ $\quad R = \{(x, y) \,;\, x, y \in \mathbb{N} \wedge x \leq y\}$
3. $\emptyset \subseteq A \times A$
4. $A \times A \subseteq A \times A$
5. $\mathrm{id}_A = \{(x, x) \,;\, x \in A\}$

Namesto $(x, y) \in R$ pišemo xRy.

Lastnosti relacij

Naj bo R relacija v A. Pravimo, da je

1. R *refleksivna* $\iff \forall x \in A : xRx$
2. R *simetrična* $\iff \forall x, y \in A : xRy \Rightarrow yRx$
3. R *antisimetrična* $\iff \forall x, y \in A : xRy \wedge yRx \Rightarrow x = y$
4. R *tranzitivna* $\iff \forall x, y, z \in A : xRy \wedge yRz \Rightarrow xRz$
5. R *sovisna* $\iff \forall x, y \in A : x \neq y \Rightarrow xRy \vee yRx$
6. R *enolična* $\iff \forall x, y, z \in A : xRy \wedge xRz \Rightarrow y = z$

Zgledi

1. Relacija id_A v A
2. Relacija $\leq$ v $\mathbb{N}$
3. Relacija $<$ v $\mathbb{N}$
4. Relacija $\subseteq$ v $\mathcal{P}A$
5. Relacija *"oče"* v množici ljudi (x oče y preberemo kot x *je oče* y*-ona.*)

Operacije z relacijami

Poleg navedenih operacij definiramo tudi:

- *inverzno relacijo* relacije R, označimo jo z R^{-1}:

$$R^{-1} := \{(y, x) \,;\, (x, y) \in R\}$$

- *produkt relacij* R in S, označimo ga z $R * S$:

$$R * S := \{(x, z) \,;\, \exists y \, (xRy \wedge ySz)\}$$

Operacije z relacijami

Relacije so posebne vrste množic. Vemo, kako so definirane operacije $\cup, \cap$ in $\setminus$.
Ponavadi se pogovarjamo o družini relacij na isti množici A. V takem primeru je *komplement* smiselno definirati kot

$$R^c := (A \times A) \setminus R = U_A \setminus R$$

Operacije z relacijami

Zgled: sorodstvene relacije med ljudmi
Relacija *oče* v množici ljudi je definirana kot

x oče $y \Leftrightarrow x$ *je oče* y*-ona.*.

Naloga: Izrazi relacije *roditelj*, *zet*, *snaha*, *ded*, *vnuk*, *tašča*, *svak* z "bolj elementarnimi" sorodstvenimi relacijami *oče*, *mati*, *sin*, *hči*, *mož*, *žena*, ...

Lastnosti operacij z relacijami

Naj bodo R, S, T relacije na A.

1. $(R^{-1})^{-1} = R$
2. $(R * S)^{-1} = S^{-1} * R^{-1}$
3. $(R * S) * T = R * (S * T) =: R * S * T$
4. $R * (S \cup T) = R * S \cup R * T$
5. $(R \cup S) * T = R * T \cup S * T$
6. $R * \mathrm{id}_A = \mathrm{id}_A * R = R$
7. $R \subseteq S \implies R * T \subseteq S * T$ in $T * R \subseteq T * S$

Potence relacij

Definiramo lahko tudi potence z negativnimi eksponenti, če je $n > 0$, potem

$$R^{-n} := (R^{-1})^n$$

Potence relacij

Zaradi asociativnosti množenja relacij lahko definiramo potence relacij. Naj bo $R \subseteq A \times A$.

$$\begin{array}{lcl} R^0 & := & \mathrm{id}_A \\ R^{n+1} & := & R^n * R, \text{ če je } n \geq 0. \end{array}$$

Velja $R^1 = R$, $R^2 = R * R$, ter za $m, n \geq 0$ tudi $R^m * R^n = R^{m+n}$.

Potence relacij

Zgled: sorodstvene relacije med ljudmi

Naloga: definiraj relacije *prednik*, *potomec*, *sorodnik*.

Grafična predstavitev relacije

R naj bo relacija v *končni* množici A.
Elemente množice A narišemo kot *točke* v ravnini. Če velja aRb, narišemo usmerjeno puščico od a do b.

elementi A ... točke v ravnini

aRb ... usmerjena puščica od a do b.

Zgled: $A = \{a, b, c, d\}$ $\quad R = \{(a, b), (b, c), (c, d), (c, a)\}$

Ekvivalenčna relacija

$R \subseteq A \times A$ je *ekvivalenčna*, če je

- refleksivna,
- simetrična in
- tranzitivna.

Algebraična karakterizacija lastnosti relacij

Naj bo R relacija v A. Relacija R je

1. R *refleksivna* $\iff \mathrm{id}_A \subseteq R$
2. R *simetrična* $\iff R^{-1} = R$
3. R *antisimetrična* $\iff R^{-1} \cap R \subseteq \mathrm{id}_A$
4. R *tranzitivna* $\iff R^2 \subseteq R$
5. R *sovisna* $\iff \mathrm{id}_A \cup R \cup R^{-1} = U_a$
6. R *enolična* $\iff R^{-1} * R \subseteq \mathrm{id}_A$

Ekvivalenčna relacija

Zgledi:

1. Relacija $||$ vzporednosti v množici vseh premic v ravnini.
2. $A = \{\text{ljudje}\}$, $xRy \iff x$ ima enako barvo oči kot y.
3. $f : A \to B$, $x, y \in A : xR_f y \Leftrightarrow f(x) = f(y)$
   x in y imata isto funkcijsko vrednost.
4. Naj bo $m \in \mathbb{N}$, $m \geq 2$. Definirajmo relacijo R v množici $\mathbb{Z}$:

$$xRy \iff m \text{ deli } |x - y|$$

Ekvivalenčni razredi

Naj bo $R \subseteq A \times A$ ekvivalenčna in $x \in A$.

$R[x] = \{y \in A \,;\, yRx\}$ je *ekvivalenčni razred* elementa x.

