Diskretna matematika

Zoran Ognjanović

zorano@mi.sanu.ac.rs

MF Beograd, 2011/12

Diskretna matematika (2RA, 2RB, 2LA, 2LB, 2MNVA, 2MNVB):

- predavanja: 2 časa nedeljno
- asistenti:
  - Angelina Ilić-Stepić (2RA, 2RB, 2MNVA) i
  - Goran Đanković (2LA, 2LB, 2MNVB)
- pravila polaganja:
  - polaganje od januara 2012. godine
  - predispitne obaveze 30 poena (2 kolokvijuma)
  - ispit 70 poena (pismeni, usmeni)
  - seminarski radovi
  - za 6 je potrebno 50 poena
- Internet-stranica predmeta u pripremi
  `http://www.mi.sanu.ac.rs/~zorano/dm/dm.html`

Literatura:

- R. Dacić, Elementarna kombinatorika, Matematički institut, Beograd, 1977.
  http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/482/RadeDacicElementarnaKombinatorika.PDF?sequence=1
- K. Ghilezan, B. Latinović, Bulova algebra i primene, Matematički institut, Beograd, 1977.
  http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/434/KoriolanGilezan
- A. Kron, Elementarna teorija skupova, Matematički institut, Beograd, 1992.
- Ž. Mijajlović, Algebra 1, MILGOR, Beograd, 1998.
  http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/462/ZarkoMijajlovicAlgebra.pdf?sequence=1
- Z. Ognjanović, N. Krdžavac, Uvod u teorijsko računarstvo, FON, Beograd, 2004.
  http://www.mi.sanu.ac.rs/~zorano/ti/TeorijskoRacunarstvo.pdf

Diskretna matematika proučava *diskretne objekte, njihova svojstva i odnose*. Glavni ciljevi:

- definisanje važnih diskretnih formalnih sistema i odgovarajućih tehnika zaključivanja i davanje motiva za njihovu upotrebu u konkretnim primenama u računarstvu,
- razumevanje formalnih dokaza na kojima se zasniva matematičko rezonovanje i
- uvođenje opštih algoritamskih postupaka rešavanja problema.

Skupovi

Pojam skupa je jedan od osnovnih u matematici.
Notacija:

- simbol $\in$ označava pripadanje elementa skupu, tj.
  - $a \in A$ znači da element a pripada skupu A, dok
  - $a \notin A$ znači da element a ne pripada skupu A, tj. $\neg(a \in A)$,
- skupovi (A, B, ...), elementi (a, b, ...);
  skupovi prirodnih, celih i racionalnih brojeva: $\mathbb{N}$ ($0 \in \mathbb{N}$), $\mathbb{Z}$ i $\mathbb{Q}$,
- $\emptyset$ – prazan skup, tj. skup koji ne sadrži ni jedan element, $\forall x(x \notin \emptyset)$.

Skupovi

Reprezentacija skupa:

- *ekstenzionalno*, tj. navođenjem svih elemenata skupa između vitičastih zagrada, na primer $\{a, b, c\}$, $\{1, 2, 3, \ldots, 17\}$, ili $\{2, 4, 6, \ldots\}$,
- *intenzionalno*, tj. navođenjem osobine koju imaju elementi skupa i samo oni, na primer $\{x : P(x)\}$, što se čita kao skup svih x za koje važi $P(x)$,

Skupovi

Example

- $\{1, 2, 3\}$ sadrži elemente - brojeve 1, 2 i 3.
- $\{\{1, 2\}, \{\{3\}, 2\}, \{1\}\}$ sadrži elemente (koji su i sami takođe skupovi): $\{1, 2\}$, $\{\{3\}, 2\}$ i $\{1\}$.
- $\{1, 2, 3, \ldots, 17\}$, oznaka $\ldots$ zamenjuje eksplicitno navođenje svih prirodnih brojeva između 3 i 17
- $\{2, 4, 6, \ldots\}$ oznaka $\ldots$ zamenjuje (neograničenu) listu svih parnih brojeva većih od 6

Skupovi

Example

Zapisi

- intenzionalni:
  $\{x : x$ je prirodan broj manji od 100 i kvadrat prirodnog broja $\}$
- ekstenzionalni: $\{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\}$

predstavljaju isti skup.

Skupovi

Značajan vid intenzionalnog predstavljanja skupova – osobina koja karakteriše elemente skupa se opisuje nekim postupkom.

Example

Skup $\mathbb{N}$ prirodnih brojeva može se definisati na sledeći način:

1. $0 \in \mathbb{N}$,
2. za bilo koji x, ako je $x \in \mathbb{N}$, onda je i $x + 1 \in \mathbb{N}$ i
3. $\mathbb{N}$ sadrži one i samo one x dobijene koracima 1 i 2.

Postupak je induktivan, tj. zadaje se početni element, kao i način za generisanje svih narednih elemenata.
Koraci 1 i 2 generišu prirodne brojeve, dok korak 3 obezbeđuje da se recimo 0.5 i a ne mogu naći u skupu.

Skupovi

Definition

Skup A je *podskup* skupa B, a skup B je *nadskup* skupa A, u oznaci $A \subset B$, odnosno $B \supset A$, ako važi da je svaki element skupa A ujedno i element skupa B, odnosno $\forall x(x \in A \rightarrow x \in B)$.
Skupovi A i B su *jednaki*, $A = B$, ako je $A \subset B$ i $B \subset A$, odnosno $\forall x(x \in A \leftrightarrow x \in B)$.
Skup A je *pravi podskup* skupa B, ako je $A \subset B$ i nije $A = B$.

Skupovi

- za svaki skup A je $\emptyset \subset A$
- svaka dva prazna skupa su međusobno jednaka
- za svaki skup A važi $A \subset A$ i $A = A$
- redosled navođenja elemenata skupa nije od značaja, tako da su skupovi $\{1, 2\}$ i $\{2, 1\}$ jednaki
- višestruko navođenje istog elementa ne utiče na formiranje skupa, tako da je $\{a, b, a\} = \{a, b\} = \{b, a, a, a, a\}$.
- A je pravi podskup skupa B: $A \subsetneq B$.

Skupovi

Example

- $A = \{1, 2, 3\}$,
- $B = \{1, 2, \{1, 2, 3\}\}$ i
- $C = \{1, 2, 3, \{1, 2, 3\}\}$.
- 1, 2 i $\{1, 2, 3\} \in B$,
- $\{1\} \subset B$,
- $\{1, 2, 3\} \not\subset B$, jer $3 \in \{1, 2, 3\}$, ali $3 \notin B$.
- $A \in B$, ali i $A \not\subset B$.
- $A \in C$ i $A \subset C$.

Skupovi

Definition

Partitivni skup skupa A, u oznaci $\mathbb{P}(A)$, je skup svih podskupova od A, $\mathbb{P}(A) = \{B : B \subset A\}$.

Example

- za svaki skup A, $\emptyset \subset A$ i $A \subset A$, onda je $\emptyset \in \mathbb{P}(A)$ i $A \in \mathbb{P}(A)$
- $A = \{a, b\}$, $\mathbb{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Skupovi

Redosled elemenata u nekom skupu nije od značaja, tako da je $\{a, b\} = \{b, a\}$. Međutim, nekada je bitno da se istakne redosled, na primer tačke sa koordinatama $(6, 2)$ i $(2, 6)$ se razlikuju.

Definition

Uređeni par objekata x i y, u oznaci $\langle x, y \rangle$, je skup

$$\{\{x\}, \{x, y\}\}.$$

Pri tome, x je prva, a y druga koordinata (projekcija, komponenta) uređenog para $\langle x, y \rangle$.

Dva uređena para su jednaka ako i samo ako su im jednake odgovarajuće koordinate.
Pojam uređenog para se prirodno uopštava na (uređenu) k-torku objekata, u oznaci $\langle x_1, x_2, \ldots, x_k \rangle$, u kojoj se tačno zna ko je koja od k-koordinata.

Skupovi

Theorem

Uređeni parovi $\langle x, y\rangle$ i $\langle a, b\rangle$ su jednaki ako i samo ako važi $x = a$ i $y = b$.

Proof.

- ($\Rightarrow$) $\langle x, y\rangle$ je jednočlan skup ako i samo ako je $x = y$
- Neka je $\langle x, y\rangle = \langle a, b\rangle$
- Ako je $x = y$, onda je i $a = b$, a zatim i $x = y = a = b$
- Ako je $x \neq y$ (mora biti i $a \neq b$)
- $\langle x, y\rangle$ i $\langle a, b\rangle$ sadrže po jedan jednočlan i jedan dvočlan skup
- $x = a$, $\{x, y\} = \{a, b\}$, $y \in \{a, b\}$
- ako $y = a$, onda $x = y$, što nije, tako da je $y = b$
- ($\Leftarrow$) ako važi $x = a$ i $y = b$, trivijalno sledi jednakost uređenih parova

Skupovi

Definition

Dekartov proizvod skupova X_1, X_2, ..., X_k, u oznaci $X_1 \times X_2 \times \cdots \times X_k$, ili $\times_{i=1}^{k} X_i$, je skup svih uređenih k-torki $\langle x_1, x_2 \ldots, x_k \rangle$, za koje je $x_1 \in X_1$, $x_2 \in X_2$, ..., $x_k \in X_k$, tj.

$$X_1 \times X_2 \times \cdots \times X_k = \{\langle x_1, x_2 \ldots, x_k \rangle : x_1 \in X_1, x_2 \in X_2, \ldots, x_k \in X_k\}.$$

Ako je $X_1 = X_2 = \ldots = X_k$, onda se $X_1 \times X_2 \times \cdots \times X_k$ obično označava sa X_1^k.

Skupovi

Example

Neka su skupovi predmeta za izborne blokove u trećem i četvrtom semestru:

- $\mathrm{ML1} = \{\mathrm{DiskretnaMatematika}, \mathrm{FinansijskaMatematika}\}$, i
- $\mathrm{ML2} = \{\mathrm{Filozofija}, \mathrm{ProgramskiPaketiZaMatematiku}\}$.

Tada $\mathrm{ML1} \times \mathrm{ML2}$ predstavlja moguće izbore studenata:

$$\begin{aligned}\{&\langle \mathrm{DiskretnaMatematika} \ , \ \mathrm{Filozofija}\rangle,\\ &\langle \mathrm{DiskretnaMatematika} \ , \ \mathrm{ProgramskiPaketiZaMatematiku}\rangle,\\ &\langle \mathrm{FinansijskaMatematika} \ , \ \mathrm{Filozofija}\rangle,\\ &\langle \mathrm{FinansijskaMatematika} \ , \ \mathrm{ProgramskiPaketiZaMatematiku}\rangle\}.\end{aligned}$$

Relacije

Pojmovi relacija i funkcija spadaju takođe u osnovne matematičke koncepte i uopštavaju osobine konretnih relacija i funkcija, poput $\geq$ ili x^2, na konkretnim matematičkim strukturama.

Definition

Neka su $X_1, X_2, \ldots, X_k$ skupovi. *Relacija* (dužine ili arnosti k, nad skupovima $X_1, X_2, \ldots, X_k$) je bilo koji podskup Dekartovog proizvoda $X_1 \times X_2 \times \cdots \times X_k$.

- ako $X_1 = X_2 = \ldots = X_k$,relacija je podskup od X_1^k
- ako su elementi $x_1 \in X_1$, $x_2 \in X_2$, $\ldots$, $x_k \in X_k$ u relaciji $R \subset X_1 \times X_2 \times \cdots \times X_k$, piše se $\langle x_1, x_2 \ldots, x_k \rangle \in R$ ili u prefiksnom zapisu $R(x_1, x_2 \ldots, x_k)$
- relacije dužine 2, ili *binarne relacije*, aRb ako su a i b u relaciji
- $\langle a, b \rangle \notin R$, ili $\neg R(a, b)$, odnosno $\neg(aRb)$

Relacije

Example

Neka su A skup reka i B skup država. Jednu binarnu relaciju $\mathrm{R} \subset \mathrm{A} \times \mathrm{B}$ možemo definisati kao: $\mathrm{R}(\mathrm{a}, \mathrm{b})$ akko reka $\mathrm{a} \in \mathrm{A}$ protiče kroz državu $\mathrm{b} \in \mathrm{B}$. Tada je:

- $\mathrm{R}(\mathrm{Dunav}, \mathrm{Austrija})$, $\mathrm{R}(\mathrm{Dunav}, \mathrm{Mađarska})$ i
- $\neg\mathrm{R}(\mathrm{Volga}, \mathrm{Italija})$.

Relacije

Definition

Kompozicija relacija $\mathrm{R} \subset \mathrm{A} \times \mathrm{B}$ i $\mathrm{S} \subset \mathrm{B} \times \mathrm{C}$, u oznaci $\mathrm{S} \circ \mathrm{R}$ je binarna relacija $\{\langle \mathrm{a}, \mathrm{c} \rangle \subset \mathrm{A} \times \mathrm{C}\}$ za koju je $\mathrm{a}(\mathrm{S} \circ \mathrm{R})\mathrm{c}$ ako i samo postoji $\mathrm{b} \in \mathrm{B}$ tako da $\mathrm{R}(\mathrm{a}, \mathrm{b})$ i $\mathrm{S}(\mathrm{b}, \mathrm{c})$.

Treba obratiti pažnju na redosled navođenja relacija. Naime, iako je reč o kompoziciji relacija R i S, relacija R se navodi "iza" S, odnosno relacija S je u zapisu levo od R.

Relacije

Example

Neka je A skup osoba i neka su relacije R i S definisane nad A^2 sa: $\mathrm{R}(\mathrm{x}, \mathrm{y})$ ako i samo ako je x majka od y, odnosno $\mathrm{S}(\mathrm{x}, \mathrm{y})$ ako i samo ako je x otac od y. Tada je $\mathrm{x}(\mathrm{S} \circ \mathrm{R})\mathrm{y}$ ako i samo ako postoji $\mathrm{z} \in \mathrm{A}$ tako da je x majka od z i z je otac od y. Drugim rečima $\mathrm{x}(\mathrm{S} \circ \mathrm{R})\mathrm{y}$ ako i samo ako je x baba po očevoj liniji od y.

Relacije

Example

Interesantni primeri relacija su: univerzalna, prazna, indentična i inverzna. U slučaju relacija arnosti 2 nad skupovima A i B, za njih se koriste oznake:

- za univerzalnu relaciju $\mathrm{U} = \mathrm{A} \times \mathrm{B}$,
- za praznu relaciju (koja ne sadrži ni jedan uređeni par) $\emptyset$,
- za relaciju identiteta $\mathrm{I} = \{\langle \mathrm{a}, \mathrm{b} \rangle : \mathrm{a} = \mathrm{b}\}$ i
- za inverznu relaciju $\mathrm{R}^{-1} \subset \mathrm{B} \times \mathrm{A}$ relacije $\mathrm{R} \subset \mathrm{A} \times \mathrm{B}$, $\mathrm{R}^{-1} = \{\langle \mathrm{b}, \mathrm{a} \rangle : \langle \mathrm{a}, \mathrm{b} \rangle \in \mathrm{R}\}$.

Relacije

Osobine binarnih relacija:

Definition

Neka je A skup i binarna relacija $\mathrm{R} \subset \mathrm{A}^2$. Tada je R:

- *refleksivna* ako i samo ako je $(\forall \mathrm{x} \in \mathrm{A})\mathrm{R}(\mathrm{x}, \mathrm{x})$,
- *irefleksivna* ili *striktna* ako i samo $(\forall \mathrm{x} \in \mathrm{A})\neg\mathrm{R}(\mathrm{x}, \mathrm{x})$,
- *simetrična* ako i samo ako $(\forall \mathrm{x}, \mathrm{y} \in \mathrm{A})(\mathrm{R}(\mathrm{x}, \mathrm{y}) \to \mathrm{R}(\mathrm{y}, \mathrm{x}))$,
- *antisimetrična* ako i samo ako $(\forall \mathrm{x}, \mathrm{y} \in \mathrm{A})(\mathrm{R}(\mathrm{x}, \mathrm{y}) \wedge \mathrm{R}(\mathrm{y}, \mathrm{x}) \to \mathrm{x} = \mathrm{y})$,
- *tranzitivna* ako i samo ako $(\forall \mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathrm{A})(\mathrm{R}(\mathrm{x}, \mathrm{y}) \wedge \mathrm{R}(\mathrm{y}, \mathrm{z}) \to \mathrm{R}(\mathrm{x}, \mathrm{z}))$.

Relacije

Example

Neka je $\mathbb{N}$ skup prirodnih brojeva. Tada je relacija $\mathrm{R} \subset \mathbb{N}^2$, definisana sa $\mathrm{R}(\mathrm{a}, \mathrm{b})$ ako i samo ako je $\mathrm{a} \leq \mathrm{b}$:

- refleksivna, jer $(\forall \mathrm{x} \in \mathbb{N})\mathrm{x} \leq \mathrm{x}$
- antisimetrična, jer za sve $\mathrm{x}, \mathrm{y} \in \mathbb{N}$ iz $\mathrm{x} \leq \mathrm{y}$ i $\mathrm{y} \leq \mathrm{x}$ sledi $\mathrm{x} = \mathrm{y}$ i
- tranzitivna, jer za sve $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathbb{N}$ iz $\mathrm{x} \leq \mathrm{y}$ i $\mathrm{y} \leq \mathrm{z}$ sledi $\mathrm{x} \leq \mathrm{z}$,

ali nije simetrična, jer na primer važi $1 \leq 2$, ali nije $2 \leq 1$.
Slično: relacija $\mathrm{R} \subset \mathbb{P}(\mathrm{A})^2$, definisanu sa $\mathrm{R}(\mathrm{x}, \mathrm{y})$ ako i samo ako je $\mathrm{x} \subset \mathrm{y}$, za proizvoljni skup A.

Relacije

Example

Relacija $\mathrm{P} \subset \mathbb{N}^2$, definisana sa $\mathrm{P}(\mathrm{a}, \mathrm{b})$ ako i samo ako je $\mathrm{a} < \mathrm{b}$ je striktna, antisimetrična i tranzitivna.
Relacija $\mathrm{Q} \subset \mathbb{N}^2 \times \mathbb{N}^2$, definisana sa $\mathrm{Q}(\langle \mathrm{a}, \mathrm{b} \rangle, \langle \mathrm{c}, \mathrm{d} \rangle)$ ako i samo ako je $\mathrm{a} + \mathrm{d} = \mathrm{b} + \mathrm{c}$ nije antisimetrična jer važi $\mathrm{Q}(\langle 1, 2 \rangle, \langle 2, 3 \rangle)$ i $\mathrm{Q}(\langle 2, 3 \rangle, \langle 1, 2 \rangle)$, pošto je $1 + 3 = 2 + 2$, ali nije $\langle 1, 2 \rangle = \langle 2, 3 \rangle$. Ova relacija jeste refleksivna, simetrična i tranzitivna.

Relacije

Vrste relacija:

Definition

Neka je A skup i binarna relacija $\mathrm{R} \subset \mathrm{A}^2$. Tada je R relacija:

- *ekvivalencije* ako i samo ako je refleksivna, simetrična i tranzitivna,
- *parcijalnog uređenja (poretka)* ako i samo je refleksivna, antisimetrična i tranzitivna,
- *totalnog* ili *linearnog uređenja (poretka)* ako i samo ako je to relacija parcijanog uređenja za koju je $(\forall \mathrm{x}, \mathrm{y} \in \mathrm{A})(\mathrm{R}(\mathrm{x}, \mathrm{y}) \vee \mathrm{R}(\mathrm{y}, \mathrm{x}))$.

Ponekad se antisimetrična i tranzitivna relacija koja je refleksivna naziva relacija *slabog (parcijalnog) uređenja*, dok je antisimetrična i tranzitivna relacija koja je irefleksivna - relacija *striktnog (parcijalnog) uređenja*.

Relacije ekvivalencije

Example

Neka su $\mathbb{N}$ i $\mathbb{Z}$ skupovi prirodnih i celih brojeva i $n \in \mathbb{N}$, takav da je $n > 0$. Tada je relacija (kongruencije po modulu n) $\equiv_n \subset \mathbb{Z}^2$, definisana sa

$$a \equiv_n b \text{ ako i samo ako je } a - b = k \cdot n, \text{ za neki } k \in \mathbb{Z}$$

jedna relacija ekvivalencije:

- refleksivnost važi jer je $a - a = 0 \cdot n$,
- simetričnost važi jer iz $a - b = k \cdot n$ sledi da je $b - a = -k \cdot n$ i
- tranzitivnost važi jer iz $a - b = k \cdot n$ i $b - c = l \cdot n$ sledi da je $a - c = (a - b) + (b - c) = k \cdot n + l \cdot n = (k + l) \cdot n$.

Alternativna oznaka za $a \equiv_n b$ je $a \equiv b \,(\mod n)$.

