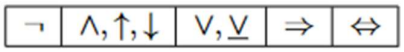
IZJAVNI RAČUN

Izjave

Izjava je vsak stavek, ki ima logično vrednost (0 ali 1). Delimo jih na enostavne in sestavljene, slednje dobimo z uporabo izjavnih veznikov.

Izjavni vezniki

Z izjavnimi vezniki dobimo sestavljene izjave iz enostavnih. Definiramo jih s pomočjo pravilnostnih tabel. Vezniki so negacija, konjunkcija, disjunkcija, implikacija (antecédens, konsékvens), ekvivalenca, ekskluzivna disjunkcija, Shefferjev (NAND) ter Piercov (NOR) operator.



Izjavni izrazi

Izjavne izraze definiramo induktivno

I1. 0 in 1 sta izjavna izraza,
I2. Izjavne spremenljivke (p, q, r) so izjavni izrazi.
I3. Če je F n-mestni izjavni veznik in so A1, A2, …, An izjavni izrazi, potem je F(A1, A2, …, An) izjavni izraz.

I3 = konstrukcijsko pravilo.

Konstrukcijsko drevo

Pri izrazu A = F(A1, …, An) izraz A postavimo v koren konstrukcijskega drevesa, sinovi tega korena pa so konstrukcijska drevesa izrazov A1, …, An. Konstrukcijsko drevo je tako definirano rekurzivno.

Globina – dolžina najdaljše poti do korenskega vozlišča.

Dolžina – število vozlišč konstrukcijskega drevesa.

Pravilnostna tabela

Pravilnostna tabela je podatkovna struktura, s katero za vsak nabor logičnih vrednosti spremenljivk v izjavnem izrazu I izračunamo logično vrednost izjavnega izraza I.

Izraz, ki ima pri vseh naborih logičnih vrednosti logično vrednost 1 je tavtologija, tisti, ki je vedno lažen je protislovje, sicer pa je nevtralen izraz.

Enakovredni izjavni izrazi

Dva izjavna izraza sta si enakovredna natanko tedaj, ko se njuni logični vrednosti ujemata pri vseh možnih naborih logičnih vrednosti spremenljivk. Pišemo I ~ J. Enakovrednost je tesno vezana z ekvivalenco: *Izraza I in J sta si enakovredna natanko tedaj, ko je I ekvivalenten J tavtologija*. Enakovrednost ugotovimo ali s pomočjo pravilnostne tabele, ali pa z uporabo zakonov izjavnega računa en izraz pretvorimo v drugega.

Normalni obliki, polni nabori

Osnovna konjunkcija je konjunkcija enega ali več literalov (izj. spremenljivka oz. njena negacija). Osnovna disjunkcija je je disjunkcija enega ali več literalov.

Disjunktivna normalna oblika je disjunkcija osnovnih konjunkcij, od katerih vsaka vsebuje vse izjavne spremenljivke (sestavljena je iz toliko literalov kot je izj. spremenljivk).

Dualna oblika DNO je konjunktivna normalna oblika, ki je konjunkcija osnovnih disjunkcij, ki prav tako vsebujejo toliko literalov, kot je izj. spremenljivk.

Da vsaka osnovna kon/disjunkcija vsebuje vse izj. spremenljivke pomeni, da je oblika zapisa polna. Vsak izjavni izraz lahko zapišemo v PDNO ali PKNO. To pomeni tudi, da vsak izjavni izraz lahko zapišemo samo z uporabo negacije, konjunkcije in disjunkcije.

Množica izj. veznikov, s katerimi lahko zapišemo vsak izj. izraz imenujemo *poln nabor izj. veznikov*

Sklepanje v izjavnem računu

Sklep s predpostavkami A1, A2, .. An in zaključkom B je pravilen, če je zaključek B resničen pri vseh tistih naborih izjavnih spremenljivk, pri katerih so resnične tudi vse predpostavke. Sklep ni pravilen, če obstaja nabor vrednosti spremenljivk, kjer so vse predpostavke resnične, zaključek pa je napačen oz. obstaja PROTIPRIMER.

Pravilom sklepanja pravimo tudi osnovni pravilni sklepi in so modus ponens, modus tollens, disjunktivni silogizem, hipotetični silogizem, združitev (konjunkcija), poenostavitev, pridružitev (disjunkcija).

Pogojni sklep

- zaključek ima obliko implikacije

Predpostavimo, da je antecédens pravilen. Če to drži, je tudi konsékvens resničen.

Sklep s protislovjem

Predpostavimo, da če je negacija zaključka ena od predpostavk, je sklep nepravilen.