$A/R = \{R[x] \,;\, x \in A\}$ (množica vseh ekvivalenčnih razredov) je *faktorska (kvocientna) množica* množice A po relaciji R.

Zgledi faktorskih množic

- "premice v ravnini" / "vzporedne premice" $=$ $\{\{\text{navpične pr.}\}, \{\text{vodoravne pr.}\}, \{\text{pr. pod kotom } 45^\circ\}, \ldots\} \cong$ "množica vseh *smeri* v ravnini" $\cong [-\pi/2, \pi/2)$

Ekvivalenčni razredi, razbitje

Trditev
Naj bo R ekvivalenčna relacija na A. Potem za poljubna $x, y \in A$ velja

$$R[x] = R[y] \iff xRy$$

Izrek
Naj bo R ekvivalenčna relacija na A. Potem je A/R razbitje množice A.

Funkcije in preslikave

Enolično relacijo imenujemo *funkcija*.
Relacija $f \subseteq A \times B$ je *preslikava iz A v B*, če velja:

- f je enolična
- $\mathcal{D}_f = A$
- $(\mathcal{Z}_f \subseteq B)$

Pišemo tudi $f : A \to B$.

Funkcije in preslikave

Naj bo f preslikava iz A v B.
Namesto $x\,f\,y$ pišemo $y = f(x)$.

- $A = \mathcal{D}_f$ ... domena ali definicijsko območje f
- $\mathcal{Z}_f$ ... zaloga vrednosti f
- B ... kodomena f

Oznaka: $B^A = \{f\,;\, f : A \to B\}$

Zgledi

1. $\emptyset$, *prazna funkcija*
   $\emptyset : \emptyset \to B$
2. $\mathrm{id}_A : A \to A$, *identiteta na* A
   $\mathrm{id}_A(x) = x$, je bijektivna
3. $p_i : A_1 \times \cdots \times A_n \to A_i$, *projekcija na* i*-to komponento*
   $p_i((a_1, \ldots, a_n)) = a_i$, je surjektivna
4. $A_1 \subseteq A$, $i = \mathrm{id}_A|_A$
   $i : A_1 \hookrightarrow A, i(x) = x$ je injektivna , *vložitev* A_1 *v* A
5. $R \subseteq A \times A$ ekvivalenčna, $p : A \to A/R$
   $p(x) = R[x]$ je surjektivna , *naravna projekcija*
6. $A \subseteq B$, $\chi_A : B \to \{0, 1\}$
   $\chi_A(x) = \begin{cases} 1, x \in A \\ 0, x \notin A \end{cases}$,
   karakteristična funkcija množice A *(v* B*)*

Lastnosti preslikav

Naj bo $f : A \to B$. Pravimo, da je

- f *injektivna*, če $\forall x, y \in A : (f(x) = f(y) \Rightarrow x = y)$
- f *surjektivna*, če $\mathcal{Z}_f = B$ (pravimo tudi, da je f preslikava iz A na B)
- f *bijektivna*, če je injektivna in surjektivna.

Inverzna funkcija in preslikava

Vprašanje: Kdaj je f^{-1} tudi funkcija oziroma preslikava?

Trditev

$f : A \to B$

1. f^{-1} *je enolična natanko tedaj, ko je* f *injektivna,*
2. $f^{-1} : B \to A$ *natanko tedaj, ko je* f *bijektivna.*

Kompozitum funkcij in preslikav

Naj bo $f \subseteq A \times B$ in $g \subseteq B \times C$. Definirajmo

$$g \circ f = f * g$$

V tem primeru je $f * g \subseteq A \times C$.

$$z = (g \circ f)(x) \ \sim \ x(f * g)z \ \sim \ \exists y \ : (xfy \wedge ygz) \ \sim$$

$$\sim \ \exists y \ : (y = f(x) \wedge z = g(y)) \ \sim \ z = g(f(x))$$

Lastnosti kompozituma

Trditev

1. f, g *enolični* $\Longrightarrow f \circ g$ *enolična in* $(f \circ g)(x) = f(g(x))$
2. $f : B \to C, g : A \to B \implies f \circ g : A \to C$

Lastnosti kompozituma

Trditev

Naj bo $f : A \to B$.

1. $f^{-1} \circ f = R_f$, *kjer* $xR_f y \Leftrightarrow f(x) = f(y)$
2. $f \circ f^{-1} = \mathrm{id}_{\mathcal{Z}_f}$
3. f *je injektivna* $\Longleftrightarrow f^{-1} \circ f = \mathrm{id}_A$
4. f *je surjektivna* $\Longleftrightarrow f \circ f^{-1} = \mathrm{id}_B$

Trditev

Naj bo $F : A \to B$. *Potem je*

$$f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$$

Lastnosti kompozituma

Trditev

$f : B \to C, g : A \to B$

1. f, g *injektivni* $\Longrightarrow f \circ g$ *injektivna*
2. f, g *surjektivni* $\Longrightarrow f \circ g$ *surjektivna*
3. $f \circ g$ *injektivna* $\Longrightarrow g$ *injektivna*
4. $f \circ g$ *surjektivna* $\Longrightarrow f$ *surjektivna*

Lastnosti kompozituma

Trditev

Naj bo $f : B \to A$, $g : A \to B$. Če je $f \circ g = \mathrm{id}_A$ in $g \circ f = \mathrm{id}_B$, potem sta f in g bijekciji in je $g = f^{-1}$.