Relacije ekvivalencije

Definition

Neka je A skup, $\mathrm{x} \in \mathrm{A}$ i $\mathrm{R} \subset \mathrm{A}^2$ relacija ekvivalencije. *Klasa ekvivalencije* elementa x u odnosu na relaciju R, u oznaci $[\mathrm{x}]_{\mathrm{R}}$, je skup svih elemenata skupa A koji su u relaciji R sa x, odnosno

$$[\mathrm{x}]_{\mathrm{R}} = \{\mathrm{y} \in \mathrm{A} : \mathrm{xRy}\}.$$

Količnički skup skupa A za relaciju ekvivalencije R, u oznaci $\mathrm{A}_{/\mathrm{R}}$ je

$$\mathrm{A}_{/\mathrm{R}} = \{[\mathrm{x}]_{\mathrm{R}} : \mathrm{x} \in \mathrm{A}\}.$$

Ako se relacija R podrazumeva uobičajeno je da se piše samo $[\mathrm{x}]$.

Relacije ekvivalencije

Theorem

Neka je $\mathrm{R} \subset \mathrm{A}^2$ *relacija ekvivalencije i* $\mathrm{x}, \mathrm{y} \in \mathrm{A}$. *Tada je* $[\mathrm{x}] = [\mathrm{y}]$ *ako i samo ako* $\mathrm{R}(\mathrm{x}, \mathrm{y})$.

Proof.

Najpre primetimo da je zbog refleksivnosti za svaki $\mathrm{x} \in \mathrm{A}$ ispunjeno $\mathrm{x} \in [\mathrm{x}]$. Prema tome ako je $[\mathrm{x}] = [\mathrm{y}]$, onda je $\mathrm{y} \in [\mathrm{x}]$, što znači da je $\mathrm{R}(\mathrm{x}, \mathrm{y})$. Obrnuto, pretpostavimo da je $\mathrm{R}(\mathrm{x}, \mathrm{y})$. To znači da je $\mathrm{y} \in [\mathrm{x}]$. Za svaki $\mathrm{z} \in [\mathrm{x}]$ zbog simetričnosti i tranzitivnosti važi da je $\mathrm{R}(\mathrm{y}, \mathrm{x})$ i $\mathrm{R}(\mathrm{x}, \mathrm{z})$, pa i $\mathrm{R}(\mathrm{y}, \mathrm{z})$, odakle je $\mathrm{z} \in [\mathrm{y}]$ i $[\mathrm{x}] \subset [\mathrm{y}]$. Na sličan način se dobija $[\mathrm{y}] \subset [\mathrm{x}]$, pa i $[\mathrm{x}] = [\mathrm{y}]$. □

Relacije ekvivalencije

Example

Prema primeru 21 relacija $\equiv_3$ je relacija ekvivalencije. Odgovarajuće klase ekvivalencije su:

- $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$,
- $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ i
- $[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Relacije poretka

Example

Neka je $\mathbb{Q}$ skup racionalnih brojeva. Relacija $\mathrm{R} \subset \mathbb{Q}^2 \times \mathbb{Q}^2$:

$$(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b}) \text{ ako i samo ako je } \mathrm{x} < \mathrm{a}, \text{ ili } \mathrm{x} = \mathrm{a} \text{ i } \mathrm{y} \leq \mathrm{b}.$$

je jedna relacija parcijalnog poretka. Iz $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b})$ sledi $\mathrm{x} \leq \mathrm{a}$.

- Refleksivnost: $\mathrm{x} = \mathrm{x}$ i $\mathrm{y} \leq \mathrm{y}$, pa je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{x}, \mathrm{y})$.
- antisimetričnost: Ako je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b})$ i $(\mathrm{a}, \mathrm{b})\mathrm{R}(\mathrm{x}, \mathrm{y})$, onda je najpre $\mathrm{x} \leq \mathrm{a}$ i $\mathrm{a} \leq \mathrm{x}$, odnosno $\mathrm{x} = \mathrm{a}$, zatim isto važi i za y i b, pa je $\langle \mathrm{x}, \mathrm{y} \rangle = \langle \mathrm{a}, \mathrm{b} \rangle$
- tranzitivnost: neka je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b})$ i $(\mathrm{a}, \mathrm{b})\mathrm{R}(\mathrm{u}, \mathrm{v})$. Tada je $\mathrm{x} \leq \mathrm{a}$ i $\mathrm{a} \leq \mathrm{u}$, pa i $\mathrm{x} \leq \mathrm{u}$. Ako je $\mathrm{x} < \mathrm{u}$, važi da je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{u}, \mathrm{v})$. Ako je $\mathrm{x} = \mathrm{u}$, tada je i $\mathrm{x} = \mathrm{a}$ i $\mathrm{a} = \mathrm{u}$, pa mora biti $\mathrm{y} \leq \mathrm{b}$ i $\mathrm{b} \leq \mathrm{v}$, odakle je $\mathrm{y} \leq \mathrm{v}$ i ponovo $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{u}, \mathrm{v})$.

Relacije poretka

Example

Neka je $\mathbb{Q}$ skup racionalnih brojeva. Relacija $\mathrm{R} \subset \mathbb{Q}^2 \times \mathbb{Q}^2$:

$$(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b}) \text{ ako i samo ako je } \mathrm{x} < \mathrm{a}, \text{ ili } \mathrm{x} = \mathrm{a} \text{ i } \mathrm{y} \leq \mathrm{b}.$$

je jedna relacija parcijalnog poretka. Iz $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b})$ sledi $\mathrm{x} \leq \mathrm{a}$.

- Refleksivnost: $\mathrm{x} = \mathrm{x}$ i $\mathrm{y} \leq \mathrm{y}$, pa je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{x}, \mathrm{y})$.
- antisimetričnost: Ako je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b})$ i $(\mathrm{a}, \mathrm{b})\mathrm{R}(\mathrm{x}, \mathrm{y})$, onda je najpre $\mathrm{x} \leq \mathrm{a}$ i $\mathrm{a} \leq \mathrm{x}$, odnosno $\mathrm{x} = \mathrm{a}$, zatim isto važi i za y i b, pa je $\langle \mathrm{x}, \mathrm{y} \rangle = \langle \mathrm{a}, \mathrm{b} \rangle$
- tranzitivnost: neka je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{a}, \mathrm{b})$ i $(\mathrm{a}, \mathrm{b})\mathrm{R}(\mathrm{u}, \mathrm{v})$. Tada je $\mathrm{x} \leq \mathrm{a}$ i $\mathrm{a} \leq \mathrm{u}$, pa i $\mathrm{x} \leq \mathrm{u}$. Ako je $\mathrm{x} < \mathrm{u}$, važi da je $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{u}, \mathrm{v})$. Ako je $\mathrm{x} = \mathrm{u}$, tada je i $\mathrm{x} = \mathrm{a}$ i $\mathrm{a} = \mathrm{u}$, pa mora biti $\mathrm{y} \leq \mathrm{b}$ i $\mathrm{b} \leq \mathrm{v}$, odakle je $\mathrm{y} \leq \mathrm{v}$ i ponovo $(\mathrm{x}, \mathrm{y})\mathrm{R}(\mathrm{u}, \mathrm{v})$.

Relacije poretka

Definition

Parcijalno uređen skup, ili *poset*, je uređeni par $\langle \mathrm{A}, \mathrm{R} \rangle$, gde je A skup, a $\mathrm{R} \subset \mathrm{A}^2$ relacija parcijalnog poretka.
Element $\mathrm{a} \in \mathrm{A}$ je *minimalan* ako za svaki element $\mathrm{x} \in \mathrm{A}$, iz xRa sledi $\mathrm{x} = \mathrm{a}$. Element $\mathrm{b} \in \mathrm{A}$ je *maksimalan* ako za svaki element $\mathrm{x} \in \mathrm{A}$, iz bRx sledi $\mathrm{b} = \mathrm{x}$.
Element $\mathrm{a} \in \mathrm{A}$ je *minimum*, ili *najmanji element skupa* A, ako za svaki element $\mathrm{x} \in \mathrm{A}$ važi aRx. Element $\mathrm{b} \in \mathrm{A}$ je *maksimum*, ili *najveći element skupa* A, ako za svaki element $\mathrm{x} \in \mathrm{A}$ važi xRb.

Ako minimum (maksimum) u nekom posetu $\langle \mathrm{A}, \mathrm{R} \rangle$ postoji, lako se vidi da je i jedinstven. Na primer, neka su a i b dva najmanja elementa. Tada je aRb i bRa, pa pošto je R antisimetričma, sledi da je $\mathrm{a} = \mathrm{b}$.

Relacije poretka

Minimum (maksimum) ne mora postojati.

Example

Neka je $\mathbb{Q}$ skup racionalnih brojeva.

- $(0,1) = \{x \in \mathbb{Q} : 0 < x < 1\}$, nema ni minimum ni maksimum
- $(0,1] = \{x \in \mathbb{Q} : 0 < x \leq 1\}$ nema minimum, ali je 1 maksimum,
- $[0,1) = \{x \in \mathbb{Q} : 0 \leq x < 1\}$ nema maksimum, a 0 je minimum.
- U skupu $[0,1] = \{x \in \mathbb{Q} : 0 \leq x \leq 1\}$ su 0 i 1 redom minimum i maksimum.

Relacije poretka

Minimalnih i maksimalnih elemenata u nekom posetu može biti više pošto međusobno ne moraju biti uporedivi.

Example

- relacija biti podskup na familiji $\mathrm{A} = \{\emptyset, \{\mathrm{a}\}, \{\mathrm{b}\}\}$ pravih podskupova skupa $\{\mathrm{a}, \mathrm{b}\}$ za koju važi $\{\mathrm{a}\} \not\subset \{\mathrm{b}\}$ i $\{\mathrm{b}\} \not\subset \{\mathrm{a}\}$.
- uređeni par $\langle \mathrm{A}, \subset \rangle$ je jedan poset
- $\emptyset$ je minimum, pa sem praznog skupa nema drugih minimalnih elemenata
- ovde ne postoji maksimum, a maksimalni elementi su $\{\mathrm{a}\}$ i $\{\mathrm{b}\}$.

Relacije poretka

Jednu od osnovnih motivacija za relacije poretka predstavlja relaciji "biti manji do jednak" na skupu celih brojeva $\mathbb{Z}$. Poznato je da tu važi da su svaka dva elementa u relaciji, pa je ovo primer relacije totalnog uređenja.

Definition

Totalno (linearno) uređenje, ili *lanac*, je uređeni par $\langle \mathrm{A}, \mathrm{R} \rangle$, gde je A skup, a $\mathrm{R} \subset \mathrm{A}^2$ relacija totalnog poretka.

Relacije poretka

Example

Skup $\{1, 2, 4, 8\}$ sa relacijom deljivosti $|$ čini jedan konačan lanac. Međutim, $\langle\{1, 2, 4, 8, 12\}, |\rangle$ nije lanac jer niti $8|12$ niti $12|8$. Jedan beskonačan lanac u odnosu na relaciju $|$ je skup $\{2^k : k \in \mathbb{N}\}$.

Example

Posmatrajmo skup A i njegov partitivni skup $\mathbb{P}(A)$. U opštem slučaju $\langle\mathbb{P}(A), \subset\rangle$ nije lanac, na primer različiti jednočlani podskupovi skupa A nisu uporedivi. Međutim, ako je $A = \emptyset$ ili je A jednočlan, $\langle\mathbb{P}(A), \subset\rangle$ jeste lanac.

Funkcije

Definition

Relacija $\mathrm{f} \subset \mathrm{A} \times \mathrm{B}$ je *funkcija (preslikavanje)* $(\mathrm{f} : \mathrm{A} \mapsto \mathrm{B})$ ako zadovoljava da za svaki $\mathrm{x} \in \mathrm{A}$ postoji najviše jedan $\mathrm{y} \in \mathrm{B}$ tako da je $(\mathrm{x}, \mathrm{y}) \in \mathrm{f}$. Pri tome je y *vrednost funkcije* f *za element* x $(\mathrm{f}(\mathrm{x}) = \mathrm{y})$.

- Skup A je *domen*, u oznaci $\mathrm{Dom}(\mathrm{f})$, funkcije f.
- Skup B je *kodomen*, u oznaci $\mathrm{Kodom}(\mathrm{f})$, funkcije f.
- *Slika funkcije* f, u oznaci $\mathrm{Im}(\mathrm{f})$, je skup $\{\mathrm{y} \in \mathrm{B} : (\exists \mathrm{x} \in \mathrm{A})(\mathrm{x}, \mathrm{y}) \in \mathrm{f}\}$.
- Skup svih funkcija iz skupa A u skup B se označava sa B^{A}.
- Totalna: Ako za svaki $\mathrm{x} \in \mathrm{A}$ postoji $\mathrm{y} \in \mathrm{B}$ tako da je $(\mathrm{x}, \mathrm{y}) \in \mathrm{f}$,
- Parcijalna: Ako postoji $\mathrm{x} \in \mathrm{A}$ takav da ni za jedno $\mathrm{y} \in \mathrm{B}$ nije $(\mathrm{x}, \mathrm{y}) \in \mathrm{f}$
- *Identička funkcija* na skupu A, $\mathrm{id}_{\mathrm{A}} \subset \mathrm{A} \times \mathrm{A}$, $\mathrm{id}_{\mathrm{A}}(\mathrm{x}) = \mathrm{x}$

Funkcije

Example

Jedna (totalna) funkcija $\mathrm{f} : \mathbb{Z} \mapsto \mathbb{N}$ je definisana sa:

$$\mathrm{f}(\mathrm{x}) = \mathrm{x}^2.$$

Za nju važi da je skup $\mathrm{Im}(\mathrm{f}) = \{0, 1, 4, 9, \ldots\}$ pravi podskup skupa $\mathrm{Kodom}(\mathrm{f}) = \mathbb{N}$.

Funkcije

Example

Neka je B neki skup i $\mathrm{A} \subset \mathrm{B}$. Funkcija $\chi_{\mathrm{A}} : \mathrm{B} \mapsto \{0, 1\}$ definisana sa

$$\chi_{\mathrm{A}}(\mathrm{x}) = \begin{cases} 1, & \mathrm{x} \in \mathrm{A} \\ 0, & \mathrm{x} \notin \mathrm{A} \end{cases}$$

je *karakteristična funkcija skupa* A.

Funkcije

Example

Funkcija $\mathrm{f} : \mathbb{Z} \mapsto \mathbb{Q}$ definisana sa:

$$\mathrm{f}(\mathrm{x}) = \frac{1}{\mathrm{x}+1}$$

je parcijalna, jer nije definisana za $\mathrm{x} = -1$.

Funkcije

Example

Relacija $\mathrm{h} = \{\langle \mathrm{x}, \mathrm{y}\rangle \in \mathbb{Q}^2 : \mathrm{x} = \mathrm{y}^2\}$ nije funkcija, jer, na primer, za $\mathrm{x} = 4$ postoje $\mathrm{y}_1 = -2$ i $\mathrm{y}_2 = 2$ za koje je $(4, -2), (4, 2) \in \mathrm{h}$.

Funkcije

Definition

Neka su $\mathrm{f} : \mathrm{A} \mapsto \mathrm{B}$ i $\mathrm{g} : \mathrm{B} \mapsto \mathrm{C}$ funkcije. *Kompozicija funkcija* f i g, u oznaci $\mathrm{g} \circ \mathrm{f}$, je skup
$(\mathrm{g} \circ \mathrm{f}) = \{\langle \mathrm{x}, \mathrm{z} \rangle :$ postoji $\mathrm{y} \in \mathrm{B}$ za koje je $\mathrm{f}(\mathrm{x}) = \mathrm{y}$ i $\mathrm{g}(\mathrm{y}) = \mathrm{z}\}$.

Funkcija $\mathrm{g} \circ \mathrm{f} : \mathrm{A} \mapsto \mathrm{C}$ za koju je $(\mathrm{g} \circ \mathrm{f})(\mathrm{x}) = \mathrm{g}(\mathrm{f}(\mathrm{x}))$

Funkcije

Example

Neka su funkcije $f : \mathbb{Z} \mapsto \mathbb{Z}$ i $g : \mathbb{Z} \mapsto \mathbb{N}$ definisane sa:

- $f(x) = 4x - 1$, odnosno
- $g(x) = 2x^2$.

Tada je $(g \circ f)(2) = g(f(2)) = g(4 \cdot 2 - 1) = g(7) = 2 \cdot 7^2 = 98$, a $(g \circ g)(1) = g(2 \cdot 1^2) = g(2) = 2 \cdot 2^2 = 8$.

Funkcije

Example

Neka su funkcije $f : \mathbb{Z} \mapsto \mathbb{Z}$ i $g : \mathbb{Z} \mapsto \mathbb{N}$ definisane sa:

- $f(x) = 4x - 1$, odnosno
- $g(x) = 2x^2$.

Tada je $(g \circ f)(2) = g(f(2)) = g(4 \cdot 2 - 1) = g(7) = 2 \cdot 7^2 = 98$, a $(g \circ g)(1) = g(2 \cdot 1^2) = g(2) = 2 \cdot 2^2 = 8$.

Funkcije

Example

Neka je funkcija $\mathrm{f} : \mathbb{Q} \mapsto \mathbb{Q}$ definisana tako da je $\mathrm{f}(\mathrm{x})$ najveći celi broj koji je manji ili jednak od x, za šta se koristi oznaka $\mathrm{f}(\mathrm{x}) = \lfloor \mathrm{x} \rfloor$. Za ovu funkciju važi $\mathrm{f} \circ \mathrm{f} = \mathrm{f}$ jer je za svaki $\mathrm{y} \in \mathbb{Z}$, $\lfloor \mathrm{y} \rfloor = \mathrm{y}$.

Funkcije

Example

Neka su funkcije $\mathrm{f} : \mathbb{Z} \mapsto \mathbb{Q}$ i $\mathrm{g} : \mathbb{Q} \mapsto \mathbb{Q}$ definisane sa:

- $\mathrm{f}(\mathrm{x}) = \frac{1}{\mathrm{x}+1}$, odnosno
- $\mathrm{g}(\mathrm{x}) = \mathrm{x} + 1$.

Tada f, pa i $\mathrm{g} \circ \mathrm{f}$ nisu definisane za $\mathrm{x} = -1$.

Funkcije

Example

Neka su funkcije $\mathrm{f} : \mathbb{Z} \mapsto \mathbb{Q}$ i $\mathrm{g} : \mathbb{Q} \mapsto \mathbb{Q}$ definisane sa:

- $\mathrm{f}(\mathrm{x}) = \frac{1}{\mathrm{x}+1}$, odnosno
- $\mathrm{g}(\mathrm{x}) = \mathrm{x} + 1$.

Tada f, pa i $\mathrm{g} \circ \mathrm{f}$ nisu definisane za $\mathrm{x} = -1$.

Funkcije

Example

Neka su funkcije $f : \mathbb{Z} \mapsto \mathbb{N}$ i $g : \mathbb{N} \mapsto \mathbb{Q}$ definisane sa:

- $f(x) = x^2$, odnosno
- $g(x) = \frac{1}{x-1}$.

Tada $g \circ f$ nije definisano za $x \in \{-1, 1\}$, jer g nije definisano za 1.

Funkcije

Example

Neka su funkcije $\mathrm{f} : \mathbb{Z} \mapsto \mathbb{N}$ i $\mathrm{g} : \mathbb{N} \mapsto \mathbb{Q}$ definisane sa:

- $\mathrm{f}(\mathrm{x}) = \mathrm{x}^2$, odnosno
- $\mathrm{g}(\mathrm{x}) = \frac{1}{\mathrm{x}-1}$.

Tada $\mathrm{g} \circ \mathrm{f}$ nije definisano za $\mathrm{x} \in \{-1, 1\}$, jer g nije definisano za 1.

Funkcije

Theorem

Neka $f : A \mapsto B$, $g : B \mapsto C$ *i* $h : C \mapsto D$. *Tada:* $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof.

Za proizvoljno $x \in A$ važi:

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$$

Funkcije

Razmatramo totalne funkcije.

Definition

Funkcija $\mathrm{f} : \mathrm{A} \mapsto \mathrm{B}$ je:

- *injektivna*, ili $1-1$, ako iz $\mathrm{f}(\mathrm{x}) = \mathrm{f}(\mathrm{y})$ sledi da je $\mathrm{x} = \mathrm{y}$,
- *surjektivna*, ili *na*, ako sa svaki $\mathrm{y} \in \mathrm{B}$ postoji $\mathrm{x} \in \mathrm{A}$ tako da je $\mathrm{f}(\mathrm{x}) = \mathrm{y}$,
- *bijektivna* ako je *injektivna* i *surjektivna*.

Za surjektivnu funkciju f, $\mathrm{Kodom}(\mathrm{f}) = \mathrm{Im}(\mathrm{f})$.

Funkcije

Example

Funkcija $f : \mathbb{Z} \mapsto \mathbb{N}$ definisana sa $f(x) = x^2$ nije ni injektivna, jer $f(-1) = f(1)$), ni surjektivna, jer za $2 \in \mathbb{N}$ ne postoji $x \in \mathbb{Z}$ tako da je $x^2 = 2$.