Analiza primerov

- ena od predpostavk ima obliko disjunkcije

Sklep razdelimo na dva sklepa, kjer vsak dobi enega od členov disjunkcije za predpostavko. Za pravilnost prvotnega sklepa morata biti resnična oba delna sklepa (vezana s konjunkcijo)

PREDIKATNI RAČUN

Predikatni račun je nadgradnja izjavnega računa. Predikat je logična preslikava, v katero vstavljamo elementa iz področja pogovora. Predikat P(x) ni izjava, saj je njegova logična vrednost odvisna od x-a, ki ga vstavimo. Predikati so lahko eno ali večmestni. Enomestni predikati opisujejo lastnost elementa, večmestni pa opisujejo relacije med elementi.

Poznamo univerzalni in eksistenčni kvantifikator. Z univerzalnim kvantifikatorjem opisujemo posplošene konjunkcije (za vse x velja …), z eksistenčnim pa opisujemo posplošene disjunkcije (izmed vseh x obstaja vsaj eden, za katerega velja …). Kvantifikatorja vežeta tako močno kot negacija.

∀x P(x) ni izjava, saj je logična vrednost tega izraza odvisna od področja pogovora in pomena predikata P.

Izjavne formule

Atomi so termi vstavljeni v predikate. Termi so izjavne spremenljivke ter izjavne konstante. Izjavne formule definiramo induktivno:

F1. Atomi so izjavne formule,
F2. Če sta V in W izjavni formuli ter je x izjavna spremenljivka, potem so tudi (W [in] V), (W [ali] V) , … , (∀x W), (∃x W) izjavne formule.

Logične konstante in spremenljivke si predstavljamo kot 0-mestne predikate.

Doseg kvantifikatorja je najkrajša izjavna formula, ki se nahaja neposredno za lastno spremenljivko izbranega kvantifikatorja.

Izjavna shema oz. zaprta formula je izjavna formula brez prostih spremenljivk. Odprta izjavna formula je izjavna formula brez kvantifikatorjev.

Interpretacija izjavne formule

Z interpretacijo izjavno formulo spremenimo v izjavni izraz. To naredimo tako, da si izberemo **področje pogovora**, **pomen predikatov**, **pomen konstant** in **vrednost prostih spremenljivk**.

Zamenjava ali substitucija spremenljivke x s termom t: W(x/t) – vse proste nastope spremenljivke x v izjavni formuli W nadomestimo s t, tako definiramo pomen kvantifikatorjev. Zamenjava (x/t) ne vpliva na vezane vstope sprem. x. Spremenljivka x je v izj. formuli W zamenljiva s termom t, če nobenega prostega vstopa spremenljivke x ne dosega kvantifikator z lastno spremenljivko t.

Formula ∀x (∃x) W je resnična v interpretaciji I s področjem pogovora D, če je za vsak (če obstaja nek) d [pripada] D v tej interpretaciji resnična tudi formula W(x/d).

Enakovrednost izjavnih formul

Izjavna formula je splošno veljavna, če ima v vsaki interpretaciji logično vrednost 1 in neizpolnljiva, če ima v vsaki interpretaciji logično vrednost 0.

Formuli sta si enakovredni, če imata v vsaki interpretaciji isto logično vrednost. Enakovredni sta si natanko tedaj, ko je formula W [ekvivalenca] V splošno veljavna. Enakovrednosti izjavnih formul ne moremo preverjati po vsaki interpretaciji posebej (z resničnostno tabelo), saj je interpretacij neskončno mnogo. Enakovrednost preverjamo z uporabo zakonov predikatnega računa:

De Morganova zakona:

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

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

Zamenjava istovrstnih kvantifikatorjev:

$$\forall x\,\forall y\,(W) \sim \forall y\,\forall x\,(W)$$

$$\exists x\,\exists y\,(W) \sim \exists y\,\exists x\,(W)$$

Distributivnost:

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

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

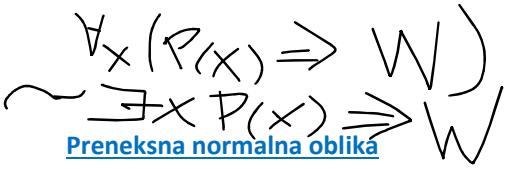
Če spremenljivka x v W ne nastopa:

$$\forall x(W \wedge P(x)) \sim W \wedge \forall x P(x)$$

$$\forall x(W \vee P(x)) \sim W \vee \forall x P(x)$$

$$\exists x(W \wedge P(x)) \sim W \wedge \exists x P(x)$$

$$\exists x(W \vee P(x)) \sim W \vee \exists x P(x)$$



Preneksna normalna oblika

V preneksni normalni obliki izjavne formule se vsi kvantifikatorji nahajajo na začetku formule. Vsako izjavno formulo lahko zapišemo s PNO. Uporabna je pri dokazovanju enakovrednosti dveh izjavnih formul z izpeljavo.