Dirichletov princip

Izrek

Naj bo A končna množica in $f : A \to A$. Potem so naslednje trditve enakovredne:

- *f je injektivna.*
- *f je surjektivna.*
- *f je bijektivna.*

Moč končnih množic

Naj bo A končna množica. Potem $|A|$ označuje *število elementov* ali *moč* množice A.
Naj bosta A in B končni množici. Pravimo, da sta A in B *enako močni*, $A \sim B$, če $|A| = |B|$.
Zgledi:

1. $|\emptyset| = 0$
2. $|\{0,1\}| = 2$
3. $|\{\{0,1\}\}| = 1$

Načelo vključitev in izključitev

Izrek
Naj bo A končna množica in $A_1, A_2, \ldots, A_n \subseteq A$. Potem je

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| &= \\ & |A_1| + |A_2| + \ldots + |A_n| \\ - & |A_1 \cap A_2| - |A_1 \cap A_3| - \ldots - |A_{n-1} \cap A_n| \\ + & \ldots \\ & \ldots \\ +(-1)^{n+1} & |A_1 \cap A_2 \cap \cdots \cap A_n| \\ = & \textstyle\sum_{i=1}^{n} (-1)^{i+1} S_i, \end{aligned}$$

kjer je $S_k = \displaystyle\sum_{\substack{\mathcal{J} \subseteq \{1,\ldots,n\} \\ |\mathcal{J}|=k}} \left| \bigcap_{i \in \mathcal{J}} A_i \right|$.

Moč končnih množic

Trditev
Naj bodo A, B, C končne množice.

1. $|A \times B| = |A| \cdot |B|$
2. $|\{f \,;\, f : A \to B\}| = \left|B^A\right| = |B|^{|A|}$
3. $|\mathcal{P}A| = 2^{|A|}$
4. *Če je $B \subseteq A$, potem je $|A \setminus B| = |A| - |B|$.*

   V splošnem je $|A \setminus B| = |A| - |A \cap B|$.
5. *Če je $A \cap B = \emptyset$, potem je $|A \cup B| = |A| + |B|$.*

   V splošnem je $|A \cup B| = |A| + |B| - |A \cap B|$.
6. $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Načelo vključitev in izključitev

Posledica
Naj bo A končna množica in $A_1, A_2, \ldots, A_n \subseteq A$. Definirajmo $A_i^c = A \setminus A_i$. Potem je

$$\begin{aligned} \left|\textstyle\bigcap_{i=1}^{n} A_i^c\right| &= \\ & |A| - |A_1| - |A_2| - \ldots - |A_n| \\ + & |A_1 \cap A_2| + |A_1 \cap A_3| + \ldots + |A_{n-1} \cap A_n| \\ - & \ldots \\ & \ldots \\ +(-1)^{n} & |A_1 \cap A_2 \cap \cdots \cap A_n| \\ = & \textstyle\sum_{i=0}^{n} (-1)^{i} S_i, \end{aligned}$$

kjer je $S_0 = |A|$ *in* $S_k = \displaystyle\sum_{\substack{\mathcal{J} \subseteq \{1,\ldots,n\} \\ |\mathcal{J}|=k}} \left| \bigcap_{i \in \mathcal{J}} A_i \right|$.

Moč neskončnih množic

Pravimo, da sta množici A in B *enako močni*, $A \sim B$, če obstaja *bijektivna* preslikava iz A v B. Pišemo tudi $|A| = |B|$.
Pravimo, da je množica B *kvečjemu močnejša* od množice A, če obstaja *injektivna* preslikava iz A v B. Pišemo tudi $|A| \leq |B|$.
Oznaka $|A| < |B|$ pomeni, da obstaja injektivna preslikava iz A v B ter, da nobena preslikava iz B v A ni injektivna.

Moč neskončnih množic

Izrek (o trihotomiji)

Za poljubni množici A in B velja natanko ena izmed možnosti $|A| < |B|$, $|A| = |B|$ ali $|A| > |B|$.

Izrek (Cantor-Bernstein)

$|A| = |B|$ *natanko tedaj, ko* $|A| \leq |B|$ *in* $|B| \leq |A|$

Deljivost celih števil

Izrek (o deljenju)

Naj bosta $m, n \in \mathbb{Z}$ in $m > 0$. Obstajata enolično določeni celi števili k in r, pri čemer je

$$n = k \cdot m + r \quad \text{in velja} \quad 0 \leq r < m.$$

k je *kvocient* števil n in m
r je *ostanek* pri deljenju števila n z m.

Razširjeni Evklidov Algoritem - REA

Zgled: Poišči $\gcd(899, 812)$.

Deljivost celih števil

Naj bosta $m, n \in \mathbb{Z}$. Pravimo, da m *deli* n,

$$m|n,$$

če obstaja tak $k \in \mathbb{Z}$, da je $n = k \cdot m$.
Če m, n nista oba 0, potem lahko definiramo

$$\gcd(m, n) = \max\{d \in \mathbb{Z}\ ;\ d|m \text{ in } d|n\}$$

največji skupni delitelj števil m in n

$$\operatorname{lcm}(m, n) = \min\{v \in \mathbb{Z}\ ;\ m|v \text{ in } n|v \text{ in } v > 0\}$$

najmanjši skupni večkratnik števil m in n

gcd in lcm sta *komutativni* in *asociativni* operaciji.

Razširjeni Evklidov Algoritem - REA

Naj bosta $m, n > 0$ in $m > n$.

$$\begin{array}{lllllllll}
 & r_{-1}(=m) & = & 1 & \cdot & m & + & 0 & \cdot & n \\
k_1(=\lfloor r_{-1}/r_0 \rfloor) & r_0(=n) & = & 0 & \cdot & m & + & 1 & \cdot & n \\
k_2(=\lfloor r_0/r_1 \rfloor) & r_1 & = & s_1 & \cdot & m & + & t_1 & \cdot & n \\
k_3 & r_2 & = & s_2 & \cdot & m & + & t_2 & \cdot & n \\
\vdots & \vdots & & \vdots & & \vdots & & & & \\
k_{z+1} & r_z(\neq 0) & = & s_z & \cdot & m & + & t_z & \cdot & n \\
 & r_{z+1}(=0) & = & s_{z+1} & \cdot & m & + & t_{z+1} & \cdot & n
\end{array}$$

$(s_{-1} = 1, s_0 = 0, t_{-1} = 0, t_0 = 1)$

Razširjeni Evklidov Algoritem - REA

Za $i = 1, \ldots, z+1$ velja:

$$\begin{aligned} s_i &= s_{i-2} - k_i \cdot s_{i-1} \\ t_i &= t_{i-2} - k_i \cdot t_{i-1} \\ r_i &= r_{i-2} - k_i \cdot r_{i-1} \end{aligned}$$

Trditev

- $r_i = s_i \cdot m + t_i \cdot n$,
  r_i je celoštevilska linearna kombinacija števil m in n.
- *r_z deli r_i*
  za vse $i = z+1, z, z-1, \ldots, 2, 1, 0, -1$.