Funkcije

Example

Funkcija $\mathrm{f} : \mathbb{Z} \mapsto \mathbb{N}$ definisana sa $\mathrm{f}(\mathrm{x}) = \mathrm{x}^2$ nije ni injektivna, jer $\mathrm{f}(-1) = \mathrm{f}(1)$), ni surjektivna, jer za $2 \in \mathbb{N}$ ne postoji $\mathrm{x} \in \mathbb{Z}$ tako da je $\mathrm{x}^2 = 2$.

Funkcije

Example

Funkcija $f : \{1, 2\} \mapsto \{1, 2, 3\}$ takva da je $f(1) = 2$ i $f(2) = 3$ jeste injektivna jer je vrednost funkcije za sve elemente njenog domena različita, ali nije surjektivna jer za $1 \in \{1, 2, 3\}$ ne postoji $x \in \{1, 2\}$, tako da je $f(x) = 1$.

Funkcije

Example

Funkcija $\mathrm{f} : \{1, 2\} \mapsto \{1, 2, 3\}$ takva da je $\mathrm{f}(1) = 2$ i $\mathrm{f}(2) = 3$ jeste injektivna jer je vrednost funkcije za sve elemente njenog domena različita, ali nije surjektivna jer za $1 \in \{1, 2, 3\}$ ne postoji $\mathrm{x} \in \{1, 2\}$, tako da je $\mathrm{f}(\mathrm{x}) = 1$.

Funkcije

Example

Funkcija $\mathrm{g} : \{1, 2\} \mapsto \{1\}$ takva da je $\mathrm{g}(1) = \mathrm{g}(2) = 1$ jeste surjektivna, ali nije injektivna, dok je funkcija $\mathrm{h} : \{1, 2\} \mapsto \{1, 2\}$ takva da je $\mathrm{h}(1) = 2$, $\mathrm{h}(2) = 1$ bijektivna.

Funkcije

Example

Funkcija $\mathrm{g} : \{1, 2\} \mapsto \{1\}$ takva da je $\mathrm{g}(1) = \mathrm{g}(2) = 1$ jeste surjektivna, ali nije injektivna, dok je funkcija $\mathrm{h} : \{1, 2\} \mapsto \{1, 2\}$ takva da je $\mathrm{h}(1) = 2$, $\mathrm{h}(2) = 1$ bijektivna.

Funkcije

Example

Neka su A i B neprazni skupovi i $\mathrm{A} \times \mathrm{B}$ njihov Dekartov proizvod. Funkcije projekcije definisane sa:

- $\pi_1 : \mathrm{A} \times \mathrm{B} \mapsto \mathrm{A}$, tako da $\pi_1(\mathrm{a}, \mathrm{b}) = \mathrm{a}$ i
- $\pi_2 : \mathrm{A} \times \mathrm{B} \mapsto \mathrm{B}$, tako da $\pi_2(\mathrm{a}, \mathrm{b}) = \mathrm{b}$

su obe surjektivne, ali nisu injektivne (ako skupovi A i B imaju više od jednog člana).

Funkcije

Example

Neka su A i B neprazni skupovi i $\mathrm{A} \times \mathrm{B}$ njihov Dekartov proizvod. Funkcije projekcije definisane sa:

- $\pi_1 : \mathrm{A} \times \mathrm{B} \mapsto \mathrm{A}$, tako da $\pi_1(\mathrm{a}, \mathrm{b}) = \mathrm{a}$ i
- $\pi_2 : \mathrm{A} \times \mathrm{B} \mapsto \mathrm{B}$, tako da $\pi_2(\mathrm{a}, \mathrm{b}) = \mathrm{b}$

su obe surjektivne, ali nisu injektivne (ako skupovi A i B imaju više od jednog člana).

Funkcije

- $\mathrm{f}(\mathrm{a}) = \mathrm{b}$
- definisati obrnuti postupak koji b preslikava u a
- nije funkcija: postoji bar jedno $\mathrm{a}_1 \in \mathrm{Dom}(\mathrm{f})$, tako da $\mathrm{a}_1 \neq \mathrm{a}$ i $\mathrm{f}(\mathrm{a}_1) = \mathrm{b}$
- nije totalna funkcija: za neko b ne postoji ni jedan element domena koji se slika u njega

Definition

Za bijektivnu funkcija $\mathrm{f} : \mathrm{A} \mapsto \mathrm{B}$ njoj *inverzna funkcija* $\mathrm{f}^{-1} : \mathrm{B} \mapsto \mathrm{A}$ je definisana sa $\mathrm{f}^{-1}(\mathrm{b}) = \mathrm{a}$ ako i samo ako je $\mathrm{f}(\mathrm{a}) = \mathrm{b}$.

Za bijektivnu funkciju f važi da je $\mathrm{f} \circ \mathrm{f}^{-1} = \mathrm{id}_\mathrm{B}$ i $\mathrm{f}^{-1} \circ \mathrm{f} = \mathrm{id}_\mathrm{A}$ i $\mathrm{f}^{-1^{-1}} = \mathrm{f}$, jer, ako je $\mathrm{f}(\mathrm{a}) = \mathrm{b}$, onda $(\mathrm{f}^{-1} \circ \mathrm{f})(\mathrm{a}) = \mathrm{f}^{-1}(\mathrm{f}(\mathrm{a})) = \mathrm{f}^{-1}(\mathrm{b}) = \mathrm{a}$.

Funkcije

- $\mathrm{f}(\mathrm{a}) = \mathrm{b}$
- definisati obrnuti postupak koji b preslikava u a
- nije funkcija: postoji bar jedno $\mathrm{a}_1 \in \mathrm{Dom}(\mathrm{f})$, tako da $\mathrm{a}_1 \neq \mathrm{a}$ i $\mathrm{f}(\mathrm{a}_1) = \mathrm{b}$
- nije totalna funkcija: za neko b ne postoji ni jedan element domena koji se slika u njega

Definition

Za bijektivnu funkcija $\mathrm{f} : \mathrm{A} \mapsto \mathrm{B}$ njoj *inverzna funkcija* $\mathrm{f}^{-1} : \mathrm{B} \mapsto \mathrm{A}$ je definisana sa $\mathrm{f}^{-1}(\mathrm{b}) = \mathrm{a}$ ako i samo ako je $\mathrm{f}(\mathrm{a}) = \mathrm{b}$.

Za bijektivnu funkciju f važi da je $\mathrm{f} \circ \mathrm{f}^{-1} = \mathrm{id}_\mathrm{B}$ i $\mathrm{f}^{-1} \circ \mathrm{f} = \mathrm{id}_\mathrm{A}$ i $\mathrm{f}^{-1^{-1}} = \mathrm{f}$, jer, ako je $\mathrm{f}(\mathrm{a}) = \mathrm{b}$, onda $(\mathrm{f}^{-1} \circ \mathrm{f})(\mathrm{a}) = \mathrm{f}^{-1}(\mathrm{f}(\mathrm{a})) = \mathrm{f}^{-1}(\mathrm{b}) = \mathrm{a}$.

Funkcije

Example

Za svaki skup A, trivijalno važi da je identička funkcija $\mathrm{id_A}$ inverzna samoj sebi, jer $(\mathrm{id_A} \circ \mathrm{id_A})(\mathrm{x}) = \mathrm{id_A}(\mathrm{id_A}(\mathrm{x})) = \mathrm{id_A}(\mathrm{x}) = \mathrm{x}$.
Neka su dati $\mathrm{A} = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$, $\mathrm{B} = \{1, 2, 3\}$ i $\mathrm{f} : \mathrm{A} \mapsto \mathrm{B}$ tako da je $\mathrm{f}(\mathrm{a}) = 1$, $\mathrm{f}(\mathrm{b}) = 2$ i $\mathrm{f}(\mathrm{c}) = 3$. Funkcija f je bijektivna, a njoj inverzna je funkcija $\mathrm{f}^{-1} : \mathrm{B} \mapsto \mathrm{A}$, za koju je $\mathrm{f}^{-1}(1) = \mathrm{a}$, $\mathrm{f}^{-1}(2) = \mathrm{b}$ i $\mathrm{f}^{-1}(3) = \mathrm{c}$.

Funkcije. Operacije

Definition

Funkcija $\mathrm{f} : \mathrm{A}^{\mathrm{n}} \mapsto \mathrm{A}$ se naziva n-*arna operacija skupa* A.

U slučaju binarnih operacija: umesto $*(\mathrm{x}, \mathrm{y})$ piše se $\mathrm{x} * \mathrm{y}$.

Definition

Za binarne operacija $*$ i $\star$ skupa A kažemo:

- $*$ je *komutativna* ako je za sve $\mathrm{B}, \mathrm{C} \in \mathrm{A}$, $\mathrm{B} * \mathrm{C} = \mathrm{C} * \mathrm{B}$,
- $*$ je *asocijativna* ako je za sve $\mathrm{B}, \mathrm{C}, \mathrm{D} \in \mathrm{A}$, $(\mathrm{B} * \mathrm{C}) * \mathrm{D} = \mathrm{B} * (\mathrm{C} * \mathrm{D})$,
- $*$ je *distributivna u odnosu na* $\star$ ako je za sve $\mathrm{B}, \mathrm{C}, \mathrm{D} \in \mathrm{A}$, $\mathrm{B} * (\mathrm{C} \star \mathrm{D}) = (\mathrm{B} * \mathrm{C}) \star (\mathrm{B} * \mathrm{D})$.

Funkcije. Operacije

A neprazan skup i $\mathbb{P}(\mathrm{A})$ partitivni skup. Operacije definisane na $\mathbb{P}(\mathrm{A})$:

- operacija *komplementa*, $\mathbb{C} : \mathbb{P}(\mathrm{A}) \mapsto \mathbb{P}(\mathrm{A})$, za koju je $\mathbb{C}(\mathrm{B}) = \{\mathrm{x} : \mathrm{x} \in \mathrm{A} \text{ i } \mathrm{x} \notin \mathrm{B}\}$,
- operacija *unije*, $\cup : \mathbb{P}(\mathrm{A}) \times \mathbb{P}(\mathrm{A}) \mapsto \mathbb{P}(\mathrm{A})$, za koju je $\mathrm{B} \cup \mathrm{C} = \{\mathrm{x} : \mathrm{x} \in \mathrm{B}, \text{ ili } \mathrm{x} \in \mathrm{C}\}$,
- operacija *preseka*, $\cap : \mathbb{P}(\mathrm{A}) \times \mathbb{P}(\mathrm{A}) \mapsto \mathbb{P}(\mathrm{A})$, za koju je $\mathrm{B} \cap \mathrm{C} = \{\mathrm{x} : \mathrm{x} \in \mathrm{B} \text{ i } \mathrm{x} \in \mathrm{C}\}$ i
- operacija *razlike*, $\setminus : \mathbb{P}(\mathrm{A}) \times \mathbb{P}(\mathrm{A}) \mapsto \mathbb{P}(\mathrm{A})$, za koju je $\mathrm{B} \setminus \mathrm{C} = \{\mathrm{x} : \mathrm{x} \in \mathrm{B} \text{ i } \mathrm{x} \notin \mathrm{C}\}$,
- operacija *simetrične razlike*, $\triangle : \mathbb{P}(\mathrm{A}) \times \mathbb{P}(\mathrm{A}) \mapsto \mathbb{P}(\mathrm{A})$, za koju je $\mathrm{B} \triangle \mathrm{C} = \{\mathrm{x} : \mathrm{x} \in \mathrm{B} \text{ i } \mathrm{x} \notin \mathrm{C}, \text{ ili } \mathrm{x} \notin \mathrm{B} \text{ i } \mathrm{x} \in \mathrm{C}\}$.

Operacija su totalne. Komplement je unarna, ostale operacije su binarne.

Funkcije. Operacije

Za konačnu familiju $B_1, B_2, \ldots, B_k \subset A$, uopštene unije i preseci:

- $\cup_{i=1}^{k} B_i = \{x : x \in B_1$, ili $x \in B_2, \ldots$, ili $x \in B_k\}$,
- $\cap_{i=1}^{k} B_i = \{x : x \in B_1$ i $x \in B_2$ i $\ldots$ i $x \in B_k\}$.

Ako je familija $B_1, B_2, \ldots$ beskonačna, $\cup_i B_i$, $\cap_i B_i$.

Funkcije. Operacije

Naredna 3 slajda: A neprazan skup, $\mathbb{P}(\mathrm{A})$ partitivni skup i $\mathrm{B}, \mathrm{C}, \mathrm{D} \in \mathbb{P}(\mathrm{A})$.

Theorem

- $\mathbb{C}(\mathbb{C}(\mathrm{B})) = \mathrm{B}$,
- *zakoni idempotencije*
  - $B \cup B = B$ *i*
  - $B \cap B = B$,
- *zakoni komutativnosti*
  - $B \cup C = C \cup B$ *i*
  - $B \cap C = C \cap B$,
- *zakoni asocijativnosti*
  - $B \cup (C \cup D) = (B \cup C) \cup D$ *i*
  - $B \cap (C \cap D) = (B \cap C) \cap D$,

Funkcije. Operacije

Theorem

- *zakoni apsorpcije*
  - $B \cup (B \cap C) = B$ *i*
  - $B \cap (B \cup C) = B$,
- *zakoni distributivnosti*
  - $B \cap (C \cup D) = (B \cap C) \cup (B \cap D)$
  - $B \cup (C \cap D) = (B \cup C) \cap (B \cup D)$,
- *De Morganovi zakoni*
  - $\mathbb{C}(B \cup C) = \mathbb{C}B \cap \mathbb{C}C$ *i*
  - $\mathbb{C}(B \cap C) = \mathbb{C}B \cup \mathbb{C}C$,

Funkcije. Operacije

Theorem

- $B \cup \emptyset = B$, $B \cap \emptyset = \emptyset$,
- $B \cap A = B$, $B \cup A = A$,
- $B \cup \mathbb{C}(B) = A$, $B \cap \mathbb{C}(B) = \emptyset$,
- $\mathbb{C}(A) = \emptyset$, $\mathbb{C}(\emptyset) = A$,
- $B \setminus C = B \cap \mathbb{C}C$,
- $B \triangle C = (B \setminus C) \cup (C \setminus B)$.

Funkcije. Operacije

Definition

Skupovi A i B su *disjunktni* ako je $A \cap B = \emptyset$.

Definition

Particija skupa A je familija B_1, B_2, ... podskupova skupa A za koju važi:

- $A = \cup_i B_i$ i
- za $i \neq j$, disjunktni su B_i i B_j.

Particija, zavisno od familije B_i, može biti konačna i beskonačna.

Kardinalnost skupova

Prirodni brojevi se u teoriji skupova definišu:

- $0 = \emptyset$,
- $1 = \emptyset \cup \{\emptyset\} = \{0\}$,
- $2 = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$,
- $3 = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}, \ldots,$
- $n + 1 = n \cup \{n\} = \{0, 1, 2, \ldots, n - 1, n\}, \ldots,$

Prirodan broj je skup svojih prethodnika.
Skup $\mathbb{N}$ najmanji skup sa osobinama da sadrži 0 i, ako mu pripada n, onda mu pripada i $n + 1 = n \cup \{n\}$.
Relacija $\leq \subset \mathbb{N}^2$ se definiše tako da $x \leq y$ ako i samo ako je $x = y$ ili $x \in y$ (x je jedan od prethodnika od y).

Kardinalnost skupova

Definition

Skupovi A i B imaju *istu kardinalnost*, u oznaci $|A| = |B|$, ako postoji bijektivna funkcija $f : A \mapsto B$.
Skup A *konačan* ako postoje prirodan broj n i bijektivna funkcija $f : A \mapsto n$. Tada je *broj elemenata (kardinalost) skupa* A, u oznaci $|A|$ jednak n. Ako skup nije konačan, onda je *beskonačan*.
Skup A je *prebrojiv*, odnosno *prebrojivo beskonačan*, ako postoji bijektivna funkcija $f : A \mapsto \mathbb{N}$. Tada $|A| = \aleph_0$.
Skup A je *neprebrojiv*, ako postoji injektivna funkcija $f : \mathbb{N} \mapsto A$, ali A i $\mathbb{N}$ nemaju istu kardinalnost.

Kardinalnost skupova

Example

Prazan skup je konačan jer je 0 jedini prirodan broj za koji postoji bijekcija iz definicije 57, pa je i $|\emptyset| = 0$. Skup $\{1, 3, 5, 7, 9, 11, 13\}$ je konačan, kardinalnosti 7.

Example

Skupovi $\mathbb{N}$, $\mathbb{Z}$ i $\mathbb{Q}$, skup svih parnih i skup svih neparnih prirodnih brojeva su svi prebrojivo beskonačni.

Kardinalnost skupova

U nastavku će pre svega biti reči o konačnim i prebrojivim skupovima. Analogno važi i za proizvoljne (beskonačne) skupove.

Theorem

Ako $|A| = k \in \mathbb{N}$, *onda je* $|\mathbb{P}(A)| = 2^k$.

Proof.

- $A = \{a_1, \ldots, a_k\}$
- $B \in \mathbb{P}(A)$: $\langle b_1, b_2, \ldots, b_k \rangle$,
  - $b_i = 1$, ako $a_i \in B$,
  - $b_i = 0$, ako $a_i \notin B$,
  - $\emptyset = \langle 0, 0, \ldots, 0 \rangle$, $A = \langle 1, 1, \ldots, 1 \rangle$,
- broj elemenata skupa $\mathbb{P}(A)$ jednak je broju različitih k-torki 0 i 1
- na svakoj od k-pozicija moguć je izbor 0 ili 1, pa je to 2^k.

Kardinalnost skupova

U nastavku će pre svega biti reči o konačnim i prebrojivim skupovima. Analogno važi i za proizvoljne (beskonačne) skupove.

Theorem

Ako $|A| = k \in \mathbb{N}$, *onda je* $|\mathbb{P}(A)| = 2^k$.

Proof.

- $A = \{a_1, \ldots, a_k\}$
- $B \in \mathbb{P}(A)$: $\langle b_1, b_2, \ldots, b_k \rangle$,
  - $b_i = 1$, ako $a_i \in B$,
  - $b_i = 0$, ako $a_i \notin B$,
  - $\emptyset = \langle 0, 0, \ldots, 0 \rangle$, $A = \langle 1, 1, \ldots, 1 \rangle$,
- broj elemenata skupa $\mathbb{P}(A)$ jednak je broju različitih k-torki 0 i 1
- na svakoj od k-pozicija moguć je izbor 0 ili 1, pa je to 2^k.

Kardinalnost skupova

U nastavku će pre svega biti reči o konačnim i prebrojivim skupovima. Analogno važi i za proizvoljne (beskonačne) skupove.

Theorem

Ako $|A| = k \in \mathbb{N}$, *onda je* $|\mathbb{P}(A)| = 2^k$.

Proof.

- $A = \{a_1, \ldots, a_k\}$
- $B \in \mathbb{P}(A)$: $\langle b_1, b_2, \ldots, b_k \rangle$,
  - $b_i = 1$, ako $a_i \in B$,
  - $b_i = 0$, ako $a_i \notin B$,
  - $\emptyset = \langle 0, 0, \ldots, 0 \rangle$, $A = \langle 1, 1, \ldots, 1 \rangle$,
- broj elemenata skupa $\mathbb{P}(A)$ jednak je broju različitih k-torki 0 i 1
- na svakoj od k-pozicija moguć je izbor 0 ili 1, pa je to 2^k.

Kardinalnost skupova

U nastavku će pre svega biti reči o konačnim i prebrojivim skupovima. Analogno važi i za proizvoljne (beskonačne) skupove.

Theorem

Ako $|A| = k \in \mathbb{N}$, *onda je* $|\mathbb{P}(A)| = 2^k$.

Proof.

- $A = \{a_1, \ldots, a_k\}$
- $B \in \mathbb{P}(A)$: $\langle b_1, b_2, \ldots, b_k \rangle$,
  - $b_i = 1$, ako $a_i \in B$,
  - $b_i = 0$, ako $a_i \notin B$,
  - $\emptyset = \langle 0, 0, \ldots, 0 \rangle$, $A = \langle 1, 1, \ldots, 1 \rangle$,
- broj elemenata skupa $\mathbb{P}(A)$ jednak je broju različitih k-torki 0 i 1
- na svakoj od k-pozicija moguć je izbor 0 ili 1, pa je to 2^k.