Postopek:

- Preimenujemo spremenljivke,
- Znebimo se implikacij in ekvivalenc,
- Z uporabo zakonov predikatnega računa kvantifikatorje prenesemo na začetek izjavne formule.

MNOŽICE

Množica je natančno določena s svojimi elementi, podamo jo lahko z naštevanjem elementov (samo končne množice) ali pa z uporabo izjavnih formul.

Univerzalna množica *S* je enaka področju pogovora teorije množic. Vsebuje vse elemente. Prazna množica {} je edina množica brez elementov.

Množica, ki ne vsebuje same sebe ne obstaja.

Množici z enim samim elementom pravimo singelton, množici z dvema elementoma pa par.

Enakost in vsebovanost

Množici A in B sta si enaki natanko tedaj, ko imata iste elemente. (A = B)

A je podmnožica množice B natanko tedaj, ko so vsi elementi množice A vsebovani tudi v množici B. ($A \subseteq B$)
A = B natanko tedaj ko je
$A \subseteq B$ in $B \subseteq A$.

A je prava podmnožica množice B natanko tedaj, ko so vsi elementi množice A vsebovani v množici B ter A in B si nista enaki.

Operacije z množicami

Operacija paru množic A in B priredi novo množico, ki je rezultat operacije.

- unija (vsi elementi, ki se pojavijo v kateri od množic)
- presek (vsi elementi, ki se pojavijo v obeh množicah)
- razlika (vsi elementi, ki pripadajo natanko eni od množic)
- simetrična razlika (vsi elementi, ki ne pripadajo preseku množic)
- komplement (množica elementov, ki ne pripadajo izbrani množici, pripadajo pa univerzalni množici)

Če je presek dveh množic enak 0, pravimo da sta množici disjunktni.

Prednost operacij:

^{c}	$\cap, \setminus$	$\cup, +$

Vsebovanosti in operacije

(i) *Če je* $A \subseteq B$, *potem je* $A \cup C \subseteq B \cup C$.

(ii) *Če je* $A \subseteq B$, *potem je* $A \cap C \subseteq B \cap C$.

(iii) $A \cap B \subseteq A \subseteq A \cup B$.

točki (i) in (ii) povesta, da je relacija vsebovanosti usklajena z operacijama unije in preseka.

Relacijo vsebovanosti lahko izrazimo na več načinov:

(a) $A \subseteq B$
(b) $A \cup B = B$
(c) $A \cap B = A$
(d) $A \setminus B = \emptyset$
(e) $B^c \subseteq A^c$

Enakosti z množicami

Ker so operacije z množicami definirane z uporabo logičnih operacij, lahko zakone izjavnega računa, enakovrednosti izjavnih izrazov lahko prepišemo v ustrezne enakosti z množicami. Konjunkcija -> presek, disjunkcija -> unija, negacija -> komplement in ekskluzivna disjunkcija -> simetrična razlika. Logični konstanti 0 in 1 ustrezata prazni ter univerzalni množici.

(napiši zakone iz str. 69, 70).

Reševanje sistemov enačb z množicami

Sisteme enačb z eno neznano množico rešimo tako, da najprej natančno določimo pogoje, pri katerih je sistem rešljiv, nato pa poiščemo vse množice X, ki ustrezajo danim enačbam.

Postopek

1. Sistem pretvorimo na eno samo enačbo, kjer je na eni strani enakosti prazna množica.
   a. A = {} in B = {} nt. ko je A ∪ B = {}
   b. A = B nt. ko je A + B = {}
2. določimo X.

Družine množic

Množica lahko vsebuje druge množice. Ne more pripadati sama sebi, lahko pa pripada neki drugi množici. Množicam množic pravimo družine množic.

Izberemo I – indeksno množico. Družina množic je preslikava A, ki vsakemu elementu z I določi množico A_i. Množice v družini imenujemo tudi člani te družine.

Unija družine A je množica vseh elementov, ki pripadajo vsaj enemu članu družine A, *presek družine A* pa je množica elementov, ki pripadajo vsem članom družine A.

$$\bigcup_{i \in \mathcal{I}} A_i = \{x \mid \exists i (i \in \mathcal{I} \wedge x \in A_i)\}$$

$$\bigcap_{i \in \mathcal{I}} A_i = \{x \mid \forall i (i \in \mathcal{I} \wedge x \in A_i)\}$$

Če je indeksna množica končna, potem je unija družine enaka uniji članov, presek družine pa preseku članov družine.

Družina množic A je pokritje množice B, če je unija družine A enaka B.

Družina množic A je razbitje množice B, če:

1. Družina A je pokritje množice B,
2. bloki (člani) družine A so neprazni,
3. bloki družine A so paroma disjunktni (nimajo skupnih elementov).