Tuja števila

Pravimo, da sta si celi števili a in b *tuji*, če je $\gcd(a, b) = 1$.
V tem primeru pišemo $a \perp b$.
Zgled: $899 \perp 813$

Razširjeni Evklidov Algoritem - REA

Izrek (REA)

$$\gcd(m, n) \;=\; r_z \;=\; s_z \cdot m + t_z \cdot n$$

Največji skupni delitelj $\gcd(m, n)$ števil m in n dobimo kot zadnji neničelni ostanek v REA. Obenem $\gcd(m, n)$ zapišemo tudi kot celoštevilsko linearno kombinacijo števil m in n.

Tuja števila

Trditev

Naj velja $a|(b \cdot c)$ in $a \perp b$. Potem $a|c$.

Izrek

Naj bosta $a, b \in \mathbb{N}$. Potem je $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = a \cdot b$.

Diofantske enačbe

Naloga: Skupina otrok je v slaščičarni jedla torte in kremne rezine. Koliko tort in koliko kremnih rezin so pojedli, če je račun znašal 32,75€, torta stane 2,25€, kremna rezina pa 1,75€.
Vemo tudi, da so pojedli manj tort kot kremnih rezin.

Diofantske enačbe

Zgled: Poišči rešitve (linearne) diofantske enačbe $6x + 15y = 7$.

Izrek

Linearna diofantska enačba

$$a \cdot x + b \cdot y = c$$

je rešljiva natanko tedaj, ko $\gcd(a, b)|c$.
Če $\gcd(a, b)$ *ne deli desne strani* c*, potem taka diofantska enačba nima rešitev.*

Diofantske enačbe

Enačba je *diofantska*, če ima celoštevilske podatke in iščemo celoštevilske rešitve.
Linearna diofantska enačba z dvema neznankama je enačba oblike

$$a \cdot x + b \cdot y = c,$$

kjer so znani $a, b, c \in \mathbb{Z}$, iščemo pa celoštevilsko rešitev x, y.
a in b sta *koeficienta* enačbe, c standardno imenujemo *desna stran*.

Diofantske enačbe

Izrek

Naj par x_0, y_0 *reši LDE* $a \cdot x + b \cdot y = c$*, in naj bo* $d = \gcd(a, b)$.
Potem so

$$\begin{aligned} x_k &= x_0 + k \cdot \frac{b}{d} \\ y_k &= y_0 - k \cdot \frac{a}{d}, \end{aligned}$$

kjer je k *poljubno celo število, vse rešitve te diofantske enačbe.*

Diofantske enačbe

Izrek
Linearna diofantska enačba

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_n \cdot x_n = c$$

je rešljiva natanko takrat, ko

$$\gcd(a_1, a_2, \ldots, a_n) | c.$$

Praštevila

Trditev

- *p praštevilo in $a \in \mathbb{Z}$. Potem $p|a$ ali $p \perp a$.*
- *p praštevilo, $a, b \in \mathbb{Z}$. Če $p|(a \cdot b)$, potem $p|a$ ali $p|b$.*
- *$n \in \mathbb{N}$, $n \geq 2$. Obstaja praštevilo p, ki deli n.*

Praštevila

Naravno število $n \geq 1$ je *praštevilo*, če ima natanko dva pozitivna delitelja.

Sicer je 1 ali pa *sestavljeno število*.

Praštevila do 100:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,$
$47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$

Par praštevil oblike $(p, p + 2)$ imenujemo *praštevilska dvojčka*.

Praštevil je neskončno mnogo

Izrek (Evklid)
Obstaja neskončno mnogo praštevil.

Enolični razcep

Izrek
Vsako naravno število $n \geq 2$ lahko zapišemo kot produkt praštevil. Zapis je enoličen, če se ne oziramo na vrstni red faktorjev.

Kako računamo Eulerjevo funkcijo

Trditev
Če je p praštevilo, je $\varphi(p) = p - 1$.

Trditev
Če je p praštevilo, je $\varphi(p^n) = p^n - p^{n-1}$.

Trditev
Če $a, b \in \mathbb{N}$ in $a \perp b$, potem je $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Eulerjeva funkcija φ

Eulerjeva funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ je definirana takole:

$$\varphi(n) = |\{k \in \mathbb{N}\,;\, 1 \leq k \leq n \text{ in } k \perp n\}|$$

$\varphi(n)$ je število števil med 1 in n, ki so tuja n.

Zgled:

$\varphi(4) = 2$	1,2,3,4
$\varphi(5) = 4$	1,2,3,4,5
$\varphi(6) = 2$	1,2,3,4,5,6

Kako računamo Eulerjevo funkcijo

Izrek
Naj bo $n = {p_1}^{k_1} {p_2}^{k_2} \cdots {p_m}^{k_m}$, kjer so $p_1, p_2, \ldots, p_m$ različna praštevila. Potem je

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m}).$$

Kongruence

Naj bo $a \in \mathbb{Z}$ in $m \in \mathbb{N}$, $m \geq 2$. Z

$$a \bmod m$$

označimo ostanek a-ja pri deljenju z m.
Definirajmo relacijo, *kongruenco po modulu m*, z naslednjim opisom:

$$a \equiv b \pmod{m} \iff m|(a-b) \iff a \bmod m = b \bmod m$$

Rezultati

Izrek (Eulerjev izrek)
Naj bo $a \in \mathbb{Z}$, $m \geq 2 \in \mathbb{N}$ in $a \perp m$. Potem je