Kardinalnost skupova

Theorem

Neka su A, B, A_1, A_2, ... konačni skupovi. Tada,

- *Ako je $|A_1| = k_1$, a $|A_2| = k_2$, $k_1, k_2 \in \mathbb{N}$, onda je $|A_1 \times A_2| = k_1 \cdot k_2$.*
- $|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.
- *Ako postoji injektivna funkcija $f : A \mapsto B$, onda je $|A| \leq |B|$. Podskup konačnog skupa je konačan.*
- *Ako postoji surjektivna funkcija $f : A \mapsto B$, onda je $|A| \geq |B|$.*
- *Ako je B^A skup svih funkcija iz A u B, onda je $|B^A| = |B|^{|A|}$.*

Kardinalnost skupova

Theorem

Neka su A i B, konačni skupovi. Tada,

$$\text{ako je } A \cap B = \emptyset, \text{ onda je } |A \cup B| = |A| + |B|.$$

- $|A| = k$ i $|B| = l$
- postoje bijektivne funkcije $f : A \mapsto k$ i $g : B \mapsto l$
- označimo elemente skupova A i B tako da je:
  - $f(a_i) = i,\ i = 0, \ldots, k-1,$
  - $g(b_j) = j,\ j = 0, \ldots, l-1,$
  - $A \cap B = \emptyset \rightarrow A \cup B = \{a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}\}$

Kardinalnost skupova

Theorem

Neka su A i B, konačni skupovi. Tada,

$$\text{ako je } A \cap B = \emptyset, \text{ onda je } |A \cup B| = |A| + |B|.$$

- $|A| = k$ i $|B| = l$
- postoje bijektivne funkcije $f : A \mapsto k$ i $g : B \mapsto l$
- označimo elemente skupova A i B tako da je:
  - $f(a_i) = i,\ i = 0, \ldots, k-1,$
  - $g(b_j) = j,\ j = 0, \ldots, l-1,$
  - $A \cap B = \emptyset \rightarrow A \cup B = \{a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}\}$

Kardinalnost skupova

Theorem

Neka su A i B, konačni skupovi. Tada,

$$\text{ako je } A \cap B = \emptyset, \text{ onda je } |A \cup B| = |A| + |B|.$$

- $|A| = k$ i $|B| = l$
- postoje bijektivne funkcije $f : A \mapsto k$ i $g : B \mapsto l$
- označimo elemente skupova A i B tako da je:
  - $f(a_i) = i$, $i = 0, \ldots, k-1$,
  - $g(b_j) = j$, $j = 0, \ldots, l-1$,
  - $A \cap B = \emptyset \rightarrow A \cup B = \{a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}\}$

Kardinalnost skupova

(nastavak dokaza):

- posmatrajmo funkciju $h : A \cup B \mapsto k + l$:
  - $h(a_i) = f(a_i) = i$, $i = 0, \ldots, k-1$,
  - $h(b_j) = g(b_j) + k = j + k$, $j = 0, \ldots, l-1$,
- h je bijekcija, pa je $|A \cup B| = k + l = |A| + |B|$.

Kardinalnost skupova

(nastavak dokaza):

- posmatrajmo funkciju $h : A \cup B \mapsto k + l$:
  - $h(a_i) = f(a_i) = i$, $i = 0, \ldots, k-1$,
  - $h(b_j) = g(b_j) + k = j + k$, $j = 0, \ldots, l-1$,
- h je bijekcija, pa je $|A \cup B| = k + l = |A| + |B|$.

Kardinalnost skupova

Theorem

Neka su A i B konačni skupovi. Tada, $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof.

- $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$
- $A \setminus B$, $B \setminus A$ i $A \cap B$ međusobno disjunktni skupovi
- $|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B| =$
- $(|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| =$
- $|A| + |B| - |A \cap B|$

□

Kardinalnost skupova

Theorem

Neka su A i B konačni skupovi. Tada, $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof.

- $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$
- $A \setminus B$, $B \setminus A$ i $A \cap B$ međusobni disjunktni skupovi
- $|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B| =$
- $(|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| =$
- $|A| + |B| - |A \cap B|$

Kardinalnost skupova

Theorem

Neka su A i B konačni skupovi. Tada, $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof.

- $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$
- $A \setminus B$, $B \setminus A$ i $A \cap B$ međusobni disjunktni skupovi
- $|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B| =$
- $(|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| =$
- $|A| + |B| - |A \cap B|$

Kardinalnost skupova

Theorem

Neka su A i B konačni skupovi. Tada, $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof.

- $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$
- $A \setminus B$, $B \setminus A$ i $A \cap B$ međusobni disjunktni skupovi
- $|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B| =$
- $(|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| =$
- $|A| + |B| - |A \cap B|$

Kardinalnost skupova

Theorem

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

$$\begin{aligned} |A_1 \cup \ldots \cup A_n| &= |A_1| + \cdots + |A_n| \\ &- \textit{ brojevi elemenata dvočlanih preseka} \\ &+ \textit{ brojevi elemenata tročlanih preseka } \ldots \end{aligned}$$

Reprezentovanje skupova u računarstvu

- u većini programskih jezika (konačni) skupovi se prikazuju u obliku niza bitova čija dužina je jednaka broju elemenata
- skupovne operacije se izvode kao logičke operacije nad bitovima, na primer preseku odgovara konjukcija po bitovima
- u konkretnim implementacijama dužina skupa može biti ograničena na broj bitova u registru
- uređenje elemenata (računarskog) skupa: 0 je $\bot$, 1 je $\top$, pa je $\bot < \top$.

Reprezentovanje skupova u računarstvu

- u većini programskih jezika (konačni) skupovi se prikazuju u obliku niza bitova čija dužina je jednaka broju elemenata
- skupovne operacije se izvode kao logičke operacije nad bitovima, na primer preseku odgovara konjukcija po bitovima
- u konkretnim implementacijama dužina skupa može biti ograničena na broj bitova u registru
- uređenje elemenata (računarskog) skupa: 0 je $\bot$, 1 je $\top$, pa je $\bot < \top$.

Reprezentovanje skupova u računarstvu

- u većini programskih jezika (konačni) skupovi se prikazuju u obliku niza bitova čija dužina je jednaka broju elemenata
- skupovne operacije se izvode kao logičke operacije nad bitovima, na primer preseku odgovara konjukcija po bitovima
- u konkretnim implementacijama dužina skupa može biti ograničena na broj bitova u registru
- uređenje elemenata (računarskog) skupa: 0 je $\bot$, 1 je $\top$, pa je $\bot < \top$.

Reprezentovanje skupova u računarstvu

- u većini programskih jezika (konačni) skupovi se prikazuju u obliku niza bitova čija dužina je jednaka broju elemenata
- skupovne operacije se izvode kao logičke operacije nad bitovima, na primer preseku odgovara konjukcija po bitovima
- u konkretnim implementacijama dužina skupa može biti ograničena na broj bitova u registru
- uređenje elemenata (računarskog) skupa: 0 je $\bot$, 1 je $\top$, pa je $\bot < \top$.

Reprezentovanje relacija u računarstvu

- Binarne relacije nad konačnim skupovima se pogodno predstavljaju matricama nula i jedinica.
- $R \subset A \times B$, $A = \{a_1, \ldots, a_k\}$ i $B = \{b_1, \ldots, b_m\}$.
- R se može prikazati binarnom matricom $M_{k \times m}$ tako da je:
  - $M_{i,j} = 1$ ako je $R(a_i, b_j)$
  - $M_{i,j} = 0$ ako je $\neg R(a_i, b_j)$
- ako je $R \subset A \times A$, odgovarajuća matrica je kvadratna
- kako izračunati: refleksivnost, simetričnost, tranzitivno zatvorenje?

Reprezentovanje relacija u računarstvu

- Binarne relacije nad konačnim skupovima se pogodno predstavljaju matricama nula i jedinica.
- $R \subset A \times B$, $A = \{a_1, \ldots, a_k\}$ i $B = \{b_1, \ldots, b_m\}$.
- R se može prikazati binarnom matricom $M_{k \times m}$ tako da je:
  - $M_{i,j} = 1$ ako je $R(a_i, b_j)$
  - $M_{i,j} = 0$ ako je $\neg R(a_i, b_j)$
- ako je $R \subset A \times A$, odgovarajuća matrica je kvadratna
- kako izračunati: refleksivnost, simetričnost, tranzitivno zatvorenje?

Reprezentovanje relacija u računarstvu

- Binarne relacije nad konačnim skupovima se pogodno predstavljaju matricama nula i jedinica.
- $R \subset A \times B$, $A = \{a_1, \ldots, a_k\}$ i $B = \{b_1, \ldots, b_m\}$.
- R se može prikazati binarnom matricom $M_{k \times m}$ tako da je:
  - $M_{i,j} = 1$ ako je $R(a_i, b_j)$
  - $M_{i,j} = 0$ ako je $\neg R(a_i, b_j)$
- ako je $R \subset A \times A$, odgovarajuća matrica je kvadratna
- kako izračunati: refleksivnost, simetričnost, tranzitivno zatvorenje?

Reprezentovanje relacija u računarstvu

- Binarne relacije nad konačnim skupovima se pogodno predstavljaju matricama nula i jedinica.
- $R \subset A \times B$, $A = \{a_1, \ldots, a_k\}$ i $B = \{b_1, \ldots, b_m\}$.
- R se može prikazati binarnom matricom $M_{k \times m}$ tako da je:
  - $M_{i,j} = 1$ ako je $R(a_i, b_j)$
  - $M_{i,j} = 0$ ako je $\neg R(a_i, b_j)$
- ako je $R \subset A \times A$, odgovarajuća matrica je kvadratna
- kako izračunati: refleksivnost, simetričnost, tranzitivno zatvorenje?

Reprezentovanje relacija u računarstvu

- Binarne relacije nad konačnim skupovima se pogodno predstavljaju matricama nula i jedinica.
- $R \subset A \times B$, $A = \{a_1, \ldots, a_k\}$ i $B = \{b_1, \ldots, b_m\}$.
- R se može prikazati binarnom matricom $M_{k \times m}$ tako da je:
  - $M_{i,j} = 1$ ako je $R(a_i, b_j)$
  - $M_{i,j} = 0$ ako je $\neg R(a_i, b_j)$
- ako je $R \subset A \times A$, odgovarajuća matrica je kvadratna
- kako izračunati: refleksivnost, simetričnost, tranzitivno zatvorenje?

Tipovi u računarstvu

- U savremenim programskim jezicima programske celine i konkretni objekti (funkcije, promenljive, datoteke), obično moraju biti deklarisane da su nekog tipa
- deklarišu se tipovi argumenata funkcija i procedura, a prilikom prevođenja programa se vrši provera usklađenosti tih tipova sa tipovima argumenata u pozivu programske celine
- primeri tipova su: celi brojevi, realni brojevi, logički tip, stringovi itd. Ovako posmatrani tipovi imaju sličnosti i razlike u odnosu na (matematičke, apstraktne) skupove na koje asocira njihovo ime
- celi brojevi predstavljeni u nekom konkretnom računarskom sistemu su (samo) konačni podskup skupa $\mathbb{Z}$. Standard programskog jezika *C*, definiše konstante (čija vrednost zavisi od konkretne implementacije):
  - INT_MAX, kao najveći podržani celi broj i
  - INT_MIN, kao najmanji podržani celi broj

  sa garantovanim vrednostima od (makar) $+32767$, odnosno -32767

Tipovi u računarstvu

- U savremenim programskim jezicima programske celine i konkretni objekti (funkcije, promenljive, datoteke), obično moraju biti deklarisane da su nekog tipa
- deklarišu se tipovi argumenata funkcija i procedura, a prilikom prevođenja programa se vrši provera usklađenosti tih tipova sa tipovima argumenata u pozivu programske celine
- primeri tipova su: celi brojevi, realni brojevi, logički tip, stringovi itd. Ovako posmatrani tipovi imaju sličnosti i razlike u odnosu na (matematičke, apstraktne) skupove na koje asocira njihovo ime
- celi brojevi predstavljeni u nekom konkretnom računarskom sistemu su (samo) konačni podskup skupa $\mathbb{Z}$. Standard programskog jezika *C*, definiše konstante (čija vrednost zavisi od konkretne implementacije):
  - INT_MAX, kao najveći podržani celi broj i
  - INT_MIN, kao najmanji podržani celi broj

  sa garantovanim vrednostima od (makar) $+32767$, odnosno -32767

Tipovi u računarstvu

- U savremenim programskim jezicima programske celine i konkretni objekti (funkcije, promenljive, datoteke), obično moraju biti deklarisane da su nekog tipa
- deklarišu se tipovi argumenata funkcija i procedura, a prilikom prevođenja programa se vrši provera usklađenosti tih tipova sa tipovima argumenata u pozivu programske celine
- primeri tipova su: celi brojevi, realni brojevi, logički tip, stringovi itd. Ovako posmatrani tipovi imaju sličnosti i razlike u odnosu na (matematičke, apstraktne) skupove na koje asocira njihovo ime
- celi brojevi predstavljeni u nekom konkretnom računarskom sistemu su (samo) konačni podskup skupa $\mathbb{Z}$. Standard programskog jezika *C*, definiše konstante (čija vrednost zavisi od konkretne implementacije):
  - INT_MAX, kao najveći podržani celi broj i
  - INT_MIN, kao najmanji podržani celi broj

  sa garantovanim vrednostima od (makar) $+32767$, odnosno -32767

Tipovi u računarstvu

- U savremenim programskim jezicima programske celine i konkretni objekti (funkcije, promenljive, datoteke), obično moraju biti deklarisane da su nekog tipa
- deklarišu se tipovi argumenata funkcija i procedura, a prilikom prevođenja programa se vrši provera usklađenosti tih tipova sa tipovima argumenata u pozivu programske celine
- primeri tipova su: celi brojevi, realni brojevi, logički tip, stringovi itd. Ovako posmatrani tipovi imaju sličnosti i razlike u odnosu na (matematičke, apstraktne) skupove na koje asocira njihovo ime
- celi brojevi predstavljeni u nekom konkretnom računarskom sistemu su (samo) konačni podskup skupa $\mathbb{Z}$. Standard programskog jezika C, definiše konstante (čija vrednost zavisi od konkretne implementacije):
  - INT_MAX, kao najveći podržani celi broj i
  - INT_MIN, kao najmanji podržani celi broj

  sa garantovanim vrednostima od (makar) $+32767$, odnosno -32767

Tipovi u računarstvu

- realni brojevi u računaru predstavljaju konačan podskup skupa $\mathbb{Q}$, i to su zapravo neki racionalni brojevi ograničene preciznosti
- u opštem slučaju, neki (računarski) skup sadrži elemente samo istog tipa - nisu dopušteni skupovi koji sadrže realni broj i string
- pojam tipa u programskom jeziku obuhvata i neke unapred zadate operacije nad objektima tog tipa - na konkretnim tipovima definisane pojedine operacije, dok neke druge operacije nisu smislene: cele brojeve je dozvoljeno sabirati, množiti, oduzimati, ali (sem kod nekih posebnih programskih jezika) besmislena je primena logičkih operatora na njih, ili korenovanje stringa

Tipovi u računarstvu

- realni brojevi u računaru predstavljaju konačan podskup skupa $\mathbb{Q}$, i to su zapravo neki racionalni brojevi ograničene preciznosti
- u opštem slučaju, neki (računarski) skup sadrži elemente samo istog tipa - nisu dopušteni skupovi koji sadrže realni broj i string
- pojam tipa u programskom jeziku obuhvata i neke unapred zadate operacije nad objektima tog tipa - na konkretnim tipovima definisane pojedine operacije, dok neke druge operacije nisu smislene: cele brojeve je dozvoljeno sabirati, množiti, oduzimati, ali (sem kod nekih posebnih programskih jezika) besmislena je primena logičkih operatora na njih, ili korenovanje stringa

Tipovi u računarstvu

- realni brojevi u računaru predstavljaju konačan podskup skupa $\mathbb{Q}$, i to su zapravo neki racionalni brojevi ograničene preciznosti
- u opštem slučaju, neki (računarski) skup sadrži elemente samo istog tipa - nisu dopušteni skupovi koji sadrže realni broj i string
- pojam tipa u programskom jeziku obuhvata i neke unapred zadate operacije nad objektima tog tipa - na konkretnim tipovima definisane pojedine operacije, dok neke druge operacije nisu smislene: cele brojeve je dozvoljeno sabirati, množiti, oduzimati, ali (sem kod nekih posebnih programskih jezika) besmislena je primena logičkih operatora na njih, ili korenovanje stringa

Tipovi u računarstvu

- zbog ograničenja konkretnih implementacija, pojedine operacije nisu istovetne matematičkim (apstraktnim) pandanima - vrednost (računarskog) sabiranja celih brojeva, zbog prekoračenja, može biti različita od (matematičke, apstraktne) vrednosti (**česta greška!**).
- u opštem slučaju se prilikom prevođenja programa vrši provera ispravnosti tipova argumenata na koje se operacije primenjuju i, u slučaju neslaganja javlja poruka o grešci. Kod nekih operacija, recimo sabiranja, ako je jedan argument celi, a drugi realni broj vrši se automatsko prevođenje celog u realni broj.

Tipovi u računarstvu

- zbog ograničenja konkretnih implementacija, pojedine operacije nisu istovetne matematičkim (apstraktnim) pandanima - vrednost (računarskog) sabiranja celih brojeva, zbog prekoračenja, može biti različita od (matematičke, apstraktne) vrednosti (**česta greška!**).
- u opštem slučaju se prilikom prevođenja programa vrši provera ispravnosti tipova argumenata na koje se operacije primenjuju i, u slučaju neslaganja javlja poruka o grešci. Kod nekih operacija, recimo sabiranja, ako je jedan argument celi, a drugi realni broj vrši se automatsko prevođenje celog u realni broj.

Relacione baze podataka

Teorijske osnove nekih osnovnih koncepata i operacija u relacionim bazama podataka: Edgar Frank Codd, A Relational Model of Data for Large Shared Data Banks, Communication of the ACM, vol. 13, no 6, 377–387, 1970. `http://www.seas.upenn.edu/~zives/03f/cis550/codd.pdf`

- podatak (*slog*) karakterišu njegove komponente ili *atributi*
- u telefonskom imeniku atributi podatka: ime, adresa, telefonski broj
- atributi imaju svoje tipove, koji svi zajedno određuju složeni, ili *slogovni* tip podatka

Relacione baze podataka

Teorijske osnove nekih osnovnih koncepata i operacija u relacionim bazama podataka: Edgar Frank Codd, A Relational Model of Data for Large Shared Data Banks, Communication of the ACM, vol. 13, no 6, 377–387, 1970. `http://www.seas.upenn.edu/~zives/03f/cis550/codd.pdf`

- podatak (*slog*) karakterišu njegove komponente ili *atributi*
- u telefonskom imeniku atributi podatka: ime, adresa, telefonski broj
- atributi imaju svoje tipove, koji svi zajedno određuju složeni, ili *slogovni* tip podatka

Relacione baze podataka

Teorijske osnove nekih osnovnih koncepata i operacija u relacionim bazama podataka: Edgar Frank Codd, A Relational Model of Data for Large Shared Data Banks, Communication of the ACM, vol. 13, no 6, 377–387, 1970. `http://www.seas.upenn.edu/~zives/03f/cis550/codd.pdf`

- podatak (*slog*) karakterišu njegove komponente ili *atributi*
- u telefonskom imeniku atributi podatka: ime, adresa, telefonski broj
- atributi imaju svoje tipove, koji svi zajedno određuju složeni, ili *slogovni* tip podatka

Relacione baze podataka

- *Tabela* je skup podataka istog slogovnog tipa. Svaka od kolona u tabeli odgovara jednom atributu, dok su redovi konkretni podaci odgovarajućeg slogovnog tipa. Predstavljanje:
  - neka su atributi u tabeli $A_1, A_2, \ldots, A_k$, njihovi tipovi $T_1, T_2, \ldots, T_k$,
  - neka je X_i skup mogućih vrednosti atributa A_i, za $i = 1, 2, \ldots, k$,
  - relaciji $R \subset X_1 \times X_2 \times \cdots \times X_k$ tada odgovara cela tabela,
  - neki slog, odnosno red tabele predstavljamo konkretnom k-torkom $\langle x_1, x_2, \ldots, x_k \rangle \in R$.
- O relaciji R se može razmišljati i kao da je promenljiva u vremenu (brisanje ili dodavanjem slogova)

Relacione baze podataka

- *Tabela* je skup podataka istog slogovnog tipa. Svaka od kolona u tabeli odgovara jednom atributu, dok su redovi konkretni podaci odgovarajućeg slogovnog tipa. Predstavljanje:
  - neka su atributi u tabeli A_1, A_2, $\ldots$, A_k, njihovi tipovi T_1, T_2, $\ldots$, T_k,
  - neka je X_i skup mogućih vrednosti atributa A_i, za $i = 1, 2, \ldots, k$,
  - relaciji $R \subset X_1 \times X_2 \times \cdots \times X_k$ tada odgovara cela tabela,
  - neki slog, odnosno red tabele predstavljamo konkretnom k-torkom $\langle x_1, x_2, \ldots, x_k \rangle \in R$.
- O relaciji R se može razmišljati i kao da je promenljiva u vremenu (brisanje ili dodavanjem slogova)

Relacione baze podataka

- *Tabela* je skup podataka istog slogovnog tipa. Svaka od kolona u tabeli odgovara jednom atributu, dok su redovi konkretni podaci odgovarajućeg slogovnog tipa. Predstavljanje:
  - neka su atributi u tabeli A_1, A_2, $\ldots$, A_k, njihovi tipovi T_1, T_2, $\ldots$, T_k,
  - neka je X_i skup mogućih vrednosti atributa A_i, za $i = 1, 2, \ldots, k$,
  - relaciji $R \subset X_1 \times X_2 \times \cdots \times X_k$ tada odgovara cela tabela,
  - neki slog, odnosno red tabele predstavljamo konkretnom k-torkom $\langle x_1, x_2, \ldots, x_k \rangle \in R$.
- O relaciji R se može razmišljati i kao da je promenljiva u vremenu (brisanje ili dodavanjem slogova)

Relacione baze podataka

Relaciona baza podataka sa atributima A_1, A_2, ..., A_k je kolekcija relacija (tabela) R_1, R_2, ..., R_m, gde je svaka od relacija (tabela)

$$R_i \subset X_{i_1} \times X_{i_2} \times \cdots \times X_{i_n}$$

definisana nad Dekartovim proizvodom odgovarajućih skupova vrednosti nekih od atributa, a indeksi $i_1, \ldots, i_n$ međusobno različiti članovi skupa $\{1, 2, \ldots, k\}$.