Potenčna množica

Potenčna množica množice A je družina vseh podmnožic množice A, vključno s prazno množico in množico A. Če ima množica A n elementov, ima potenčna množica množice A natanko 2^n elementov.

Kartezični produkt

Kartezični produkt A x B je množica vseh urejenih parov s prvo koordinato iz A in drugo iz B.

Namesto urejenih parov lahko definiramo tudi urejene trojice, četverke, n-terice. Dve n-terici sta enaki nt. ko se ujemata v vseh koordinatah.

Kartezični produkt ni komutativen, je pa asociativen.

(v zvezek napiši lastnosti iz str. 78)

RELACIJE

R je relacija v množici A, če je podmnožica kartezičnega produkta A x A. V dvomestni predikat definiran na PP A vstavljamo urejene pare elementov množice A. Množica R je podmnožica sestavljena iz urejenih parov, za katere je ta predikat resničen.

(a, b) ∈ R zapišemo aRb. (infiksno)

Primeri relacij so relacija vsebovanosti, enakovrednosti, manjše ali enako, univerzalna relacija (enaka A x A), prazna relacija, relacija identitete oz. enakosti (množica vseh urejenih parov z enakimi koordinatami).

Množica prvih koordinat iz parov v R je definicijsko območje (domena) R, množica drugih koordinat pa zaloga vrednosti R.

Če je R relacija v A in je B ⊆ A, potem je *zožitev* relacije R na množico B enaka R ∩ (B x B).

Lastnosti relacij

Refleksivna relacija: vsi elementi so v relaciji sami s sabo. (id, vsebovanost)

Simetrična relacija: če aRb potem bRa. (enakost, »sorodnik«)

Antisimetrična relacija: če aRb in bRa, potem je a = b. (vsebovanost, večje ali enako, manjše ali enako)

Tranzitivna relacija: če aRb in bRc, potem aRc. (večje, manjše, enakost)

Sovisna relacija: če a ni enak b, potem aRb ali bRa. (večje, manjše (ali enako))

Enolična relacija: če aRb in aRc, potem je b = c. (enakost, »zakonec«)

Operacije z relacijami

Če sta R in S relaciji v A, želimo da so rezultati operacij tudi relacije v A.

- unija, presek, razlika, sim. razlika
- komplement relacije (vsi pari A x A, ki niso v relaciji R)
- inverzna relacija (zamenjamo koordinati v vseh parih relacije, npr. večje in manjše)
- produkt relacij (xR * Sy n. tedaj, ko obstaja z: xRz in zSy.

(napiši enakosti z relacijami str. 85)

Zaradi asociativnosti produkta lahko definiramo potenciranje, pri množenju dveh potenc relacije ne smemo seštevati nasprotno predznačenih eksponentov.

Grafična predstavitev relacij in potence

Lastnosti relacije lahko določimo iz grafa. Relacija je refleksivna, če ima graf v vsaki točki zanko. Relacija je simetrična, če je med vsakima dvema točkama puščica v obe smeri, ali pa sploh ni puščice (ko sovpada z inverzno rel.). Relacija je antisimetrična, če v grafu ni dvostranskih puščic med različnimi elementi. Relacija je sovisna, če med poljubnima elementoma obstaja vsaj ena povezava. Relacija je enolična, če iz vsake točke v grafu izhaja največ ena puščica. Relacija je tranzitivna, če velja aR * Rb, torej aR^2b: če se lahko iz a z uporabo dveh zaporednih puščic premaknemo v b.

aR^nb velja, ko se lahko v grafu aRb v n korakih sprehodimo od a do b.

Ovojnice relacij

R je relacija v A. L je lastnost relacije. Če R nima lastnosti L, mogoče lahko z dodajanjem urejenih parov iz A, R dobi lastnost L. Najmanjšo tako relacijo imenujemo L-ovojnica relacije R:

1. $R \subseteq R_L$,
2. R_L ima lastnost L,
3. Če ima relacija S lastnost L in je $R \subseteq S$, potem velja $R_L \subseteq S$.

Vsaka lastnost ne dopušča ovojnice npr. antisimetričnost.

Refleksivna ovojnica R je enaka uniji R z id. Simetrična ovojnica R je enaka uniji R z njenim inverzom. Tranzitivna ovojnica R je unija vseh pozitivnih potenc relacije R (R^+) – od x do y v grafu R lahko pridemo v 1 ali več korakih. Tranzitivno-refleksivna ovojnica R je unija vseh nenegativnih potenc relacije R (R^*) – od x do y v grafu R pridemo v 0 ali več korakih.

Ekvivalenčna relacija

Relacija R v A je ekvivalenčna, če je refleksivna, simetrična in tranzitivna.