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

Posledica (mali Fermatov izrek)
Če je p praštevilo in $1 \leq a < p$, potem je

$$a^{(p-1)} \equiv 1 \pmod{p}.$$

Za vse $a \in \mathbb{Z}$ pa velja

$$a^p \equiv a \pmod{p}.$$

Lastnosti kongruenc

1. *kongruenca po modulu m* je ekvivalenčna relacija v $\mathbb{Z}$
2. Če $a \equiv b \pmod{m}$, potem
$$a \pm c \equiv b \pm c \pmod{m}$$
$$a \cdot c \equiv b \cdot c \pmod{m}$$
$$a^n \equiv b^n \pmod{m}$$
3. Če $a \equiv b \pmod{m}$ in $c \equiv d \pmod{m}$, potem
$$a \pm c \equiv b \pm d \pmod{m}$$
$$a \cdot c \equiv b \cdot d \pmod{m}$$
4. Če $a \cdot c \equiv b \cdot c \pmod{m}$ in $c \perp m$, potem $a \equiv b \pmod{m}$

Zgledi

Zgledi:

- Izračunaj ostanek pri deljenju števila 3^{120} s 13.
- Izračunaj zadnjo cifro števila $9^{8^{7^6}}$.
- Izračunaj ostanek pri deljenju števila $9^{8^{7^6}}$ z 11.
- Naj bosta p in q različni praštevili. Pokaži, da je

$$a \equiv b \pmod{p} \text{ in } a \equiv b \pmod{q} \iff a \equiv b \pmod{pq}$$

RSA kriptosistem

RSA kriptosistem deluje na principu *javnih* in *privatnih ključev*.

Pogovarjajmo se o dveh uporabnikih *Ančki* in *Borutu*. Vsak izmed njiju ima svoj *privatni ključ* P_A, P_B, ki ga hrani na skrivnem mestu, svoj *javni ključ* J_A, J_B da na vpogled vsem.

Kolobarji ostankov

Naj bo m naravno število večje ali enako 2.
Kolobar ostankov po modulu m je struktura $(Z_m, +, \cdot)$, kjer je $Z_m = \mathbb{Z}/(\text{mod } m)$, medtem ko sta $+$ in $\cdot$ operaciji *porojeni* na celih številih.
Dogovor: elemente Z_m pišemo kot $0, 1, \ldots, m-1$, po potrebi uporabljamo tudi druge "vrednosti", npr. $-1 = m - 1$.

RSA kriptosistem

Komunikacija med Ančko in Borutom:

- Ančka bi rada Borutu posredovala sporočilo x:
  $x,\ J_B(x) \quad \xrightarrow{!} \quad J_B(x),\ P_B(J_B(x)) = x$
- Ančka bi rada Borutu posredovala sporočilo x in Borut bi rad bil prepričan, da mu je sporočilo res posredovala Ančka.:
  $x,\ P_A(x),\ J_B(P_A(x)) \quad \xrightarrow{!}$
  $\xrightarrow{!} \quad J_B(P_A(x)),\ P_B(J_B(P_A(x))) = P_A(x),\ J_A(P_A(x)) = x$

Veljati mora:

1. P_A in J_A kot tudi P_B in J_B sta *inverzni preslikavi*.
2. Če poznamo J_A iz tega ne moremo (vsaj ne enostavno) izračunati P_A.

Lastnosti operacij

Naj bodo $a, b, c \in Z_m$, *ničla* $0 \in Z_m$ ter *enica* $1 \in Z_m$.

$$(a+b)+c = a+(b+c)$$
$$a+b = b+a$$
$$a+0 = 0+a \ = \ a$$
$$a+(-a) = (-a)+a \ = \ 0$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$a \cdot b = b \cdot a$$
$$a \cdot 1 = 1 \cdot a \ = \ a$$

$$(a+b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b+c) = a \cdot b + a \cdot c$$

Obrnljivi elementi in delitelji niča

Problem: V kolobarju ostankov Z_m enačba $a \cdot x = 1$ ni nujno rešljiva, četudi je $a \neq 0$.
Element $a \in Z_m$ je *obrnljiv*, če obstaja $b \in Z_m$, za katerega velja

$$a \cdot b = 1.$$

Takšnemu b pravimo tudi *(multiplikativni) inverz* a in pišemo $b = a^{-1}$
Element $c \in Z_m \setminus \{0\}$ je *delitelj niča*, če obstaja $d \in Z_m \setminus \{0\}$, za katerega velja

$$c \cdot d = 0.$$

Obrnljivi elementi

Trditev

Z_m sestavljajo 0-ničla, delitelji niča in obrnljivi elementi.

Trditev

V Z_m so obrnljivi natanko tisti elementi, ki so tuji modulu m. V Z_m imamo torej $\varphi(m)$ obrnljivih elementov.
In še, po Eulerjevem izreku, je a^{-1}, inverz elementa a, enak $a^{\varphi(m)-1}$.

Linearne enačbe v Z_m

Linearna enačba v Z_m je enačba oblike

$$a \cdot x = b,$$

kjer je x *neznanka*, $a, b \in Z_m$, $a \neq 0$.

Trditev

Enačba $a \cdot x = b$ ima v Z_m, če je a obrnljiv, natančno eno rešitev.

Trditev

Enačba $a \cdot x = b$ je rešljiva natanko tedaj, ko $\gcd(a, m) | b$. V tem primeru ima enačba v Z_m natančno $\gcd(a, m)$ rešitev.

Permutacije

Naj bo A poljubna množica. *Permutacija* na A je vsaka bijektivna preslikava $f : A \to A$.

Permutacija reda n je permutacija v $\{1, 2, \ldots, n\}$. Množico vseh permutacij reda n imenujemo *simetrična grupa reda n* in jo označimo z S_n.

Zgled:

- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ je permutacija reda 3.
- $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ je permutacija reda 4.
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}$ je permutacija reda 6.