Relacione baze podataka

- *Ključevi kandidati* su takvi skupovi atributa čije vrednosti na jedinstven način određuju vrednosti ostalih atributa slogova u tabeli, dok to ne važi za prave podskupove ključevi kandidata.
- Jedan od ključevi kandidata, *primarni ključ*, se bira da bude aktuelni ključ.
- Atribut koji pripada nekom ključu kandidatu je *primitivan*, a *nije primitivan* atribut koji ne pripada ni jednom ključu kandidatu.

Example

Matični broj je uveden da na jedinstven način odredi osobu koja ga poseduje, ali treba obratiti pažnju da, iako je matični broj jedan atribut, u opštem slučaju ključ sadrži više atributa.

Relacione baze podataka

- *Ključevi kandidati* su takvi skupovi atributa čije vrednosti na jedinstven način određuju vrednosti ostalih atributa slogova u tabeli, dok to ne važi za prave podskupove ključevi kandidata.
- Jedan od ključevi kandidata, *primarni ključ*, se bira da bude aktuelni ključ.
- Atribut koji pripada nekom ključu kandidatu je *primitivan*, a *nije primitivan* atribut koji ne pripada ni jednom ključu kandidatu.

Example

Matični broj je uveden da na jedinstven način odredi osobu koja ga poseduje, ali treba obratiti pažnju da, iako je matični broj jedan atribut, u opštem slučaju ključ sadrži više atributa.

Relacione baze podataka

Example

Atributi sa vrednostima u $X_1, \ldots, X_6$:

- A_1, matični broj,
- A_2, ime i prezime,
- A_3, ulica i broj,
- A_4, grad,
- A_5, datum i
- A_6, težina,

Relaciona baza podataka sadrži dve tabele predstavljene relacijama:

- $R_1 \subset X_1 \times X_2 \times X_3 \times X_4$ (lični podaci osoba) i
- $R_1 \subset X_1 \times X_5 \times X_6$ (težine merene nekih datuma).

Primarni ključevi: za R_1 atribut A_1, matični broj; za R_2, atributi A_1 i A_5, matični broj i datum.

Relacione baze podataka

Osnovni postupci sa relacionom bazom:

- izdvajanje onih slogova koji zadovoljavaju neki uslov i
- kreiranje novih tabela na osnovu postojećih.

- selekcija,
- prirodno spajanje
- projekcija,
- unija, presek, razlika.

Relacione baze podataka

Osnovni postupci sa relacionom bazom:

- izdvajanje onih slogova koji zadovoljavaju neki uslov i
- kreiranje novih tabela na osnovu postojećih.

- selekcija,
- prirodno spajanje
- projekcija,
- unija, presek, razlika.

Relacione baze podataka

Selekcija - izbor onih slogova iz neke tabele $R \subset X_1 \times X_2 \times \cdots \times X_k$ koji imaju neke specificirane vrednosti atributa:

$$\{\langle x_1, x_2, \ldots, x_k \rangle : x_{i_1} = r_{i_1}, \ldots, x_{i_m} = r_{i_m}\}.$$

Relacione baze podataka

Prirodno spajanje dve tabele $R \subset X_1 \times \cdots \times X_k \times Y_1 \times \cdots \times Y_m$ i $S \subset X_1 \times \cdots \times X_k \times Z_1 \times \cdots \times Z_n$ proizvodi tabelu:

$$\{\langle x_1, \ldots, x_k, y_1, \ldots, y_m, z_1, \ldots, z_n, \rangle \quad : \quad \langle x_1, \ldots, x_k, y_1, \ldots, y_m \rangle \in R, \\ \langle x_1, \ldots, x_k, z_1, \ldots, z_n \rangle \in S\}.$$

Relacione baze podataka

Projekcija je izdvajanje kolona neke tabele. Projekcijom tabele

$$R \subset X_1 \times X_2 \times \cdots \times X_k$$

po atributima $A_2, \ldots, A_k$, dobija se

$$R' = \{\langle x_2, \ldots, x_k \rangle : \text{ postoji } x_1 \in X_1, \langle x_1, \ldots, x_k \rangle \in R\}.$$

R' je kodomen funkcije:

$$f_I : X_1 \times X_2 \times \cdots \times X_k \mapsto X_2 \times \cdots \times X_k$$

kod koje je $Dom(f_I) = R$, $f_I(x_1, x_2, \ldots, x_k) = \langle x_2, \ldots, x_k \rangle$, a skup indeksa $I = \{2, \ldots, k\}$.

Relacione baze podataka

Example

Atributi sa vrednostima u $X_1, \ldots, X_6$:

- A_1, matični broj,
- A_2, ime i prezime,
- A_3, ulica i broj,
- A_4, grad,
- A_5, datum i
- A_6, težina,

Relaciona baza podataka sadrži dve tabele predstavljene relacijama:

- $R_1 \subset X_1 \times X_2 \times X_3 \times X_4$ (lični podaci osoba) i
- $R_1 \subset X_1 \times X_5 \times X_6$ (težine merene nekih datuma).

Primarni ključevi: za R_1 atribut A_1, matični broj; za R_2, atributi A_1 i A_5, matični broj i datum.

Relacione baze podataka

Matični broj	Ime i prezime	Ulica i broj	Grad
$JMBG_1$	Pera Perić	Glavna 7a	Beograd
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad
$JMBG_4$	Stevo Stević	R. Domanovića 14	Kragujevac

Table: Tabela R_1 sa ličnim podacima

Relacione baze podataka

Matični broj	Datum	Težina
$JMBG_1$	12. 01. 2009.	80
$JMBG_1$	12. 07. 2009.	81
$JMBG_2$	12. 01. 2009.	87
$JMBG_2$	12. 07. 2009.	86
$JMBG_3$	12. 01. 2009.	77
$JMBG_4$	12. 07. 2009.	80

Table: Tabela R_2 sa podacima o merenjima

Relacione baze podataka

Selekcijom iz tabele R_1 po kriterijumu da je vrednost atributa 'Grad' jednaka ' Novi Sad' dobijamo $R_1^{NoviSad}$:

Matični broj	Ime i prezime	Ulica i broj	Grad
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad

Table: Tabela $R_1^{NoviSad}$ sa ličnim podacima stanovnika Novog Sada

Relacione baze podataka

Prirodnim spajanjem tabela R_1 i R_2 dobijamo R_3

Matični broj	Ime i prezime	Ulica i broj	Grad	Datum	Težina
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 01. 2009.	80
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 07. 2009.	81
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 01. 2009.	87
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 07. 2009.	86
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad	12. 01. 2009.	77
$JMBG_4$	Stevo Stević	R. Domanovića 14	Kragujevac	12. 07. 2009.	80

Table: Tabela R_3 dobijena prirodnim spajanjem tabela R_1 i R_2

Relacione baze podataka

Relacione baze podataka su dinamičke, tj. tokom vremena podaci se menjaju, brišu i dodaju.
Normalne forme se definišu kako bi se tokom rada izbegla pojava nekonzistentnosti do kojih može doći zbog postojanja zavisnosti između atributa u tabelama.
Svaka tabela definisana kao skup podataka istog slogovnog tipa je u *prvoj normalnoj formi (1NF)*.

Relacione baze podataka

Matični broj	Ime i prezime	Ulica i broj	Grad	Datum	Težina
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 01. 2009.	80
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 07. 2009.	81
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 01. 2009.	87
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 07. 2009.	86
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad	12. 01. 2009.	77
$JMBG_4$	Stevo Stević	R. Domanovića 14	Kragujevac	12. 07. 2009.	80

Problemi:

- umnogostručavanje podataka u njoj: imena osoba i njihove adrese se neprestano ponavljaju,
- Pera Perić je promenio adresu. Ako bi se ta izmena svuda unosila, u principu je potrebno izvršiti dosta ispitivanja i upisivanja, ako se izmena ne unosi, u različitim slogovima adresa Pere Perića bi bila različita. Šta daje projekcija po imenima i adresama?
- Nije moguće ubaciti novu osobu čija merenja treba pratiti, dok god se ne izvrši prvo merenje.
- Ako se obriše red tabele, a u tom redu je jedina pojava neke osobe, automatski se gube i podaci o toj osobi.

Relacione baze podataka

Funkcionalna zavisnost - vrednosti jednog skupa atributa jednoznačno određuju vrednosti drugog, disjunktnog, skupa atributa:

- $I = \{i_1, \ldots, i_k\}$ i $J = \{j_1, \ldots, j_m\}$ dva skupa indeksa atributa tako da je $I \cap J = \emptyset$ (jednostavnosti radi, $i_1 < \ldots < i_k < j_1 < \ldots < j_m$),
- $A_I = \{A_{i_1}, \ldots, A_{i_k}\}$, $A_J = \{A_{j_1}, \ldots, A_{j_m}\}$ i $A_{I \cup J} = A_I \cup A_J$,
- R tabela u kojoj skup atributa sadrži atribute $A_{I \cup J}$ i
- $R_{I \cup J}$ projekcija tabele R po $A_{I \cup J}$.

A_J je *funkcionalno zavisan* od A_I, ako je $R_{I \cup J}$ funkcija iz R_I u R_J, odnosno za svaku k-torku $r_k \in R_I$ postoji tačno jedna m-torka $r_m \in R_J$, tako da je $\langle r_k, r_m \rangle \in R_{I \cup J}$.

Relacione baze podataka

Funkcionalna zavisnost - vrednosti jednog skupa atributa jednoznačno određuju vrednosti drugog, disjunktnog, skupa atributa:

- $I = \{i_1, \ldots, i_k\}$ i $J = \{j_1, \ldots, j_m\}$ dva skupa indeksa atributa tako da je $I \cap J = \emptyset$ (jednostavnosti radi, $i_1 < \ldots < i_k < j_1 < \ldots < j_m$),
- $A_I = \{A_{i_1}, \ldots, A_{i_k}\}$, $A_J = \{A_{j_1}, \ldots, A_{j_m}\}$ i $A_{I \cup J} = A_I \cup A_J$,
- R tabela u kojoj skup atributa sadrži atribute $A_{I \cup J}$ i
- $R_{I \cup J}$ projekcija tabele R po $A_{I \cup J}$.

A_J je *funkcionalno zavisan* od A_I, ako je $R_{I \cup J}$ funkcija iz R_I u R_J, odnosno za svaku k-torku $r_k \in R_I$ postoji tačno jedna m-torka $r_m \in R_J$, tako da je $\langle r_k, r_m \rangle \in R_{I \cup J}$.

Relacione baze podataka

- *Druga normala forma (2NF)* - ako i samo ako u tabeli svaki ne-primitivni atribut (ne pripada ni jednom ključu kandidatu) nije funkcionalno zavisan od nekog pravog podskupa nekog ključa kandidata.
- Tabela je u 2NF ako su svi ključevi kandidati jednočlani. Ako postoje višečlani ključevi kandidati moguće je da neki njihov pravi podskup na jedinstven određuje vrednosti nekih od ne-primitivnih atributa.
- Normalizacija, ili transformacija u drugu normalnu formu, se vrši delenjem tabele u nove dve tabele (R_1 i R_2).

Relacione baze podataka

- *Druga normala forma (2NF)* - ako i samo ako u tabeli svaki ne-primitivni atribut (ne pripada ni jednom ključu kandidatu) nije funkcionalno zavisan od nekog pravog podskupa nekog ključa kandidata.
- Tabela je u 2NF ako su svi ključevi kandidati jednočlani. Ako postoje višečlani ključevi kandidati moguće je da neki njihov pravi podskup na jedinstven određuje vrednosti nekih od ne-primitivnih atributa.
- Normalizacija, ili transformacija u drugu normalnu formu, se vrši delenjem tabele u nove dve tabele (R_1 i R_2).

Relacione baze podataka

- *Druga normala forma (2NF)* - ako i samo ako u tabeli svaki ne-primitivni atribut (ne pripada ni jednom ključu kandidatu) nije funkcionalno zavisan od nekog pravog podskupa nekog ključa kandidata.
- Tabela je u 2NF ako su svi ključevi kandidati jednočlani. Ako postoje višečlani ključevi kandidati moguće je da neki njihov pravi podskup na jedinstven određuje vrednosti nekih od ne-primitivnih atributa.
- Normalizacija, ili transformacija u drugu normalnu formu, se vrši delenjem tabele u nove dve tabele (R_1 i R_2).

Relacione baze podataka

Matični broj	Ime i prezime	Ulica i broj	Grad	Datum	Težina
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 01. 2009.	80
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 07. 2009.	81
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 01. 2009.	87
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 07. 2009.	86
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad	12. 01. 2009.	77
$JMBG_4$	Stevo Stević	R. Domanovića 14	Kragujevac	12. 07. 2009.	80

- matični broj na jedinstven način određuje osobu, ali nije ključ kandidat - vrednost $JMBG_1$ se nalazi u dva sloga. Skup {Matični broj, Datum} jeste ključ kandidat
- Narušavanje 2NF - 'Matični broj' na jedinstven način određuje vrednost 'Ime i prezime'
- Normalizacija: R_3 podeliti u R_1 i R_2: U R_1 primarni ključ je 'Matični broj', a u R_2 {Matični broj, Datum}.

Relacione baze podataka

Matični broj	Ime i prezime	Ulica i broj	Grad	Datum	Težina
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 01. 2009.	80
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 07. 2009.	81
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 01. 2009.	87
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 07. 2009.	86
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad	12. 01. 2009.	77
$JMBG_4$	Stevo Stević	R. Domanovića 14	Kragujevac	12. 07. 2009.	80

- matični broj na jedinstven način određuje osobu, ali nije ključ kandidat - vrednost $JMBG_1$ se nalazi u dva sloga. Skup {Matični broj, Datum} jeste ključ kandidat
- Narušavanje 2NF - 'Matični broj' na jedinstven način određuje vrednost 'Ime i prezime'
- Normalizacija: R_3 podeliti u R_1 i R_2: U R_1 primarni ključ je 'Matični broj', a u R_2 {Matični broj, Datum}.

Relacione baze podataka

Matični broj	Ime i prezime	Ulica i broj	Grad	Datum	Težina
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 01. 2009.	80
$JMBG_1$	Pera Perić	Glavna 7a	Beograd	12. 07. 2009.	81
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 01. 2009.	87
$JMBG_2$	Žika Žikić	Nova b.b.	Beograd	12. 07. 2009.	86
$JMBG_3$	Mika Mikić	Dunavska 21	Novi Sad	12. 01. 2009.	77
$JMBG_4$	Stevo Stević	R. Domanovića 14	Kragujevac	12. 07. 2009.	80

- matični broj na jedinstven način određuje osobu, ali nije ključ kandidat - vrednost $JMBG_1$ se nalazi u dva sloga. Skup {Matični broj, Datum} jeste ključ kandidat
- Narušavanje 2NF - 'Matični broj' na jedinstven način određuje vrednost 'Ime i prezime'
- Normalizacija: R_3 podeliti u R_1 i R_2: U R_1 primarni ključ je 'Matični broj', a u R_2 {Matični broj, Datum}.

Prebrojavanje

Prebrojavanje – utvrđivanje broja elemenata nekog skupa.

Problemi u kojima se traži:

- dokaz postojanja rešenja i
- broj rešenja.

Prebrojavanje

Prebrojavanje – utvrđivanje broja elemenata nekog skupa.

Problemi u kojima se traži:

- dokaz postojanja rešenja i
- broj rešenja.

Prebrojavanje

Oblasti:

- kombinatorika
- rekurentne relacije
- generatorne funkcije

Uobičajeni pristup:

- transformacija polaznog problema (u neki problem nad uređenim k-torkama) i
- dekompozicija problema u jednostavnije.

Prebrojavanje

Oblasti:

- kombinatorika
- rekurentne relacije
- generatorne funkcije

Uobičajeni pristup:

- transformacija polaznog problema (u neki problem nad uređenim k-torkama) i
- dekompozicija problema u jednostavnije.

Transformacija problema

Tvrđenja o kardinalnosti skupova:

- ako postoji bijekcija $f : A \mapsto B$, onda je $|A| = |B|$,
- ako postoji injekcija ("1-1") $f : A \mapsto B$, onda je $|A| \leq |B|$ i
- ako postoji surjekcija ("na") $f : A \mapsto B$, onda je $|A| \geq |B|$.

Transformacija problema

Example

U dokazu tvrđenja o broju elemenata partitivnog skupa $\mathbb{P}(A)$ je iskorištena bijekcija koja elemente partitivnog skupa preslikava u k-torke nula i jedinica:

- $|A| = k$, $A = \{a_1, \ldots, a_k\}$
- $f : \mathbb{P}(A) \mapsto \{0,1\}^k$
- $B \in \mathbb{P}(A)$, $f(B) = \langle b_1, \ldots, b_k \rangle$, $b_i = 1$ akko $a_i \in B$
- $|\mathbb{P}(A)| = |\{0,1\}^k| = 2^k$.

Princip golubarnika

Kontrapozicija pravila:

- ako postoji injekcija ("1-1") $f : A \mapsto B$, onda je $|A| \leq |B|$

glasi:

Ako je $|A| > |B|$ onda ni jedna funkcija $f : A \mapsto B$ nije injektivna.

Ako je $|A| > |B|$, za svaku funkciju $f : A \mapsto B$ moraju postojati bar dva elementa $a_1, a_2 \in A$, tako da je $a_1 \neq a_2$ i $f(a_1) = f(a_2)$.

Princip golubarnika

Kontrapozicija pravila:

- ako postoji injekcija ("1-1") $f : A \mapsto B$, onda je $|A| \leq |B|$

glasi:

> Ako je $|A| > |B|$ onda ni jedna funkcija $f : A \mapsto B$ nije injektivna.

Ako je $|A| > |B|$, za svaku funkciju $f : A \mapsto B$ moraju postojati bar dva elementa $a_1, a_2 \in A$, tako da je $a_1 \neq a_2$ i $f(a_1) = f(a_2)$.

Princip golubarnika

Example

Ako u nekom golubarniku postoji k pregrada i $k+1$ golub, onda da bi svi golubovi bili smešteni, u bar jednoj od pregrada moraju biti smeštena bar dva goluba.

Johann Peter Gustav Lejeune Dirichlet, 1805 – 1859

Nemački matematičar. Veruje se da je prvi formulisao princip golubarnika (*pigeonhole principle*, *Dirichlet-ov princip*). Pored drugih brojnih rezultata prvi je formulisao modernu definiciju funkcije: 'Ako je promenljiva y u vezi sa promenljivom x tako da kad god x dobije numeričku vrednost, postoji pravilo koje na jedinstveni način određuje vrednost y, kaže se da je y funkcija nezavisne promenljive x". Nakon smrti Gausa preuzeo je katedru na Univerzitetu u Göttingen-u. Njegovi studenti su bili, pored ostalih, Leopold Kronecker i Rudolf Lipschitz.

Princip golubarnika

Example

- skup A od 90 dekadnih brojeva od po 25 cifara
- $|\mathbb{P}(A)| = 2^{90}$
- Najveća suma brojeva u podsupu skupa A sigurno $\leq 90 \cdot 10^{25}$
- $2^{90} > 90 \cdot 10^{25}$
- u skupu A moraju postojati dva različita podskupa sa istim zbirovima elemenata

Princip golubarnika

Example

- skup A od 90 dekadnih brojeva od po 25 cifara
- $|\mathbb{P}(A)| = 2^{90}$
- Najveća suma brojeva u podsupu skupa A sigurno $\leq 90 \cdot 10^{25}$
- $2^{90} > 90 \cdot 10^{25}$
- u skupu A moraju postojati dva različita podskupa sa istim zbirovima elemenata

Princip golubarnika

Uopštenje principa golubarnika glasi:

- Ako je $|A| > k \cdot |B|$ tada za svaku funkciju $f : A \mapsto B$ postoji bar $k + 1$ elemenata skupa A koji se preslikavaju u isti element skupa B.

Example

- u Beogradu postoji $n = 100000$ bradatih muškaraca
- broj dlaka u njihovoj bradi $\leq k = 40000$
- $n > 2 \cdot k$
- bar trojica moraju imati isti broj dlaka u bradi.

Princip golubarnika

Uopštenje principa golubarnika glasi:

- Ako je $|A| > k \cdot |B|$ tada za svaku funkciju $f : A \mapsto B$ postoji bar $k + 1$ elemenata skupa A koji se preslikavaju u isti element skupa B.