Zgledi: vzporednost, kongruenca v Z.

Ekvivalenčni razredi

R je ekvivalenčna relacija v A. Ekvivalenčni razred elementa a je množica vseh elementov množice A, ki so v relaciji z a.

Ekvivalenčni razredi so neprazni, saj vsak element pripada svojemu ekvivalenčnemu razredu. Če sta si dva elementa v relaciji (aRb), potem sta njuna ekvivalenčna razreda enaka.

Družina vseh ekvivalenčnih razredov množice A se imenuje faktorska oz. kvocientna množica množice A po ekvivalenčni relaciji R. (ozn. A/R)

R je ekvivalenčna relacija v množici A. Kvocientna množica A/R je **razbitje** množice A. Vsako razbitje množice A porodi ekvivalenčno relacijo.

aRb nt. tedaj, ko a in b pripadata istemu bloku razbitja.

Relacije urejenosti

Vse relacije urejenosti so tranzitivne.

Delna in linearna urejenosti

Delna urejenost je vsaka relacija, ki je refleksivna tranzitivna in antisimetrična

- $a \preccurlyeq b$ preberemo z "*a je pod b*",
- $a \prec b$ pomeni isto kot $a \preccurlyeq b$ in $a \neq b$, kar preberemo kot "*a je strogo pod b*",
- $a \succcurlyeq b$ in $a \succ b$ pomenita isto kot $b \preccurlyeq a$ in $b \prec a$, zvezi preberemo tudi kot "*a je nad b*" oziroma "*a je strogo nad b*",
- zapis $a \prec b \preccurlyeq c$ pomeni konjunkcijo $a \prec b$ in $b \preccurlyeq c$.

Primeri urejenosti so vsebovanost v družini množic, deljivost v naravnih št., večje in manjše ali enako.

Če je relacija R delna urejenost v množici A ter za elementa a, b velja a pod b in b pod a, potem sta si elementa primerljiva.

Če sta si vsaka dva elementa v A primerljiva, potem relaciji rečemo linearna urejenost. Linearna urejenost je delna urejenost, ki je sovisna.

Delna urejenost množice A lahko linearno ureja kako podmnožico množice A. Taka podmnožica je veriga.

Posebni elementi

(i) a je *minimalni element*, če za vsak $a' \in A$ velja $a' \not\prec a$,

(ii) a je *prvi element*, če za vsak $a' \in A$ velja $a \preccurlyeq a'$,

(iii) a je *maksimalni element*, če za vsak $a' \in A$ velja $a \not\prec$

(iv) a je *zadnji element*, če za vsak $a' \in A$ velja $a' \preccurlyeq a$.

V inverzni urejenosti (urejenosti z inverzno relacijo) sta minimalni in prvi element maksimalni in zadnji element.

V delni urejenosti je kvečjemu en prvi element. Če obstaja prvi element je to tudi edini minimalni element in obratno za zadnji element.

Minimalni element v linearni urejenosti je tudi prvi element in obratno, medtem ko delna urejenost dopušča več (neprazne množice družine množice A glede na vsebovanost – vsi singletoni so minimalni elementi) ali nobenega minimalnega elementa (relacija manjše ali enako v R).

Hassejev diagram

Tranzitivno refleksivna ovojnica delne urejenosti R v množici A je enaka R.

V množici A definiramo še relacijo neposrednega naslednika oz. predhodnika. Element a je neposredni predhodnik b, če je a strogo pod b in ne obstaja nek x, ki je nad a in pod b. Ta relacija ureja N, Z, relacijo vsebovanosti v potenčni množici …, ne ureja pa npr. Q ali R.

Dobra urejenost in dobra osnovanost

Delna urejenost je *dobra osnovanost*, če ima vsaka neprazna podmnožica množice A minimalni element. To velja, ko A ne vsebuje neskončnih padajočih verig.

Linearna urejenost je *dobra urejenost*, če ima vsaka neprazna podmnožica množice A minimalni element.

PRESLIKAVE

f ⊆ A × B je preslikava iz A v B če:

1. je relacija f enolična
2. definicijsko območje f je cela množica A

Družino vseh preslikav iz A v B označimo z B^A.

Lastnosti preslikav

Preslikava je INJEKTIVNA, če velja ∀x∀y (f(x) = f(y) ➔ x = y). (injekcija)

Preslikava je SURJEKTIVNA, če velja Z_f = B. (surjekcija)

Preslikava je BIJEKTIVNA, če je injektivna in surjektivna. (bijekcija)

Inverzna preslikava

Za vsako preslikavo lahko konstruiramo inverzno relacijo. Ta relacija je preslikava, če je originalna preslikava injekcija, inverzna preslikava slika iz B v A, če je originalna preslikava bijekcija.