Inverzna permutacija

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 7 & 6 & 5 \end{pmatrix} \qquad \psi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 3 & 2 & 7 & 1 \end{pmatrix}$$

$$\pi * \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 2 & 3 & 7 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

Produkt permutacij

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

$$\pi * \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

$$\psi * \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

Zapis permutacije z disjunktnimi cikli

Permutacijo lahko zapišemo tudi *z disjunktnimi cikli* in ne v obliki *tabelice*.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}$$

Ciklična struktura permutacije

Ciklična struktura permutacije je število dolžin posameznih ciklov v zapisu permutacije z disjunktnimi cikli.

Ciklična struktura permutacije π je
ciklična struktura permutacije ψ je

1-ciklu pravimo tudi *fiksna točka* permutacije,
2-ciklu pravimo *transpozicija*.

Potenciranje ciklov

Potencirajmo 5- in 6-cikel, $\alpha = (1\,2\,3\,4\,5)$, $\beta = (1\,2\,3\,4\,5\,6)$.

Trditev
Naj bo α permutacija, sestavljena iz samo enega cikla dolžine n. Permutacija α^k je sestavljena iz $\gcd(n,k)$ disjunktnih ciklov, ki so vsi iste dolžine $\dfrac{n}{\gcd(n,k)}$.

Posledica
Naj bo α permutacija, sestavljena iz samo enega cikla dolžine n. Potem je $\alpha^n = \mathrm{id}$ in $\alpha^{-1} = \alpha^{n-1}$ in je n najmanjše naravno število (> 0) s to lastnostjo.

Potenciranje permutacij

Za potenciranje permutacij je ugodnješi zapis permutacije *z disjunktnimi cikli* kot pa zapis v obliki *tabelice*.

$$\pi =$$

Kako izračunati $\pi^2, \pi^3, \pi^4, \ldots$?

$\pi^2 =$
$\pi^3 =$
$\vdots$

Potenciranje permutacij

Izrek
Naj bo

$$\pi = \alpha_1 * \alpha_2 * \cdots * \alpha_m,$$

kjer so α_i, $i = 1, \ldots, m$, cikli v zapisu permutacije π z disjunktnimi cikli. Potem je

$$\pi^k = {\alpha_1}^k * {\alpha_2}^k * \cdots * {\alpha_m}^k.$$

Zapis permutacije s transpozicijami

Trditev

Vsako permutacijo lahko zapišemo kot produkt transpozicij .

Komentar: Ker že *zapis cikla* ni enoličen, tudi zapis kot produkt transpozicij ni enolično določen.

Parnost permutacij

Permutacija je *soda*, če jo lahko zapišemo kot produkt sodo mnogo transpozicij, permutacija je *liha*, če jo lahko zapišemo kot produkt liho mnogo transpozicij.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 6 & 5 \end{pmatrix}$$

Pravimo, da sta (v permutaciji π) števili 1 in 2 v *inverziji*, ker sta v spodnji vrstici tabelice v *napačnem* vrstnem redu: 1 je manjše kot 2, toda 2 je zapisana pred 1.

Parnost permutacij

Izrek (o parnosti permutacij)

Denimo, da lahko permutacijo π zapišemo kot produkt m transpozicij, pa tudi kot produkt (morda drugih) n transpozicij. Potem je

$$m \equiv n \pmod 2.$$

Igra 15

Igro 15 igramo na kvadratni igralni površini, na kateri je 15 ploščic s številskimi oznakami in eno *prazno polje*.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Naš cilj je, da s premikanjem ploščic dosežemo *ciljno konfiguracijo*, v kateri so številke po poljih urejene po velikosti. V tem primeru pravimo, da smo igro *uspešno zaključili.*
Kakšna je zveza s permutacijami? Kaj je ena poteza?

Red permutacije

Red permutacije π je najmanjše naravno število $k \geq 1$, za katerega je

$$\pi^k = \mathrm{id}.$$

Trditev

Red permutacije π je najmanjši skupni večkratnik dolžin ciklov v zapisu permutacije π z disjunktnimi cikli.

Konjugirane permutacije

Permutaciji α in β sta *konjugirani*, če obstaja permutacija π, za katero je

$$\beta = \pi^{-1} * \alpha * \pi.$$

Trditev

Konjugiranost je ekvivalenčna relacija v S_n.

Izrek

Permutaciji α in β sta konjugirani natanko takrat, ko imata isto ciklično strukturo.

Kaj je graf

Graf je urejen par $G = (V, E)$, kjer je

- V neprazna končna množica *vozlišč (točk)* grafa G in
- E množica povezav grafa G, pri čemer je vsaka povezava *par* vozlišč .

Zgled:
$V = \{u, v, w, x, y\}$ $\quad E = \{\{u, v\}, \{u, w\}, \{v, w\}, \{v, x\}\}$

Pisava: Namesto $e = \{u, v\}$ pišemo krajše $e = uv$ ali $e = vu$. V tem primeru pravimo, da sta vozlišči u in v *krajišči* povezave e. Pravimo tudi, da sta u in v *sosednji*, kar označimo z $u \sim v$.

Oznake: $V = V(G)$ ... množica vozlišč grafa G
$E = E(G)$ ... množica povezav grafa G

Stopnje vozlišč

Izrek (lema o parnosti)

Naj bo G graf z n vozlišči in m povezavami. Potem je

$$\sum_{i=1}^{n} \deg(v_i) = 2 \cdot m$$

Posledica

V vsakem grafu je sodo mnogo vozlišč lihe stopnje.

Posledica

Naj bo G d-regularen graf z n vozlišči in m povezavami. Potem je

$$n \cdot d = 2 \cdot m$$

Stopnje vozlišč

Stopnja vozlišča $v \in V(G)$ je število povezav, ki imajo v za krajišče. Stopnjo vozlišča v označimo z $\deg(v)$.
Vozlišče stopnje 0 je *izolirano vozlišče*, vozlišču stopnje 1 pravimo tudi *list* grafa.

Graf G je *d-regularen*, če so vsa vozlišča grafa G stopnje d.
3-regularnim grafom pravimo tudi *kubični grafi*.

Izomorfizem grafov

Grafa G_1 in G_2 sta *izomorfna*, če obstaja preslikava $f : V(G_1) \to V(G_2)$, za katero velja:

1. f je bijektivna in
2. $u \sim_{G_1} v \;\Leftrightarrow\; f(u) \sim_{G_2} f(v)$.