Example

- u Beogradu postoji $n = 100000$ bradatih muškaraca
- broj dlaka u njihovoj bradi $\leq k = 40000$
- $n > 2 \cdot k$
- bar trojica moraju imati isti broj dlaka u bradi.

Princip golubarnika

Variranje pravila dovodi do uopštavanja pojma injektivne (odnosno $1-1$) funkcije na $k-u-1$-*funkciju* koja u svaki element kodomena slika tačno k elemenata domena:

Ako je $f : A \mapsto B$ $k-$u-1-funkcija, onda je $|A| = k \cdot |B|$.

Princip golubarnika

Example

- na koliko različitih načina se na šahovskoj tabli mogu postaviti dva topa tako da se ne nalaze ni u istom redu, ni u istoj koloni?
- poziciju topa i $(i = 1, 2)$ predstavimo kao uređeni par koordinata $\langle r_i, k_i \rangle$, gde su $r_i, k_i \in \{1, \ldots, 8\}$ i r_i označava red, a k_i kolonu topa i
- pozicija dva topa se preslikava na skup $\langle r_1, k_1, r_2, k_2 \rangle$
- jedno rešenje problema je $\langle 1, 1, 2, 2 \rangle$
- isto rešenje: $\langle 1, 1, 2, 2 \rangle$ i $\langle 2, 2, 1, 1 \rangle$, različite četvorke
- skup pozicija koje jesu rešenja A, skup svih njima odgovarajućih uređenih četvorki B, prethodno opisano preslikavanje iz B u A je $2-$u-1-funkcija, $|A| = \frac{|B|}{2}$
- par r_1, k_1 možemo izabrati na $8 \cdot 8 = 64$ načina, dok par r_2, k_2 biramo na $7 \cdot 7 = 49$ načina
- $|B| = 8^2 \cdot 7^2$, $|A| = \frac{8^2 \cdot 7^2}{2} = 1568$

Princip golubarnika

Example

- na koliko različitih načina se na šahovskoj tabli mogu postaviti dva topa tako da se ne nalaze ni u istom redu, ni u istoj koloni?
- poziciju topa i $(i = 1, 2)$ predstavimo kao uređeni par koordinata $\langle r_i, k_i \rangle$, gde su $r_i, k_i \in \{1, \ldots, 8\}$ i r_i označava red, a k_i kolonu topa i
- pozicija dva topa se preslikava na skup $\langle r_1, k_1, r_2, k_2 \rangle$
- jedno rešenje problema je $\langle 1, 1, 2, 2 \rangle$
- isto rešenje: $\langle 1, 1, 2, 2 \rangle$ i $\langle 2, 2, 1, 1 \rangle$, različite četvorke
- skup pozicija koje jesu rešenja A, skup svih njima odgovarajućih uređenih četvorki B, prethodno opisano preslikavanje iz B u A je $2-$u-1-funkcija, $|A| = \frac{|B|}{2}$
- par r_1, k_1 možemo izabrati na $8 \cdot 8 = 64$ načina, dok par r_2, k_2 biramo na $7 \cdot 7 = 49$ načina
- $|B| = 8^2 \cdot 7^2$, $|A| = \frac{8^2 \cdot 7^2}{2} = 1568$

Princip golubarnika

Example

- na koliko različitih načina se na šahovskoj tabli mogu postaviti dva topa tako da se ne nalaze ni u istom redu, ni u istoj koloni?
- poziciju topa i $(i = 1, 2)$ predstavimo kao uređeni par koordinata $\langle r_i, k_i \rangle$, gde su $r_i, k_i \in \{1, \ldots, 8\}$ i r_i označava red, a k_i kolonu topa i
- pozicija dva topa se preslikava na skup $\langle r_1, k_1, r_2, k_2 \rangle$
- jedno rešenje problema je $\langle 1, 1, 2, 2 \rangle$
- isto rešenje: $\langle 1, 1, 2, 2 \rangle$ i $\langle 2, 2, 1, 1 \rangle$, različite četvorke
- skup pozicija koje jesu rešenja A, skup svih njima odgovarajućih uređenih četvorki B, prethodno opisano preslikavanje iz B u A je $2-$u-1-funkcija, $|A| = \frac{|B|}{2}$
- par r_1, k_1 možemo izabrati na $8 \cdot 8 = 64$ načina, dok par r_2, k_2 biramo na $7 \cdot 7 = 49$ načina
- $|B| = 8^2 \cdot 7^2$, $|A| = \frac{8^2 \cdot 7^2}{2} = 1568$

Princip golubarnika

Example

- na koliko različitih načina se na šahovskoj tabli mogu postaviti dva topa tako da se ne nalaze ni u istom redu, ni u istoj koloni?
- poziciju topa i ($i = 1, 2$) predstavimo kao uređeni par koordinata $\langle r_i, k_i \rangle$, gde su $r_i, k_i \in \{1, \ldots, 8\}$ i r_i označava red, a k_i kolonu topa i
- pozicija dva topa se preslikava na skup $\langle r_1, k_1, r_2, k_2 \rangle$
- jedno rešenje problema je $\langle 1, 1, 2, 2 \rangle$
- isto rešenje: $\langle 1, 1, 2, 2 \rangle$ i $\langle 2, 2, 1, 1 \rangle$, različite četvorke
- skup pozicija koje jesu rešenja A, skup svih njima odgovarajućih uređenih četvorki B, prethodno opisano preslikavanje iz B u A je $2-$u-1-funkcija, $|A| = \frac{|B|}{2}$
- par r_1, k_1 možemo izabrati na $8 \cdot 8 = 64$ načina, dok par r_2, k_2 biramo na $7 \cdot 7 = 49$ načina
- $|B| = 8^2 \cdot 7^2$, $|A| = \frac{8^2 \cdot 7^2}{2} = 1568$

Princip golubarnika

Example

- na koliko različitih načina se na šahovskoj tabli mogu postaviti dva topa tako da se ne nalaze ni u istom redu, ni u istoj koloni?
- poziciju topa i $(i = 1, 2)$ predstavimo kao uređeni par koordinata $\langle r_i, k_i \rangle$, gde su $r_i, k_i \in \{1, \ldots, 8\}$ i r_i označava red, a k_i kolonu topa i
- pozicija dva topa se preslikava na skup $\langle r_1, k_1, r_2, k_2 \rangle$
- jedno rešenje problema je $\langle 1, 1, 2, 2 \rangle$
- isto rešenje: $\langle 1, 1, 2, 2 \rangle$ i $\langle 2, 2, 1, 1 \rangle$, različite četvorke
- skup pozicija koje jesu rešenja A, skup svih njima odgovarajućih uređenih četvorki B, prethodno opisano preslikavanje iz B u A je $2-$u-1-funkcija, $|A| = \frac{|B|}{2}$
- par r_1, k_1 možemo izabrati na $8 \cdot 8 = 64$ načina, dok par r_2, k_2 biramo na $7 \cdot 7 = 49$ načina
- $|B| = 8^2 \cdot 7^2$, $|A| = \frac{8^2 \cdot 7^2}{2} = 1568$

Princip golubarnika

Example

- na koliko različitih načina se na šahovskoj tabli mogu postaviti dva topa tako da se ne nalaze ni u istom redu, ni u istoj koloni?
- poziciju topa i $(i = 1, 2)$ predstavimo kao uređeni par koordinata $\langle r_i, k_i \rangle$, gde su $r_i, k_i \in \{1, \ldots, 8\}$ i r_i označava red, a k_i kolonu topa i
- pozicija dva topa se preslikava na skup $\langle r_1, k_1, r_2, k_2 \rangle$
- jedno rešenje problema je $\langle 1, 1, 2, 2 \rangle$
- isto rešenje: $\langle 1, 1, 2, 2 \rangle$ i $\langle 2, 2, 1, 1 \rangle$, različite četvorke
- skup pozicija koje jesu rešenja A, skup svih njima odgovarajućih uređenih četvorki B, prethodno opisano preslikavanje iz B u A je $2-$u-1-funkcija, $|A| = \frac{|B|}{2}$
- par r_1, k_1 možemo izabrati na $8 \cdot 8 = 64$ načina, dok par r_2, k_2 biramo na $7 \cdot 7 = 49$ načina
- $|B| = 8^2 \cdot 7^2$, $|A| = \frac{8^2 \cdot 7^2}{2} = 1568$

Dekompozicije problema

Problem dekomponujemo na jednostavnije, tako da se kombinovanjem njihovih dobija rešenja polaznog problema.

Postupci su bazirani na:

- pravilo proizvoda
- pravilo zbira
- pravilo uključenja-isključenja

Pravilo proizvoda

Pravilo proizvoda se odnosi na veličinu proizvoda skupova:

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Example

Neka su redovi u nekoj sali numerisani rimskim brojevima I, II, $\ldots$, XXV, a sedišta u svakom redu arapskim brojevima 1, 2, $\ldots$, 30. Ukupan broj sedišta je tada, prema pravilu proizvoda jednak $25 \cdot 30 = 750$.
Broj različitih binarnih reči dužine n jednak je

$$|\underbrace{\{0,1\} \times \ldots \times \{0,1\}}_{n}| = |\{0,1\}|^n = 2^n$$

Pravilo proizvoda

Pravilo proizvoda se odnosi na veličinu proizvoda skupova:

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Example

Neka su redovi u nekoj sali numerisani rimskim brojevima I, II, ..., XXV, a sedišta u svakom redu arapskim brojevima 1, 2, ..., 30. Ukupan broj sedišta je tada, prema pravilu proizvoda jednak $25 \cdot 30 = 750$.
Broj različitih binarnih reči dužine n jednak je

$$|\underbrace{\{0,1\} \times \ldots \times \{0,1\}}_{n}| = |\{0,1\}|^n = 2^n$$

Pravilo zbira

Pravilo zbira se odnosi na veličinu unije uzajamno disjunktnih skupova:

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

Example

Neka od grada A do grada B postoje autobuska i železnička veza, i to svakog dana 3 polaska autobusa i 2 polaska voza. Broj načina da neko iz A stigne u B je prema pravilu zbira jednak $3 + 2 = 5$.

Pravilo zbira

Pravilo zbira se odnosi na veličinu unije uzajamno disjunktnih skupova:

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

Example

Neka od grada A do grada B postoje autobuska i železnička veza, i to svakog dana 3 polaska autobusa i 2 polaska voza. Broj načina da neko iz A stigne u B je prema pravilu zbira jednak $3 + 2 = 5$.

Pravilo zbira

Pravilo uključenja-isključenja odnosi se na uniju proizvoljnih skupova:

$$\begin{aligned} |A_1 \cup \ldots \cup A_n| &= |A_1| + \cdots + |A_n| \\ &- \text{ brojevi elemenata dvočlanih preseka} \\ &+ \text{ brojevi elemenata tročlanih preseka } \ldots \end{aligned}$$

što je za $n = 2$ izraz oblika:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|,$$

a za $n = 3$:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Pravilo zbira

Example

Posmatrajmo sve binarne reči dužine 4 koje bilo počinju sa 1 bilo završavaju sa 0:

- 8 binarnih reči $1x_2x_3x_4$
- 8 binarnih reči $y_1y_2y_30$
- 4 reči oblika $1z_2z_30$ su brojane dva puta
- broj traženih reči, prema pravilu uključenja-isključenja je $8 + 8 - 4 = 12$.

Pravilo zbira

Example

- koliko je prirodnih brojeva između 1 i 100 deljivo sa 3 ili 7
- brojevi deljivi i sa 3 i sa 7 su deljivi sa 21 i to su 21, 42, 63 i 84, ima ih 4
- brojeva deljivih sa 3 ima 33, dok brojeva deljivih sa 7 ima 14
- prema pravilu uključenja-isključenja traženi broj je jednak $33 + 14 - 4 = 43$.

Pravilo zbira

Example

- u sobi je 12-oro ljudi, od kojih je 10 visokih i 5 vitkih
- broj visokih i vitkih x
- prema pravilu uključenja-isključenja je $12 = 10 + 5 - x$, pa je $x = 3$

Dekompozicije problema

Example

Neka se šifra računarskog sistema formira kao reč dužine od 7 ili 8 znaka, pri čemu prvi znak mora biti slovo, a dozvoljeni znaci su mala i velika ASCII-slova i dekadne cifre. Posmatrajmo skupove

- $P = \{a, \ldots, z, A, \ldots, Z\}$ (iz kog se bira prvi znak u šifri) i
- $O = \{a, \ldots, z, A, \ldots, Z, 0, \ldots 9\}$ (iz kog se biraju ostali znaci u šifri),

za koje je $|P| = 52$ i $|O| = 62$. Ukupan broj mogućih šifara je tada

$|(P \times O^6) \cup (P \times O^7)| = |P \times O^6| + |P \times O^7|$, prema pravilu zbira,

$= |P| \cdot |O^6| + |P| \cdot |O^7|$, prema pravilu proizvoda,

$= 52 \cdot 62^6 + 52 \cdot 62^7$.

Permutacije. Kombinacije

Definition

k-permutacija skupa od n elemenata je svaka uređena k-torka različitih elemenata iz skupa od n elemenata.
Permutacija skupa od n elemenata je svaka n-permutacija tog skupa.
k-kombinacija skupa od n elemenata je svaki podskup od k (različitih) elemenata iz skupa od n elemenata.

- kod permutacija se vodi računa o redosledu elemenata, dok to nije slučaj sa kombinacijama
- (za sada) naglasak je na *različitim* elementima polaznog skupa
- k-permutacija = *varijacija bez ponavljanja k-te klase od n elemenata*.

Permutacije. Kombinacije

Definition

k-permutacija skupa od n elemenata je svaka uređena k-torka različitih elemenata iz skupa od n elemenata.
Permutacija skupa od n elemenata je svaka n-permutacija tog skupa.
k-kombinacija skupa od n elemenata je svaki podskup od k (različitih) elemenata iz skupa od n elemenata.

- kod permutacija se vodi računa o redosledu elemenata, dok to nije slučaj sa kombinacijama
- (za sada) naglasak je na *različitim* elementima polaznog skupa
- k-permutacija = *varijacija bez ponavljanja k-te klase od n elemenata*.

Permutacije. Kombinacije

Example

Neka je skup $A = \{1, 2, 3\}$. Sve 2-permutacije skupa A su:

$$\langle 1, 2\rangle \langle 2, 1\rangle \langle 3, 1\rangle$$
$$\langle 1, 3\rangle \langle 2, 3\rangle \langle 3, 2\rangle$$

Različite 2-permutacije su: $\langle 1, 2\rangle$ i $\langle 2, 1\rangle$.
Sve 2-kombinacije skupa A su:

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

Istu 2-kombinaciju predstavlja $\{1, 2\}$ i $\{2, 1\}$.

- ako za svaku 2-kombinacije skupa A posmatramo njene permutacije, dobijaju se sve 2-permutacije skupa A
- može se uopštiti i na proizvoljno k

Permutacije. Kombinacije

Example

Sve permutacije skupa A su

$$\begin{array}{lll} \langle 1,2,3\rangle & , & \langle 1,3,2\rangle, \\ \langle 2,1,3\rangle & , & \langle 2,3,1\rangle, \\ \langle 3,1,2\rangle & , & \langle 3,2,1\rangle. \end{array}$$

U ovom slučaju postoji i 6 permutacija kupa A.

Permutacije. Kombinacije

- $P(n, k)$ - broj k-permutacija skupa od n elemenata
- $P(n, n)$ - broj permutacija skupa od n elemenata
- $C(n, k)$ - broj k-kombinacija skupa od n elemenata.

Broj k-kombinacija od n elemenata zapravo broj k-to članih podskupova skupa od n elemenata, pa onda $C(n, k)$ određuje i taj broj.

Permutacije. Kombinacije

- $P(n, k)$ - broj k-permutacija skupa od n elemenata
- $P(n, n)$ - broj permutacija skupa od n elemenata
- $C(n, k)$ - broj k-kombinacija skupa od n elemenata.

Broj k-kombinacija od n elemenata zapravo broj k-to članih podskupova skupa od n elemenata, pa onda $C(n, k)$ određuje i taj broj.

Permutacije. Kombinacije

Theorem

1. $P(n,k) = n \cdot (n-1) \cdots (n-k+1) = \dfrac{n!}{(n-k)!}$,
2. $P(n,n) = n \cdot (n-1) \cdots 2 \cdot 1 = n!$

Proof.

- Prvi član k-permutacije skupa od n elemenata može biti izabran na n načina
- Pošto je izabran jedan element, a u permutaciji se nalaze samo različiti elementi, preostaje $n-1$ element, koji se bira na $n-1$ način
- poslednji član permutacije se bira iz skupa koji sadrži $n-(k-1)$ element
- Prema pravilu proizvoda, $P(n,k) = n \cdot (n-1) \cdots (n-k+1)$.

(2) Direktna posledica (1) za $k = n$. □

Permutacije. Kombinacije

Theorem

1. $P(n,k) = n \cdot (n-1) \cdots (n-k+1) = \dfrac{n!}{(n-k)!}$,
2. $P(n,n) = n \cdot (n-1) \cdots 2 \cdot 1 = n!$

Proof.

- Prvi član k-permutacije skupa od n elemenata može biti izabran na n načina
- Pošto je izabran jedan element, a u permutaciji se nalaze samo različiti elementi, preostaje $n-1$ element, koji se bira na $n-1$ način
- poslednji član permutacije se bira iz skupa koji sadrži $n-(k-1)$ element
- Prema pravilu proizvoda, $P(n,k) = n \cdot (n-1) \cdots (n-k+1)$.

(2) Direktna posledica (1) za $k = n$. □

Permutacije. Kombinacije

Theorem

1. $P(n,k) = n \cdot (n-1) \cdots (n-k+1) = \dfrac{n!}{(n-k)!}$,
2. $P(n,n) = n \cdot (n-1) \cdots 2 \cdot 1 = n!$

Proof.

- Prvi član k-permutacije skupa od n elemenata može biti izabran na n načina
- Pošto je izabran jedan element, a u permutaciji se nalaze samo različiti elementi, preostaje $n-1$ element, koji se bira na $n-1$ način
- poslednji član permutacije se bira iz skupa koji sadrži $n-(k-1)$ element
- Prema pravilu proizvoda, $P(n,k) = n \cdot (n-1) \cdots (n-k+1)$.

(2) Direktna posledica (1) za $k = n$. □

Permutacije. Kombinacije

Theorem

1. $P(n,k) = n \cdot (n-1) \cdots (n-k+1) = \dfrac{n!}{(n-k)!}$,
2. $P(n,n) = n \cdot (n-1) \cdots 2 \cdot 1 = n!$

Proof.

- Prvi član k-permutacije skupa od n elemenata može biti izabran na n načina
- Pošto je izabran jedan element, a u permutaciji se nalaze samo različiti elementi, preostaje $n-1$ element, koji se bira na $n-1$ način
- poslednji član permutacije se bira iz skupa koji sadrži $n-(k-1)$ element
- Prema pravilu proizvoda, $P(n,k) = n \cdot (n-1) \cdots (n-k+1)$.

(2) Direktna posledica (1) za $k = n$. □

Permutacije. Kombinacije

Theorem

1. $P(n,k) = n \cdot (n-1) \cdots (n-k+1) = \dfrac{n!}{(n-k)!}$,
2. $P(n,n) = n \cdot (n-1) \cdots 2 \cdot 1 = n!$

Proof.

- Prvi član k-permutacije skupa od n elemenata može biti izabran na n načina
- Pošto je izabran jedan element, a u permutaciji se nalaze samo različiti elementi, preostaje $n-1$ element, koji se bira na $n-1$ način
- poslednji član permutacije se bira iz skupa koji sadrži $n-(k-1)$ element
- Prema pravilu proizvoda, $P(n,k) = n \cdot (n-1) \cdots (n-k+1)$.

(2) Direktna posledica (1) za $k = n$. □

Permutacije. Kombinacije

Theorem

$$C(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Proof.

- k-kombinacija od n elemenata - skup sa k elemenata
- Broj permutacija tog skupa je $k!$
- Ako je $C(n,k)$ broj k-kombinacija od n elemenata, onda je $k! \cdot C(n,k)$ ukupan broj k-permutacija od n elemenata
- $k! \cdot C(n,k) = \frac{n!}{(n-k)!}$
- $C(n,k) = \frac{n!}{k!(n-k)!}$

$\square$

$\binom{n}{k}$ se naziva *binomni koeficijent*

Permutacije. Kombinacije

Theorem

$$C(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Proof.

- k-kombinacija od n elemenata - skup sa k elemenata
- Broj permutacija tog skupa je $k!$
- Ako je $C(n,k)$ broj k-kombinacija od n elemenata, onda je $k! \cdot C(n,k)$ ukupan broj k-permutacija od n elemenata
- $k! \cdot C(n,k) = \frac{n!}{(n-k)!}$
- $C(n,k) = \frac{n!}{k!(n-k)!}$

□

$\binom{n}{k}$ se naziva *binomni koeficijent*

Permutacije. Kombinacije

Theorem

$$C(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Proof.