Kompozitum preslikav

(g ◦ f)(x) = (f * g)(x) = g(f(x))

Če sta f in g enolični, je tudi g(f(x)) enolična. Če f slika iz A v B in g slika iz B v C, potem g ◦ f slika iz A v C.

$f \circ id_A = id_B \circ f = f$

Kompozitum preslikav je asociativen, ni pa komutativen.

(i) *Če sta* f *in* g *injektivni, potem je tudi preslikava* $g \circ f : A \to C$ *injektivna.*
(ii) *Če sta* f *in* g *surjektivni, potem je tudi preslikava* $g \circ f : A \to C$ *surjektivna.*
(iii) *Če sta* f *in* g *bijektivni, potem je tudi preslikava* $g \circ f : A \to C$ *bijektivna.*

(i) *Če je* $g \circ f : A \to C$ *injektivna, potem je injektivna tudi preslikava* f.
(ii) *Če je* $g \circ f : A \to C$ *surjektivna, potem je surjektivna tudi preslikava* g.

Slike in praslike

f: A ➔ B

Preslikavo Potenčne množice A v potenčno množico B imenujemo *slika* f (F), preslikavo potenčne množice B v potenčno množico A pa *praslika* f (F^{-1}).

Preslikava praslike v splošnem ni inverzna preslikava preslikavi slike!

$$F : \mathcal{P}A \to \mathcal{P}B,$$
$$F(A') = \{f(a') ; a' \in A'\} \subseteq B,$$

$$F^{-1} : \mathcal{P}B \to \mathcal{P}A,$$
$$F^{-1}(B') = \{a' ; a' \in A \wedge f(a) \in B'\} \subseteq A.$$

$$\text{(i) } F(A' \cup A'') = F(A') \cup F(A'')$$
$$\text{(ii) } F(A' \cap A'') \subseteq F(A') \cap F(A'')$$
$$\text{(iii) } F^{-1}(B' \cup B'') = F^{-1}(B') \cup F^{-1}(B'')$$
$$\text{(iv) } F^{-1}(B' \cap B'') = F^{-1}(B') \cap F^{-1}(B'')$$

F je inverzna preslikava F^{-1} natanko tedaj, ko je f bijekcija.

MOČ KONČNIH MNOŽIC

Množici A in B sta enako močni, če med njima obstaja bijektivna preslikava f: A ➔ B : |A| = |B|. Če velja to, velja tudi |B| = |A|, saj je inverzna preslikava bijekcije prav tako bijekcija. Velja tudi : |A| = |B| && |B| = |C| ➔ |A| = |C|, saj je kompozitum bijekcij A ➔ B in B ➔ C bijekcija A ➔ C.

Končne množice

Množica je neskončna, če obstaja kaka njena prava podmnožica, za katero velja |A'| = |A|. Množica je končna, če ni neskončna. (npr. : množica N je neskončna, prav tako pa je neskončna množica sodih nar. št. |N| = |S|

Dirichletov princip

B je končna množica, f: B ➔ B.

f je injekcija ⇔ f je surjekcija

Moč končne množice je enaka številu njenih elementov, {} je edina množica z močjo 0.

Moč končnih množic in operacije

Kartezični produkt: |A x B| = |A| * |B|

Družina preslikav: $|A^B| = |A|^{|B|}$

Potenčna množica: $|PA| = 2^{|A|}$

Razlika množic: |A \ B| = |A| - |A ∩ B|

Unija dveh množic:
|A ∪ B| = |A| + |B| - |A ∩ B|

Princip vključitve in izključitve

Ko računamo moč unije elementov, prištejemo vse lihe preseke elementov (preseke z lihim številom elementov) in odštejemo vse sode preseke elementov.

OSNOVE TEORIJE ŠTEVIL

Celi del realnega števila

Spodnji celi del realnega števila je realno število, ki mu odrežemo decimalke, je manjši od originalnega realnega števila. – navzdol zaokroženo.

Zgornji del realnega števila je navzgor zaokroženo število po prvi decimalki.

$$\lceil a \rceil = -\lfloor -a \rfloor \text{ in } \lfloor a \rfloor = -\lceil -a \rceil,$$

$$\text{če } a \notin \mathbb{Z}, \text{ potem je } \lceil a \rceil - \lfloor a \rfloor = 1.$$

Deljivost celih števil

n in m sta celi števili:

n = k * m + r, 0 <= r < m

k … celoštevilski koeficient, r … ostanek, k = (sp. cel.) m/n.

$D_{m,n}$: {d : d|m in d|n in d /= 0} – množica vseh skupnih deliteljev m in n.

$V_{m,n}$: {v : m|v in n|v in v >= 0} – množica vseh večkratnikov m in n.