V tem primeru pravimo, da je f *izomorfizem* grafov G_1 in G_2, ter pišemo $G_1 \cong G_2$.

Trditev

Izomorfizem ohranja število vozlišč, število povezav, stopnje vozlišč, število trikotnikov, ...

Grafično zaporedje

Končno zaporedje naravnih števil

$$d_1 \geq d_2 \geq d_3 \geq \ldots \geq d_n$$

je *grafično*, če obstaja graf G z n vozlišči, ki imajo stopnje enake $d_1, d_2, \ldots, d_n$.
Naloga: Ali je zaporedje $5, 4, 3, 2, 2, 1$ grafično?

Grafično zaporedje

Izrek
Zaporedje $d_1 \geq d_2 \geq d_3 \geq \ldots \geq d_n$ je grafično natanko tedaj, ko je tudi zaporedje

$$d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$$

grafično.

Posledica
Zaporedje $d_1 \geq d_2 \geq d_3 \geq \ldots \geq d_n$ je grafično natanko tedaj, ko požrešna metoda uspe.

Grafično zaporedje

Naloga: Ali je zaporedje $6, 4, 4, 3, 2, 2, 1$ grafično?

Polni grafi

Graf je *poln*, če sta vsaki njegovi točki sosedi. Poln graf na n točkah označimo s K_n.

$V(K_n) = \{v_1, v_2, \ldots, v_n\}$	$\lvert V(K_n)\rvert = n$
$E(K_n) = \{v_i v_j \,;\, 1 \leq i < j \leq n\}$	$\lvert E(K_n)\rvert = \frac{n(n-1)}{2}$
$\deg(v_1) = n - 1$	K_n je $(n-1)$-regularen graf.

Prazni grafi

Graf je *prazen*, če nobeni njegovi točki nista sosedi. Prazen graf na n točkah označimo s $\overline{K_n}$.

$V(\overline{K_n}) = \{v_1, v_2, \ldots, v_n\}$	$\lvert V(\overline{K_n})\rvert = n$
$E(\overline{K_n}) = \emptyset$	$\lvert E(\overline{K_n})\rvert = 0$
$\deg(v_1) = 0$	$\overline{K_n}$ je 0-regularen graf.

$\overline{K_1} = K_1$

Cikli

Cikel na $n \geq 3$ točkah označimo s C_n.

$V(C_n) = \{v_1, v_2, \ldots, v_n\}$	$\lvert V(C_n)\rvert = n$
$E(C_n) = \{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n, v_nv_1\}$	$\lvert E(C_n)\rvert = n$
$\deg(v_1) = 2$	C_n je 2-regularen graf.

$C_3 = K_3, C_4 = K_{2,2}$

Polni dvodelni grafi

$K_{m,n}$ je *polni dvodelni graf* na $n + m$ točkah. Vsebuje dva *barvna razreda* s po n in m točkami, točki sta sosedi natanko tedaj, ko sta v različnih barvnih razredih.

$V(K_{m,n}) = \{v_1, v_2, \ldots, v_m, u_1, u_2, \ldots, u_n\}$	$\lvert V(K_{m,n})\rvert = m + n$
$E(K_{m,n}) = \{v_iu_j \,;\, 1 \leq i \leq m \text{ in } 1 \leq j \leq n\}$	$\lvert E(K_{m,n})\rvert = m \cdot n$
$\deg(v_1) = n\,,\ \deg(u_1) = m$	$K_{n,n}$ je n-regularen.

$K_{1,1} = K_2$

Poti

Pot na n točkah označimo s P_n.

$V(P_n) = \{v_1, v_2, \ldots, v_n\}$	$\lvert V(P_n)\rvert = n$
$E(P_n) = \{v_1v_2, v_2v_3, \ldots, v_{n-1}v_n\}$	$\lvert E(P_n)\rvert = n - 1$
$\deg(v_1) = 1, \deg(v_2) = 2$	če $n \geq 3$.

$P_1 = K_1 = \overline{K_1}, P_2 = K_2 = K_{1,1}, P_3 = K_{2,1}$

Hiperkocke

Točke *d-razsežne hiperkocke Q_d* so zaporedja ničel in enic dolžine d. Dve takšni točki-zaporedji sta sosedi, če se razlikujeta v natanko enem členu.

$|V(Q_d)| = 2^d$
$|E(Q_d)| = d \cdot 2^{d-1}$
Q_d je d regularen graf.

$Q_0 = K_1, Q_1 = K_2, Q_2 = C_4$

Podgrafi

Podgraf H grafa G je *vpet podgraf*, če je $V(H) = V(G)$.

Podgraf H grafa G je *induciran podgraf*, če za vsako povezavo $e = uv \in E(G)$ velja: če sta u in v vozlišči grafa H, potem je tudi e povezava v grafu H.

Oznake: Naj bo G graf in $U \subseteq V(G)$ ter $F \subseteq E(G)$.

Z $G[U]$ označimo inducirani podgraf z množico vozlišč U.
Z $G[F]$ označimo vpet podgraf z množico povezav F.

Podgrafi

Naj bosta H in G grafa.

Pravimo, da je H *podgraf* grafa G, $H \subseteq G$,če je $V(H) \subseteq V(G)$ in $E(H) \subseteq E(G)$.

Definicija sprehoda

Sprehod S v grafu $G = (V, E)$ je zaporedje vozlišč

$$u_0 u_1 u_2 \dots u_{n-1} u_n,$$

pri čemer sta zaporedni vozlišči sprehoda u_i in u_{i+1} sosedi v grafu G $(i = 0, \dots, n-1)$.

Dolžina sprehoda $S = u_0 u_1 \dots u_n$ je enaka n, $|S| = n$.

Vozlišče u_0 imenujemo *začetek*, vozlišče u_n pa *konec* sprehoda.
$u - v$ sprehod je sprehod z začetkom v u in koncem v v.