- k-kombinacija od n elemenata - skup sa k elemenata
- Broj permutacija tog skupa je $k!$
- Ako je $C(n,k)$ broj k-kombinacija od n elemenata, onda je $k! \cdot C(n,k)$ ukupan broj k-permutacija od n elemenata
- $k! \cdot C(n,k) = \frac{n!}{(n-k)!}$
- $C(n,k) = \frac{n!}{k!(n-k)!}$

□

$\binom{n}{k}$ se naziva *binomni koeficijent*

Permutacije. Kombinacije

Theorem

$$C(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Proof.

- k-kombinacija od n elemenata - skup sa k elemenata
- Broj permutacija tog skupa je $k!$
- Ako je $C(n,k)$ broj k-kombinacija od n elemenata, onda je $k! \cdot C(n,k)$ ukupan broj k-permutacija od n elemenata
- $k! \cdot C(n,k) = \frac{n!}{(n-k)!}$
- $C(n,k) = \frac{n!}{k!(n-k)!}$

□

$\binom{n}{k}$ se naziva *binomni koeficijent*

Permutacije. Kombinacije

Theorem

$$C(n,k) = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Proof.

- k-kombinacija od n elemenata - skup sa k elemenata
- Broj permutacija tog skupa je $k!$
- Ako je $C(n,k)$ broj k-kombinacija od n elemenata, onda je $k! \cdot C(n,k)$ ukupan broj k-permutacija od n elemenata
- $k! \cdot C(n,k) = \frac{n!}{(n-k)!}$
- $C(n,k) = \frac{n!}{k!(n-k)!}$

□

$\binom{n}{k}$ se naziva *binomni koeficijent*

Permutacije. Kombinacije

Example

Ako je $A = \{1, 2, 3\}$ i $|A| = |\{1, 2, 3\}| = 3$:

- $P(3, 2) = \frac{3!}{(3-2)!} = \frac{6}{1} = 6$,
- $P(3, 3) = 3! = 6$ i
- $C(n, k) = \binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{3!}{2!(3-2)!} = \frac{6}{2} = 3$.

Permutacije. Kombinacije

Broj k-kombinacija od n elemenata je broj k-to članih podskupova skupa od n elemenata:

Example

Broj načina na koji možemo izabrati 3 od 10 knjiga je

$$C(10,3) = \binom{10}{3} = \frac{10!}{3! \cdot 7!} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = \frac{720}{6} = 120$$

Example

- podskup od k elemenata n-to članog skupa prikazuje se binarnom reči dužine n sa tačno k jedinica
- broj podskupova sa tačno k elemenata skupa sa n elemenata je $C(n,k) = \binom{n}{k}$
- $C(n,k) = \binom{n}{k}$ je broj binarnih reči dužine n sa tačno k jedinica.

Permutacije. Kombinacije

Broj k-kombinacija od n elemenata je broj k-to članih podskupova skupa od n elemenata:

Example

Broj načina na koji možemo izabrati 3 od 10 knjiga je

$$C(10,3) = \binom{10}{3} = \frac{10!}{3! \cdot 7!} = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = \frac{720}{6} = 120$$

Example

- podskup od k elemenata n-to članog skupa prikazuje se binarnom reči dužine n sa tačno k jedinica
- broj podskupova sa tačno k elemenata skupa sa n elemenata je $C(n,k) = \binom{n}{k}$
- $C(n,k) = \binom{n}{k}$ je broj binarnih reči dužine n sa tačno k jedinica.

Permutacije. Kombinacije

Example

12 osoba treba da sedne za okrugli sto (sa 12 stolica). Ako u dva razmeštaja:

- svaka od 12 osoba ima istog suseda sa leve, odnosno sa desne strane,

reč je o istom rasporedu (razmeštaji se dobijaju rotacijom oko stola).
Rasporedi osoba - neke od permutacije tog skupa.
A - skup traženih rasporeda sedenja i B - skup svih permutacija osoba.
Broj osoba je 12, to je $|B| = P(12, 12) = 12!$.
Jednom rasporedu odgovara tačno 12 (zarotiranih) razmeštaja dobijenih pomeranjem proizvoljno određene prve osobe za po jedno mesto.
Postoji preslikavanje $f : B \mapsto A$ koje je $12-$u-1-funkcija.
Traženi broj rasporeda je $|A| = \frac{|B|}{12} = \frac{12!}{12} = 11!$.

Permutacije objekata među kojima ima istih

- ponekad je pogodno posmatrati skupove u kojima postoji više istih elemenata, takozvane n-skupove (multiskupove)
- $\{a, a, b\} \neq \{a, b\}$
- brojanje resurse iste vrste: da li je skup od 4 kuće isto što i skup koji ima samo jedan element (kuću)?
- indeksiranje elemenata: umesto skupa $\{a, a, b\}$ posmatramo skup $\{a_1, a_2, b\}$

Na dalje: pod (uopštenim) permutacijama n (ne nužno različitih) objekata podrazumevaćemo n-torke objekata bez obzira da li su oni različiti, ili ne.

Permutacije objekata među kojima ima istih

Example

Reč *aparat*: po jedno slovo p, r i t, i tri slova a.
(Uopštene) permutacije: *aaaprt*, *aaaptr*, ...
Koliko se različitih reči (uopštenih permutacija) dobija od slova iz *aparat*.
Slova a indeksiramo kao: a_1, a_2 i a_3. Reči oblika ...*prt*, su:

$$\langle a_1, a_2, a_3, p, r, t\rangle, \langle a_1, a_3, a_2, p, r, t\rangle, \langle a_2, a_1, a_3, p, r, t\rangle$$
$$\langle a_2, a_3, a_1, p, r, t\rangle, \langle a_3, a_1, a_2, p, r, t\rangle, \langle a_3, a_2, a_1, p, r, t\rangle$$

Od permutacije *aaaprt* tako bismo dobili $3! = 6$ novih. Isto važi i za bilo koji drugi fiksiran raspored slova p, r i t.
x - broj (uopštenih) permutacija
$x \cdot 3!$ - broju permutacija u kojima smo iste objekte indeksirali i smatramo ih za različite
$x \cdot 3! = P(6,6) = 6!$ (jer je $|\{a_1, a_2, a_3, p, r, t\}| = 6$), pa je $x = \frac{6!}{3!}$.

Permutacije objekata među kojima ima istih

Theorem

Neka su je dato k vrsta objekata, tako da i-te vrste ima n_i objekata, i neka je $n = \sum_{i=1}^{k} n_i$. Tada je broj permutacija tih n objekata jednak

$$\frac{n!}{n_1! \cdots n_k!}.$$

Proof.

- neka je x traženi broj permutacija
- za fiksiranu permutaciju n objekata, ako indeksiramo objekte prve vrste, dobijamo $x \cdot n_1!$ permutacija u kojima se svi objekti prve vrste posmatraju kao različiti, što se ponavlja dalje
- $x \cdot n_1! \cdots n_k! = P(n, n) = n!$
- $x = \frac{n!}{n_1! \cdots n_k!}$

Permutacije objekata među kojima ima istih

Theorem

Neka su je dato k vrsta objekata, tako da i-te vrste ima n_i objekata, i neka je $n = \sum_{i=1}^{k} n_i$. Tada je broj permutacija tih n objekata jednak

$$\frac{n!}{n_1! \cdots n_k!}.$$

Proof.

- neka je x traženi broj permutacija
- za fiksiranu permutaciju n objekata, ako indeksiramo objekte prve vrste, dobijamo $x \cdot n_1!$ permutacija u kojima se svi objekti prve vrste posmatraju kao različiti, što se ponavlja dalje
- $x \cdot n_1! \cdots n_k! = P(n, n) = n!$
- $x = \frac{n!}{n_1! \cdots n_k!}$

Permutacije objekata među kojima ima istih

Theorem

Neka su je dato k vrsta objekata, tako da i-te vrste ima n_i objekata, i neka je $n = \sum_{i=1}^{k} n_i$. Tada je broj permutacija tih n objekata jednak

$$\frac{n!}{n_1! \cdots n_k!}.$$

Proof.

- neka je x traženi broj permutacija
- za fiksiranu permutaciju n objekata, ako indeksiramo objekte prve vrste, dobijamo $x \cdot n_1!$ permutacija u kojima se svi objekti prve vrste posmatraju kao različiti, što se ponavlja dalje
- $x \cdot n_1! \cdots n_k! = P(n, n) = n!$
- $x = \frac{n!}{n_1! \cdots n_k!}$

Permutacije objekata među kojima ima istih

Theorem

Neka su je dato k vrsta objekata, tako da i-te vrste ima n_i objekata, i neka je $n = \sum_{i=1}^{k} n_i$. Tada je broj permutacija tih n objekata jednak

$$\frac{n!}{n_1! \cdots n_k!}.$$

Proof.

- neka je x traženi broj permutacija
- za fiksiranu permutaciju n objekata, ako indeksiramo objekte prve vrste, dobijamo $x \cdot n_1!$ permutacija u kojima se svi objekti prve vrste posmatraju kao različiti, što se ponavlja dalje
- $x \cdot n_1! \cdots n_k! = P(n, n) = n!$
- $x = \frac{n!}{n_1! \cdots n_k!}$

Permutacije objekata među kojima ima istih

Theorem

Neka su je dato k vrsta objekata, tako da i-te vrste ima n_i objekata, i neka je $n = \sum_{i=1}^{k} n_i$. Tada je broj permutacija tih n objekata jednak

$$\frac{n!}{n_1! \cdots n_k!}.$$

Proof.

- neka je x traženi broj permutacija
- za fiksiranu permutaciju n objekata, ako indeksiramo objekte prve vrste, dobijamo $x \cdot n_1!$ permutacija u kojima se svi objekti prve vrste posmatraju kao različiti, što se ponavlja dalje
- $x \cdot n_1! \cdots n_k! = P(n, n) = n!$
- $x = \frac{n!}{n_1! \cdots n_k!}$

Permutacije objekata među kojima ima istih

Example

Broj različitih reči koje se dobijaju od slova reči *poplava* je prema teoremi 89 jednak $\frac{7!}{2!\cdot 2!}$, jer je dužina reči 7, a slova *p* i *a* se u njoj javljaju po 2 puta.

Permutacije i kombinacije sa ponavljanjem

k-permutacije skupova sa višestrukim elementima:

- obično se podrazumeva da u svakoj vrsti postoji neograničen broj objekata, što se naziva i *k-permutacije sa ponavljanjem*
- može biti i $k > n$, gde je n broj vrsta objekata
- alternativno: u svakoj vrsti postoji samo jedan objekat, ali se on može birati neograničen broj puta. Tada je broj n vrsta objekata ujedno i broj objekata.

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-permutacija sa ponavljanjem je jednak n^k.

Proof.

Pošto u svakom od k koraka izbora možemo izabrati jedan od n elemenata, rezultat neposredno sledi prema pravilu proizvoda. □

Example

Broj različitih binarnih reči dužine 8 je $2^8 = 256$.
Reči dužine 2 sastavljenih od slova $\{a, b, c\}$ ima $3^2 = 9$: aa, ab, ac, ba, bb, bc, ca, cb i cc.

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-permutacija sa ponavljanjem je jednak n^k.

Proof.

Pošto u svakom od k koraka izbora možemo izabrati jedan od n elemenata, rezultat neposredno sledi prema pravilu proizvoda. □

Example

Broj različitih binarnih reči dužine 8 je $2^8 = 256$.
Reči dužine 2 sastavljenih od slova $\{a, b, c\}$ ima $3^2 = 9$: aa, ab, ac, ba, bb, bc, ca, cb i cc.

Permutacije i kombinacije sa ponavljanjem

k-kombinacije sa ponavljanjem:

- posmatraju se mogući izbori skupova, ali sada su to skupovi sa višestrukim elementima,
- postoji n objekata, ali se svaki od njih može birati više puta.

Example

Tri boje: plava, žuta i crvena (u dovoljnim količinama).
Treba obojiti 5 loptica: PPPPP, ŽŽŽŽŽ, CCCCC, PPCCC=CPCPC (reč je o kombinacijama!), ŽCPPP, ...

Permutacije i kombinacije sa ponavljanjem

k-kombinacije sa ponavljanjem:

- posmatraju se mogući izbori skupova, ali sada su to skupovi sa višestrukim elementima,
- postoji n objekata, ali se svaki od njih može birati više puta.

Example

Tri boje: plava, žuta i crvena (u dovoljnim količinama).
Treba obojiti 5 loptica: PPPPP, ŽŽŽŽŽ, CCCCC, PPCCC=CPCPC (reč je o kombinacijama!), ŽCPPP, ...

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-kombinacija sa ponavljanjem je jednak

$$\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Proof.

- $C = \{1, 2, \ldots, n\}$, $B = \{1, 2, \ldots, n, n+1, \ldots, n+k-1\}$
- $C' = \{c_1, \ldots, c_k\}$ jedna kombinacija, $c_i \leq c_{i+1}$, za $i = 1, k-1$ (moguće jer kombinacije su skupovi, redosled nije bitan)
- $C' \mapsto \{b_1, \ldots, b_k\} \subset B$: $b_1 = c_1$, $b_2 = c_2 + 1$, $\ldots$, $b_k = c_k + k - 1$
- pridruživanje je bijekcija, broj k-kombinacija bez ponavljanja za B je $C(n+k-1, k) = \binom{n+k-1}{k}$.

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-kombinacija sa ponavljanjem je jednak

$$\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Proof.

- $C = \{1, 2, \ldots, n\}$, $B = \{1, 2, \ldots, n, n+1, \ldots, n+k-1\}$
- $C' = \{c_1, \ldots, c_k\}$ jedna kombinacija, $c_i \leq c_{i+1}$, za $i = 1, k-1$ (moguće jer kombinacije su skupovi, redosled nije bitan)
- $C' \mapsto \{b_1, \ldots, b_k\} \subset B$: $b_1 = c_1$, $b_2 = c_2 + 1$, $\ldots$, $b_k = c_k + k - 1$
- pridruživanje je bijekcija, broj k-kombinacija bez ponavljanja za B je $C(n+k-1, k) = \binom{n+k-1}{k}$.

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-kombinacija sa ponavljanjem je jednak

$$\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Proof.

- $C = \{1, 2, \ldots, n\}$, $B = \{1, 2, \ldots, n, n+1, \ldots, n+k-1\}$
- $C' = \{c_1, \ldots, c_k\}$ jedna kombinacija, $c_i \leq c_{i+1}$, za $i = 1, k-1$ (moguće jer kombinacije su skupovi, redosled nije bitan)
- $C' \mapsto \{b_1, \ldots, b_k\} \subset B$: $b_1 = c_1$, $b_2 = c_2 + 1$, $\ldots$, $b_k = c_k + k - 1$
- pridruživanje je bijekcija, broj k-kombinacija bez ponavljanja za B je $C(n+k-1, k) = \binom{n+k-1}{k}$.

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-kombinacija sa ponavljanjem je jednak

$$\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Proof.

- $C = \{1, 2, \ldots, n\}$, $B = \{1, 2, \ldots, n, n+1, \ldots, n+k-1\}$
- $C' = \{c_1, \ldots, c_k\}$ jedna kombinacija, $c_i \leq c_{i+1}$, za $i = 1, k-1$ (moguće jer kombinacije su skupovi, redosled nije bitan)
- $C' \mapsto \{b_1, \ldots, b_k\} \subset B$: $b_1 = c_1$, $b_2 = c_2 + 1$, $\ldots$, $b_k = c_k + k - 1$
- pridruživanje je bijekcija, broj k-kombinacija bez ponavljanja za B je $C(n+k-1, k) = \binom{n+k-1}{k}$.

Permutacije i kombinacije sa ponavljanjem

Theorem

Neka su je dato n objekata. Broj k-kombinacija sa ponavljanjem je jednak

$$\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Proof.

- $C = \{1, 2, \ldots, n\}$, $B = \{1, 2, \ldots, n, n+1, \ldots, n+k-1\}$
- $C' = \{c_1, \ldots, c_k\}$ jedna kombinacija, $c_i \leq c_{i+1}$, za $i = 1, k-1$ (moguće jer kombinacije su skupovi, redosled nije bitan)
- $C' \mapsto \{b_1, \ldots, b_k\} \subset B$: $b_1 = c_1$, $b_2 = c_2 + 1$, $\ldots$, $b_k = c_k + k - 1$
- pridruživanje je bijekcija, broj k-kombinacija bez ponavljanja za B je $C(n+k-1, k) = \binom{n+k-1}{k}$.

Permutacije i kombinacije sa ponavljanjem

Example

- tri boje: plava, žuta i crvena (u dovoljnim količinama)
- Treba obojiti 5 loptica: PPPPP, ŽŽŽŽŽ, CCCCC, PPCCC, ŽCPPP, ...
- $n = 3$, $k = 5$
- broj različitih bojenja je $\binom{3+5-1}{5} = \binom{7}{5} = \frac{7!}{5!(7-5)!} = 21$

Kombinatorijalni dokazi

Primena tehnika prebrojavanja u dokazivanju nekih identiteta - *kombinatorijani dokaz*:

- Posmatra se neki skup A
- pomoću postupaka prebrojavanja se utvrdi da je $|A| = n$ i $|A| = m$
- zaključak: $n = m$.

Theorem (Pascal-ov identitet)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Blaise Pascal, 1623 – 1662

Francuski naučnik i pronalazač, pisac i (nakon mističnog iskustva) hrišćanski filozof. Konstruisao mehanički kalkulator Pascaline (1642-1652). Kao veoma mlad postavio osnove teorije verovatnoće i projektivne geometrije (sa 17 godina).

Pascal-ov identitet

Theorem (Pascal-ov identitet)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Proof.

- $\binom{n}{k}$ broj k-točlanih podskupova n-točlanog skupa A
- a - jedan fiksiran element skupa
- k-točlani podskupovi skupa A se dele u dve grupe:
  - skupovi koji sadrže a i njih ima $\binom{n-1}{k-1}$ i
  - skupovi koji ne sadrže a i njih ima $\binom{n-1}{k}$

□

Pascal-ov identitet

Theorem (Pascal-ov identitet)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Proof.

- $\binom{n}{k}$ broj k-točlanih podskupova n-točlanog skupa A
- a - jedan fiksiran element skupa
- k-točlani podskupovi skupa A se dele u dve grupe:
  - skupovi koji sadrže a i njih ima $\binom{n-1}{k-1}$ i
  - skupovi koji ne sadrže a i njih ima $\binom{n-1}{k}$

Pascal-ov identitet

Theorem (Pascal-ov identitet)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Proof.

- $\binom{n}{k}$ broj k-točlanih podskupova n-točlanog skupa A
- a - jedan fiksiran element skupa
- k-točlani podskupovi skupa A se dele u dve grupe:
  - skupovi koji sadrže a i njih ima $\binom{n-1}{k-1}$ i
  - skupovi koji ne sadrže a i njih ima $\binom{n-1}{k}$

Pascal-ov identitet

Theorem (Pascal-ov identitet)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Proof.

- $\binom{n}{k}$ broj k-točlanih podskupova n-točlanog skupa A
- a - jedan fiksiran element skupa
- k-točlani podskupovi skupa A se dele u dve grupe:
  - skupovi koji sadrže a i njih ima $\binom{n-1}{k-1}$ i
  - skupovi koji ne sadrže a i njih ima $\binom{n-1}{k}$

Binomni koeficijent

Vrednosti $\binom{n}{k}$ se, pomoću Pascal-ovog identiteta, određuju iz *Pascal-ovog trougla*:

$$
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
 & & & & \dots & & & & & &
\end{array}
$$

koji zapravo predstavlja zapis za

$$
\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & & & & \dots & & & & & &
\end{array}
$$

Kombinatorijalni dokazi

Theorem (Binomna teorema)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof.

- $(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n}$
- primenom distributivnih zakona dobija se zbir od 2^n proizvoda oblika $e_1 \cdot e_2 \cdots e_n$, gde je svaki od e_i dobijen izborom iz skupa $\{x, y\}$ u i-tom faktoru proizvoda
- $e_1 \cdot e_2 \cdots e_n$ možemo posmatrati kao reči nad dvočlanim skupom, (binarne reči dužine n sa k jedinica kodiraju k-točlane podskupove skupa sa n elemenata)
- proizvoda $e_1 \cdot e_2 \cdots e_n$ koji se svode na $x^{n-k} y^k$ ima upravo $\binom{n}{k}$

Kombinatorijalni dokazi

Theorem (Binomna teorema)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof.

- $(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n}$
- primenom distributivnih zakona dobija se zbir od 2^n proizvoda oblika $e_1 \cdot e_2 \cdots e_n$, gde je svaki od e_i dobijen izborom iz skupa $\{x, y\}$ u i-tom faktoru proizvoda
- $e_1 \cdot e_2 \cdots e_n$ možemo posmatrati kao reči nad dvočlanim skupom, (binarne reči dužine n sa k jedinica kodiraju k-točlane podskupove skupa sa n elemenata)
- proizvoda $e_1 \cdot e_2 \cdots e_n$ koji se svode na $x^{n-k} y^k$ ima upravo $\binom{n}{k}$

Kombinatorijalni dokazi

Theorem (Binomna teorema)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof.