Deljivost v naravnih številih

V množici naravnih števil je relacija deljivosti delna urejenost. Njen maksimalni element je 0, saj ga delijo vsa naravna števila, njen minimalni element pa je 1, ki deli vsa naravna števila.

Lastnosti gcd in lcm:

- idempotenca: gcd(a,a) = a
- komutativnost: lcm(a,b) = lcm(b,a)
- asociativnost:
  gcd(a, gcd(b,c)) = gcd(gcd(a,b), c)
- distributivnost:
  - gcd(lcm(a,b), lcm(a,c)) = lcm(a, gcd(b,c))
  - lcm(gcd(a,b), gcd(a,c)) = gcd(a, lcm(b,c))
- gcd(0,n) = |n|

Razširjeni Evklidov algoritem

Z REA izračunamo gcd. Pogoji:

gcd(m,n) : m > 0, n > 0, m > n

m in n sta naravni števili, linearna kombinacija m in n je sm + tn.

m in n izražamo z linearnimi kombinacijami, rezultat kombinacije pa je r oz. ostanek. Ostanek v zadnji vrstici REA označimo z r_z. $r_z = 0$.

gcd(m,n) je enak zadnjemu neničelnemu ostanku r_{z-1} REA.

lcm(m,n) preberemo iz zadnje vrstice, tako da pomnožimo enega od produktov v linearni kombinaciji na levi strani (s_z * m ALI t_z * n).

Tuja števila

Števili m in n sta si tuji, če je gcd(m,n) = 1. Oznaka: ⊥

1 je tuje vsem številom, tudi samemu sebi.

m in n sta celi št., m > 0

- gcd(m, n) = gcd(m, n mod m)
- m ⊥ n nat. tedaj ko m ⊥ (n mod m)

a, b in c so cela števila. Če a deli produkt b in c, ter je a ⊥ b, potem a deli c.

Če sta a in b naravni števili, potem je gcd(a, b) * lcm(a, b) = a * b.

Linearne diofantske enačbe

LDE je enačba oblike ax + by = c. Parametra a, b sta koeficienta, parameter c pa je desna stran enačbe. Enačba je rešljiva nat. tedaj, ko gcd(a, b) deli parameter c.

Vse rešitve enačbe dobimo s formulo:

$$x_t = x_0 + t \cdot \frac{b}{\gcd(a,b)},$$
$$y_t = y_0 - t \cdot \frac{a}{\gcd(a,b)},$$

Praštevila

Praštevilo je število, ki ima natanko dva delitelja v množici naravnih števil in velja: ∀p : p⊥a OR p|a.

Vsako naravno število n>1 je deljivo s kakim od praštevil, torej lahko vsako tako naravno število zapišemo kot produkt praštevil. Množica praštevil je neskončna.

Eulerjeva funkcija

Eulerjeva funkcija je preslikava iz naravnih v naravna št., definirana je kot moč množice ϕ(n), kjer je k ∈ N, 0<k<=n in k⊥n. Je št. n tujih števil, ki so manjša od n.

ϕ(praštevilo) = p – 1;

ϕ(praštevilo$^{n:\, n>0}$) = $p^n - p^{n-1}$

Naravni števili a, b ≠ 0: Eulerjeva funkcija produkta ab je enaka produktu Eulerjevih funkcij teh dveh števil.

Modulska aritmetika

Celi števili a in b sta kongruentni po modulu m, če pri deljenju z m dasta isti ostanek.

a ≡ b (mod m) ⇔ a mod m = b mod m ⇔ m|(a – b)

*Nekaj pravil v zvezku, učb str. 145

Števil pri kongruenci praviloma ne krajšamo: 5 * 6 ≡ 9 * 6 (mod 8) velja, 5 ≡ 9 (mod 8) pa NE velja. Pravilo krajšanja lahko uporabimo le, če krajšamo faktor, ki je tuje število m.

Eulerjev izrek

Če je št. a tuje modulu m, potem s potenciranjem števila a dobimo število, ki je kongruentno 1.

a^ϕ(m) ≡ 1 (mod m); a⊥m

Mali Fermatov izrek

a je celo število, p je praštevilo:

a^p ≡ a (mod p)

Računanje z ostanki

Kongruenca po modulu m je ekvivalenčna relacija. Ekvivalenčni razred m v tej relaciji so ostanki po modulu m.

$$Z_m = \mathbb{Z}/\text{mod } m.$$?

Ostanek a je obrnljiv, če obstaja x:

a * x ≡ 1 (mod m)

Neničelni ostanek a je delitelj niča, če obstaja neničelni x:

a * x ≡ 0 (mod m)

/~~ Sori ne da se mi več teh jebenih modulov delat ^^ ~~\

PERMUTACIJE

Permutacija je bijektivna preslikava A → A. Omejimo se na končne množice naravnih števil.