Sprehod $S = u_0 \dots u_n$ je *pot*, če $u_i \neq u_j$ za vse $0 \leq i < j \leq n$.
Sprehod $S = u_0 \dots u_n$ je *obhod*, če je $u_0 = u_n$.
Sprehod $S = u_0 \dots u_n$ je *cikel*, če je $u_0 = u_n$, sicer pa so točke med sabo različne in je $n \geq 3$.

Sprehod ali pot

Lema
Če v grafu $G = (V, E)$ obstaja $u - v$ sprehod S, potem v G obstaja tudi $u - v$ pot.

Posledica (dokaza zgornje leme)
Najkrajši $u - v$ sprehod v grafu je pot.

Povezane komponente

V množici točk grafa G definirajmo relacijo P z naslednjim predpisom:

$$uPv \iff \text{v } G \text{ obstaja } u - v \text{ sprehod.}$$

Povezanost grafov

Graf G je *povezan*, če za vsaki dve vozlišči $u, v \in V(G)$ v grafu G obstaja $u - v$ sprehod .

Razdalja v povezanem grafu

Naj bo G povezan graf. *Razdalja* med točkama u in v v grafu G, $\mathrm{dist}(u, v)$, je dolžina najkrajše $u - v$ poti (sprehoda) v G.

Trditev
Razdalja dist *v povezanem grafu ustreza trikotniški neenakosti, za poljubne tri točke u, v, w grafa G velja*

$$\mathrm{dist}(u, w) \leq \mathrm{dist}(u, v) + \mathrm{dist}(v, w)$$

Dvodelni grafi

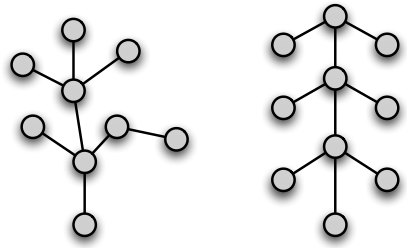
Graf G je *dvodelen*, če lahko točke grafa G pobarvamo z dvema barvama takó, da ima vsaka povezava krajišči različnih barv.

Izrek

Graf G je dvodelen natanko tedaj, ko G ne vsebuje ciklov lihe dolžine.

Zgledi

Grafi P_n in $K_{1,n}$ so drevesa.



Drevesa in gozdovi

Drevo je povezan graf brez ciklov.
Gozd je graf brez ciklov.

Trditev

G je gozd $\iff$ povezane komponente G so drevesa.
G je drevo $\iff$ G je povezan gozd.

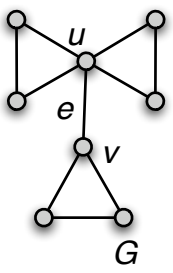
Prerezne točke in povezave

$v \in V(G)$ je *prerezna točka* grafa G, če ima $G - v$ strogo več povezanih komponent kot G.
$e \in E(G)$ je *prerezna povezava* grafa G, če ima $G - e$ strogo več povezanih komponent kot G.

Trditev

$e \in E(G)$ je prerezna povezava natanko tedaj, ko e ne leži na nobenem ciklu v grafu G.

Zgledi



Vpeto drevo

Naj bo G graf in $H \subseteq G$. H je *vpeto drevo* v G, če je

- H vpet podgraf v G in
- H drevo.

Lastnosti dreves

Naj bo T drevo z n točkami in m povezavami.

1. T je povezan graf.
2. T je brez ciklov.
3. $m = n - 1$.
4. Vsaka povezava v T je prerezna.
5. Za poljubni točki $u, v \in V(T)$ obstaja natančno ena $u - v$ pot v T.
6. Če drevesu T dodamo katerokoli novo povezavo, vsebuje dobljeni graf natanko en cikel.

Lastnosti

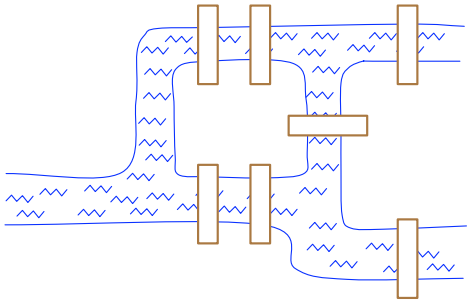
Izrek
G je povezan $\iff$ G ima vsaj eno vpeto drevo.

Trditev
Če je T drevo in $|V(T)| \geq 2$, potem ima T vsaj dva lista.

Posledica
Če je G povezan in $|V(G)| \geq 2$, potem vsebuje G vsaj dve točki, ki nista prerezni.

Eulerjev problem

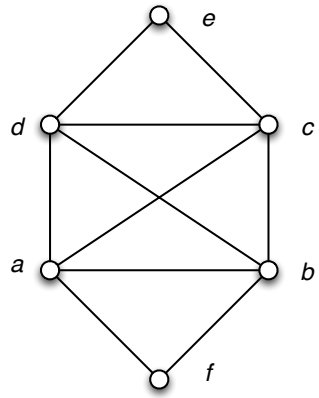
Euler, 1736
Königsberg.



- *Ali obstaja obhod po mestu, ki bi prehodil vse mostove in sicer vsakega natanko enkrat?*

Eulerjevi grafi

Zgled:



- Eulerjev obhod:

Eulerjevi grafi

Sprehod v grafu G je *enostaven*, če vsako povezavo *uporabi* največ enkrat.

Problem: Ali v grafu G obstaja enostaven obhod, ki vsebuje vse povezave in vsa vozlišča?

Enostaven obhod v grafu G, ki vsebuje vse povezave in vsa vozlišča imenujemo *Eulerjev obhod*.

Graf G je *Eulerjev*, če ima kak Eulerjev obhod.

Eulerjev izrek

Izrek (Euler)

Graf G je Eulerjev natanko tedaj, ko je G povezan in so vsa njegova vozlišča sodih stopenj.

Posledica

Graf je Eulerjev natanko tedaj, ko ga lahko narišemo z eno samo potezo, ki je povrh vsega še sklenjena.