Zapis permutacije

Dolžino permutacije določa moč množice A. Družina vseh permutacij dolžine n je **simetrična grupa reda n**, oznaka S_n.

Permutacije lahko zapišemo tabelarično. št. a se slika v št. b: ϕ(a) = b. Številu, ki se slika samo vase pravimo **negibna točka** permutacije.

Permutacijo majhne dolžine lahko interpretiramo kot permutacijo večje dolžine, če tabelici dodajamo stolpce, ki se slikajo sami vase. V permutaciji id (identitete) se vsa števila slikajo sama vase. Permutacija id je pripada simetričnim grupam vseh redov.

Produkt permutacij in inverzna permutacija

Pri množenju permutacij uporabimo pravila za produkt relacij. Produkt permutacij ni komutativna relacija.

Inverzno permutacijo dobimo tako, da zamenjamo vrstici, prvo vrstico uredimo po vrsti. Produkt permutacije s svojim inverzom je permutacija identitete.

Simetrična grupa

(V zvezku, učb str. 158)

Zapis z disjunktnimi cikli

Graf permutacije je sestavljen iz enega ali več disjunktnega cikla (nimajo skupnih števil). Če ima permutacija 3 cikle dolžine 1, 5 in 6 ima **ciklično strukturo permutacije** [1, 5, 6].

Ciklu dolžine k pravimo k-cikel. 2-cikel je transpozicija, 1-cikel pa negibna točka. Ciklična permutacija ima en sam cikel (razen morebitnih negibnih točk).

Ciklična struktura produkta permutacij je neodvisna od vrstnega reda faktorjev.

Inverzno permutacijo z disjunktnimi cikli zapišemo tako, da permutacijo prepišemo od zadaj naprej.

Potenciranje permutacij

Ko potenciramo permutacijo, potenciramo vsak disjunktni cikel posebej.

α^1 = (1 2 3 4 5 6)

α^0 = (1) (2) (3) (4) (5) (6)

α^6 = (1) (2) (3) (4) (5) (6)

$\beta^n = \beta_1^n * \beta_2^n * \dots$

Če je dolžina cikla enaka k, potem je $\alpha_x^n = \alpha^{n \bmod k}$

Če je α ciklična permutacija dolžine n, potem ima α^k točno gcd(n, k) ciklov dolžine n / gcd(n, k)

Red permutacije ord(α) je najmanjši pozitivni koeficient permutacije α, kjer je α^k = id → **lmc** dolžin ciklov permutacije.

Parnost permutacij

Vsako permutacijo lahko zapišemo kot produkt transpozicij, ne nujno disjunktnih in ne enolično (na več načinov).

id = (1) (2) (3) = (1 2) (1 2) (2 3) (2 3) (3 1) (3 1)

Recept za zapis permutacije kot produkta transpozicij:

$$(1\,2\,3\,4\,5\,6\,7) = (1\,2)(1\,3)(1\,4)(1\,5)(1\,6)(1\,7)$$
$$(1\,3\,9\,2\,7)(4\,6\,5\,8) = (1\,3)(1\,9)(1\,2)(1\,7)(4\,6)(4\,5)(4\,8)$$
$$(1\,2\,4)(3\,6\,5)(7)(8\,9) = (1\,2)(1\,4)(3\,6)(3\,5)(8\,9)$$

Če permutacijo zapišemo s transpozicijami na več različnih načinov bo število : št. ciklov MOD 2 enako pri vseh.

Permutacija α je **soda**, če jo lahko zapišemo kot produkt sodega števila transpozicij. Produkt dveh isto parnih permutacij bo soda permutacija.

Permutacija α je **liha**, če jo lahko zapišemo kot produkt lihega števila transpozicij. produkt dveh različno parnih permutacij bo liha permutacija.

Sodost ali lihost = parnost permutacije.

Števili i, j, kjer i < j sta si v permutaciji **v inverzu**, če se v spodnji vrstici tabelaričnega zapisa permutacije pojavita v napačnem vrstnem redu. Število inverzij v α označimo z inv(α). Pove nam »oddaljenost« permutacije od identitete. Če je inv(α) sodo število, je permutacija soda, sicer je liha.

Potenčna enačba s permutacijami

$\pi^k = \alpha$

Če je α en sam n-cikel, je tudi π lahko samo n-cikel. Enačba je rešljiva samo, če je gcd(n, k) = 1.

Če je α več ciklov iste dolžine n, je π sestavljena iz ciklov dolžin, ki lahko razpadejo na več n ciklov.

Če je α sestavljena iz več ciklov različnih dolžin, enako velja tudi za π. Nalogo razcepimo na več manjših nalog prejšnjih tipov.