- $(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n}$
- primenom distributivnih zakona dobija se zbir od 2^n proizvoda oblika $e_1 \cdot e_2 \cdots e_n$, gde je svaki od e_i dobijen izborom iz skupa $\{x, y\}$ u i-tom faktoru proizvoda
- $e_1 \cdot e_2 \cdots e_n$ možemo posmatrati kao reči nad dvočlanim skupom, (binarne reči dužine n sa k jedinica kodiraju k-točlane podskupove skupa sa n elemenata)
- proizvoda $e_1 \cdot e_2 \cdots e_n$ koji se svode na $x^{n-k}y^k$ ima upravo $\binom{n}{k}$

Kombinatorijalni dokazi

Theorem (Binomna teorema)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof.

- $(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n}$
- primenom distributivnih zakona dobija se zbir od 2^n proizvoda oblika $e_1 \cdot e_2 \cdots e_n$, gde je svaki od e_i dobijen izborom iz skupa $\{x, y\}$ u i-tom faktoru proizvoda
- $e_1 \cdot e_2 \cdots e_n$ možemo posmatrati kao reči nad dvočlanim skupom, (binarne reči dužine n sa k jedinica kodiraju k-točlane podskupove skupa sa n elemenata)
- proizvoda $e_1 \cdot e_2 \cdots e_n$ koji se svode na $x^{n-k}y^k$ ima upravo $\binom{n}{k}$

Kombinatorijalni dokazi

Primene:

- $(x+y)^4 = 1 \cdot x^4 + 4 \cdot x^3 \cdot y + 6 \cdot x^2 \cdot y^2 + 4 \cdot x \cdot y^3 + 1 \cdot y^4$
- (za $x = y = 1$):

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$$

- (za $y = 1$):

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Rekurentne relacije

Rekurentna relacija je jednačina u kojoj se n-ti član niza definiše preko svojih prethodnika.

Fibonačijevi brojevi:

- inicijalne vrednosti $F_0 = 0$ i $F_1 = 1$ i
- rekurentna relacija $F_n = F_{n-1} + F_{n-2}$,

tako da je:

- $F_2 = F_1 + F_0 = 1$,
- $F_3 = F_2 + F_1 = F_1 + F_0 + F_1 = 2 \cdot F_1 + F_0 = 2$ itd.

Prvih nekoliko članova niza su: $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

Leonardo Fibonacci, oko 1170 - oko 1250

Leonardo Pisano Bigollo, Leonardo Fibonacci (filius Bonacci, "sin Bonaccio-a") je u tekstu "Liber Abaci" ("Knjiga o abakusu", ili: "Knjiga o izračunavanju") iz 1202. godine, predstavljajući istočnjačke matematičke rezultate zapadno-evropskoj naučnoj publici, opisao niz brojeva kasnije nazvan po njemu.

Leonardo Fibonacci, oko 1170 - oko 1250

Ako se par zečeva razmnožava svakog meseca i dobija novi par (ženku i mužjaka), a novi par se kroz dva meseca razmnožava na isti način, koliko zečeva će biti na kraju godine ako je na početku godine bio jedan par zečeva spremnih za reprodukciju?

Pravilnost koja određuje članove ovog niza se često javlja u prirodi. Količnik uzastopnih članova niza teži zlatnom preseku $\frac{1+\sqrt{5}}{2} = 1,618\ldots$

`http://www.youtube.com/watch?v=kkGeOWYOFoA&feature=player_embedded`

Film ilustruje Fibonačijevu krivu koja povezuje naspramne uglove kvadrata stranica 1, 1, 2, 3, 5, 8, 13, ... (Fibonačijevi brojevi).

Rekurentne relacije

Definition

(Linearna) homogena rekurentna relacija sa konstantnim simbolima reda k je jednačina oblika:

$$a_n = \sum_{i=1}^{k} c_i \cdot a_{n-i}$$

gde su $c_1, \ldots, c_k$ konstante, $c_k \neq 0$, i $n \geq k$. Niz $\{x_n\}_n$ je *rešenje* ove relacije ako je za svako $n \geq k$ ispunjeno da je $x_n = \sum_{i=1}^{k} c_i \cdot x_{n-i}$.

Tek davanje inicijalnih vrednosti $a_0, \ldots, a_{k-1}$ za početne članove na jedinstveni način određuje niz $\{x_n\}_n$. Bez tih vrednosti postoji beskonačno mnogo rešenja, tj. nizova koji zadovoljavaju konkretnu rekurentnu relaciju.

Rekurentne relacije

Example

Fibonačijev niz brojeva je određen linearnom rekurentnom relacijom sa konstantnim simbolima reda 2 u kojoj su $c_1 = c_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ i inicijalne vrednosti $F_0 = 0$ i $F_1 = 1$.

Example

Označimo sa s_n broj podskupova skupa sa n elemenata. Tada je linearna rekurentna relacija sa konstantnim simbolima reda 1 u kojoj su $c_1 = 2$:

- $s_0 = 1$, inicijalna vrednost i
- $s_{n+1} = 2 \cdot s_n$.

Rekurentne relacije

Definition

Opšte rešenje linearne rekurentne relacije $a_n = \sum_{i=1}^{k} c_i \cdot a_{n-i}$ reda k je niz koji zavisi od k parametara $\alpha_1, \ldots, \alpha_k$ čijim pogodnim izborom se dobija svako drugo rešenje posmatrane relacije.

Cilj nam je da polazeći od neke rekurentne relacije konstruišemo njeno opšte rešenje iz koga se kasnije dobijaju svi konkretni nizovi koji zadovoljavaju relaciju.

Rekurentne relacije

Definition

Karakteristični polinom linearne rekurentne relacije sa konstantnim simbolima reda k

$$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k}$$

je polinom oblika

$$P(x) = x^k - c_1 \cdot x^{k-1} - c_2 \cdot x^{k-2} - \cdots - c_k$$

sa koeficijentima $c_1, \ldots, c_k$ koji se javljaju u rekurentnoj relaciji.

U nastavku, jednostavnosti radi, pretpostavimo da je red rekurentne relacije $k = 2$.

Rekurentne relacije

Theorem

Neka je $a_{n+2} = c_1 \cdot a_{n+1} + c_2 \cdot a_n$ rekurentna relacija i $x^2 - c_1 \cdot x - c_2$ njoj odgovarajući karakteristični polinom. Ako je r koren karakterističnog polinoma, onda niz $\{r^i\}_{i=0}^{\infty}$ zadovoljava rekurentnu relaciju.

Proof.

Neka je r rešenje jednačine $x^2 - c_1 \cdot x - c_2 = 0$. Ako je niz $\{r^i\}_{i=0}^{\infty}$ rešenje relacije:

$$r^{n+1} = c_1 \cdot r^n + c_2 \cdot r^{n-1}, \text{ tj.}$$

$$0 = r^{n-1}(r^2 - c_1 \cdot r - c_2),$$

što je tačno s obzirom da je r rešenje jednačine $x^2 - c_1 \cdot x - c_2 = 0$. □

Rekurentne relacije

Theorem

Neka je $a_{n+2} = c_1 \cdot a_{n+1} + c_2 \cdot a_n$ rekurentna relacija i neka su nizovi $\{x_i\}_i$ i $\{y_i\}_i$ njena rešenja i A i B proizvoljni realni brojevi. Tada je i niz

$$\{A \cdot x_i + B \cdot y_i\}_i$$

rešenje posmatrane relacije.

Proof.

Pošto su $\{x_i\}_i$ i $\{y_i\}_i$ rešenja važi:

- $x_{n+2} = c_1 \cdot x_{n+1} + c_2 \cdot x_n$, $y_{n+2} = c_1 \cdot y_{n+1} + c_2 \cdot y_n$,
- $A \cdot x_{n+2} = c_1 \cdot A \cdot x_{n+1} + c_2 \cdot A \cdot x_n$, $B \cdot y_{n+2} = c_1 \cdot B \cdot y_{n+1} + c_2 \cdot B \cdot y_n$ i
- $A \cdot x_{n+2} + B \cdot y_{n+2} = c_1(A \cdot x_{n+1} + B \cdot y_{n+1}) + c_2(A \cdot x_n + B \cdot y_n)$,

pa je i posmatrana linearna kombinacija rešenje rekurentne relacije. □

Rekurentne relacije

Theorem

Neka su r_1 i r_2 dva različita realna rešenje jednačine $x^2 - c_1 \cdot x - c_2 = 0$. Tada je niz

$$\{d_1 \cdot r_1^n + d_2 \cdot r_2^n\}_n,$$

gde su d_1 i d_2 proizvoljne konstante, opšte rešenje rekurentne relacije $a_{n+2} = c_1 \cdot a_{n+1} + c_2 \cdot a_n$.

Proof.

Prema prethodnom: $\{r_1^n\}_n$ i $\{r_2^n\}_n$ jesu rešenja,pa je to i njihova linearna kombinacija.
Neka je $\{b_n\}_n$ proizvoljno rešenje posmatrane rekurentne relacije.
Odredimo d_1 i d_2 tako da je $b_n = d_1 \cdot r_1^n + d_2 \cdot r_2^n$. □

Rekurentne relacije

Nastavak dokaza:

Pošto je svako konkretno rešenje jednoznačno određeno vrednostima prva dva člana niza:

$$\begin{aligned} d_1 + d_2 &= b_0 \\ d_1 r_1 + d_2 r_2 &= b_1 \end{aligned}$$

koji ima jedinstvena rešenja po d_1 i d_2:

$$d_1 = \frac{b_1 - b_0 r_2}{r_1 - r_2}, \quad d_2 = \frac{b_1 r_1 - b_2}{r_1 - r_2}$$

jer je $r_1 \neq r_2$. $\{b_n\}_n$ je dobijeno iz opšteg rešenja.

Rekurentne relacije

Theorem

Neka je r jedinstveno realno rešenje jednačine $x^2 - c_1 \cdot x - c_2 = 0$. Tada je niz

$$\{d_1 \cdot r^n + d_2 \cdot (n+1) \cdot r^n\}_n,$$

gde su d_1 i d_2 parametri (proizvoljne konstante), opšte rešenje rekurentne relacije $a_{n+2} = c_1 \cdot a_{n+1} + c_2 \cdot a_n$.

Rekurentne relacije

Theorem

Neka su dati linearna rekurentna relacija sa konstantnim simbolima reda k $a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \cdots + c_k \cdot a_{n-k}$ *i njen karakteristični polinom* $P(x) = x^k - c_1 \cdot x^{k-1} - c_2 \cdot x^{k-2} - \cdots - c_k$. *Neka su svi koreni polinoma* $r_1, \ldots, r_k$ *međusobno različiti, onda je opšte rešenje rekurentne relacije oblika:*

$$\{d_1 r_1^n + d_2 r_2^n + \cdots + d_k r_k^n\}_n.$$

Ako je neki koren r_a *polinoma višestruk (reda l), onda će njemu odgovarati član u zbiru (koji daje opšte rešenje) oblika*

$$r_a^n[d_1 + d_2(n+1)\cdots + d_l(n+1)^{l-1}].$$

Rekurentne relacije

Example

Linearna rekurentna relacija za Fibonačijev niz brojeva je oblika

$$F_n = c_1 \cdot F_{n-1} + c_2 \cdot F_{n-2},$$

pri čemu važi $c_1 = c_2 = 1$. Ponovimo da bez zadavanja vrednosti prva dva člana niza ova relacija određuje beskonačno mnogo nizova. Karakteristični polinom je oblika

$$x^2 - x - 1$$

i njegovi koreni su

$$r_1 = \frac{1+\sqrt{5}}{2} \quad \text{i} \quad r_2 = \frac{1-\sqrt{5}}{2}.$$

Rekurentne relacije

Nastavak primera:

$$\left\{ d_1 \left(\frac{1+\sqrt{5}}{2} \right)^n + d_2 \left(\frac{1-\sqrt{5}}{2} \right)^n \right\}_n$$

je opšte rešenje relacije.

Inicijalne vrednosti su $F_0 = 0$ i $F_1 = 1$: $d_1 = \frac{1}{\sqrt{5}}$, $d_2 = -\frac{1}{\sqrt{5}}$.

Formula opšteg člana Fibonačijevog niza F_n je:

$$\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Rekurentne relacije

Example

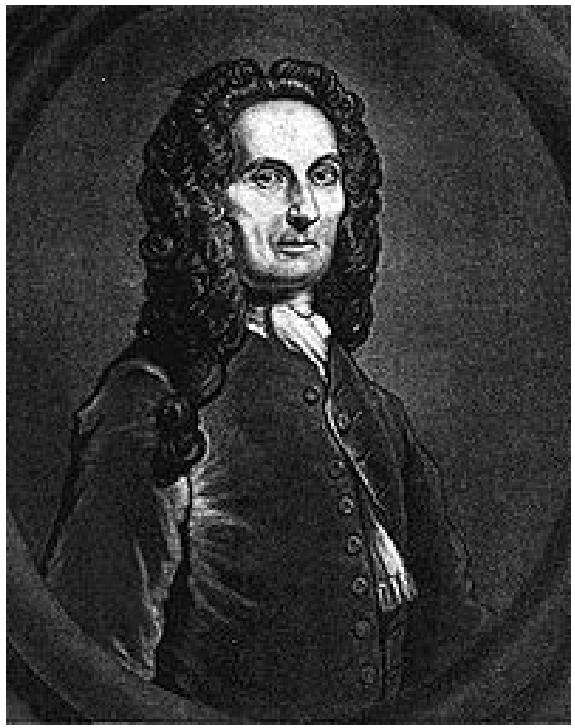
- s_n broj binarnih reči dužine n koje ne sadrže podreč 00
- $s_1 = 2$, jer obe reči dužine 1 ispunjavaju traženo svojstvo, $s_2 = 3$
- $s_1 = F_3$, $s_3 = F_4$, F_n je n-ti član Fibonačijevog niza
- kao i kod Fibonačijevog niza, rekurentna relacija je $s_n = s_{n-1} + s_{n-2}$
- svaka binarna reč koja ne sadrži podreč 00 završava se sa 1 ili 10
- broj reči dužine n koje se završavaju sa 1 je s_{n-1} jer brisanjem poslednjeg znaka 1 iz binarnih reči dužine n dobijamo reči dužine $n-1$ u kojima se ne nalazi podreč 00
- broj reči dužine n koje se završavaju sa 10 je s_{n-2}.
- $s_n = F_{n+2}$.

Generatorne funkcije

Generatorne funkcije (*proizvodne funkcije*):

- formalni zapisi stepenih redova čiji koeficijenti na neki način kodiraju informaciju o nizovima brojeva
- 'formalni':
  - domeni i kodomeni ovih funkcija se ne određuju
  - njihove vrednosti se ne izračunavaju za konretne vrednosti argumenata
  - naglasak je na (matematičkim) operacijama koje se primenjuju prilikom manipulacije koeficijentima
- interesantne su primene u situacijama kada se problemi koji se originalno odnose na nizove rešavaju sredstvima koja se odnose na funkcije.

Abraham de Moivre, 1667 – 1754



Abraham de Moivre, francuski matematčar, uveo generatorne funkcije kao sredstvo za rešavanje rekurentnih relacija (za Fibonačijeve brojeve). Poznat je po radovima iz verovatnoće, kompleksnih brojeva i trigonometrije. Kao protestant je prešao u Englesku, gde je drugovao sa Newton-om, Halley-em, Stirling-om. Umro je u Londonu.

Generatorne funkcije

Definition

Stepeni red

$$G(a) = \sum_{n=0}^{\infty} a_n \cdot x^n$$

je *generatorna funkcija* niza brojeva $\{a_n\}_n$.

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ oblika $\langle 1, 0, 0, \ldots \rangle$, tj. dat sa $a_0 = 1$ i $a_n = 0$, za $n > 0$, onda je generatorna funkcija:

- $G(a) = 1$.

Ako je niz $\{a_n\}_n$ oblika $\langle c, 0, 0, \ldots \rangle$, tj. dat sa $a_0 = c$, za neku konstantu c, a $a_n = 0$, za $n > 0$, onda je generatorna funkcija:

- $G(a) = c$, tj. konstanta funkcija.

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ oblika $\langle 1, 0, 0, \ldots \rangle$, tj. dat sa $a_0 = 1$ i $a_n = 0$, za $n > 0$, onda je generatorna funkcija:

- $G(a) = 1$.

Ako je niz $\{a_n\}_n$ oblika $\langle c, 0, 0, \ldots \rangle$, tj. dat sa $a_0 = c$, za neku konstantu c, a $a_n = 0$, za $n > 0$, onda je generatorna funkcija:

- $G(a) = c$, tj. konstanta funkcija.

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ oblika $\langle 0, 1, 0, \ldots \rangle$, tj. dat sa $a_0 = 0$, $a_1 = 1$ i $a_n = 0$, za $n > 1$, onda je generatorna funkcija:

- $G(a) = x$, tj. identička funkcija.

Ako je niz $\{a_n\}_n$ oblika $\langle 1, 1, 1, \ldots \rangle$, tj. dat sa $a_n = 1$, za $n \geq 0$, onda je generatorna funkcija:

- $G(a) = 1 + x + x^2 + \cdots + x^n + \cdots$ geometrijski red

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ oblika $\langle 0, 1, 0, \ldots \rangle$, tj. dat sa $a_0 = 0$, $a_1 = 1$ i $a_n = 0$, za $n > 1$, onda je generatorna funkcija:

- $G(a) = x$, tj. identička funkcija.

Ako je niz $\{a_n\}_n$ oblika $\langle 1, 1, 1, \ldots \rangle$, tj. dat sa $a_n = 1$, za $n \geq 0$, onda je generatorna funkcija:

- $G(a) = 1 + x + x^2 + \cdots + x^n + \cdots$ geometrijski red

Generatorne funkcije

- niz $\{a_n\}_n = \langle 1, 1, 1, \ldots \rangle$
- generatorna funkcija (geometrijski red)
  $G(a) = 1 + x + x^2 + \cdots + x^n + \cdots$
- za realne $|x| < 1$, geometrijski red generatorne funkcije konvergira i to je razvoj funkcije

$$\frac{1}{1-x}$$

  u Tejlorov red
- ne vodi se računa o konvergenciji
- izraz $\frac{1}{1-x}$ naziva *zatvorena forma* generatorne funkcije
  $1 + x + x^2 + \cdots + x^n + \cdots$

Brook Taylor, 1685 - 1731, James Gregory, 1638 - 1675

Brook Taylor, engleski matematičar (slika levo), po kome je nazvan red koji aproksimira funkciju u okolini tačke:

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f^{(3)}(a)}{3!}(x-a)^3 + \cdots$$

mada je prvi taj rezultat dobio James Gregory (desno).

Generatorne funkcije - metoda

Example

- niz $\{a_n\}_n$ za koji važi: $a_0 = 0$, $a_{n+1} = 2a_n + 1$
- $G(a) = \sum_{n=0}^{\infty} a_n \cdot x^n$.
- pomnožiti obe strane rekurentne relacije sa x^n:
  - $\sum_{n\geq 0} a_{n+1}x^n = \frac{1}{x}[(a_0 + a_1x + a_2x + \cdots) - a_0] = \frac{G(a)}{x}$ $(a_0 = 0)$
  - $\sum_{n\geq 0}(2a_n + 1)x^n = 2G(a) + \sum_{n\geq 0} x^n = 2G(a) + \frac{1}{1-x}$
- $\frac{G(a)}{x} = 2G(a) + \frac{1}{1-x}$
- $G(a) = \frac{x}{(1-x)(1-2x)}$
- $G(a) = x\left(\frac{2}{1-2x} - \frac{1}{1-x}\right) =$
  $(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots) - (1 + x + x^2 + x^3 + \cdots)$
- $a_n = 2^n - 1$

Generatorne funkcije - metoda

Example

- niz $\{a_n\}_n$ za koji važi: $a_0 = 0$, $a_{n+1} = 2a_n + 1$
- $G(a) = \sum_{n=0}^{\infty} a_n \cdot x^n$.
- pomnožiti obe strane rekurentne relacije sa x^n:
  - $\sum_{n\geq 0} a_{n+1}x^n = \frac{1}{x}[(a_0 + a_1x + a_2x + \cdots) - a_0] = \frac{G(a)}{x}$ $(a_0 = 0)$
  - $\sum_{n\geq 0}(2a_n + 1)x^n = 2G(a) + \sum_{n\geq 0} x^n = 2G(a) + \frac{1}{1-x}$
- $\frac{G(a)}{x} = 2G(a) + \frac{1}{1-x}$
- $G(a) = \frac{x}{(1-x)(1-2x)}$
- $G(a) = x\left(\frac{2}{1-2x} - \frac{1}{1-x}\right) =$
  $(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots) - (1 + x + x^2 + x^3 + \cdots)$
- $a_n = 2^n - 1$

Generatorne funkcije - metoda

Example

- niz $\{a_n\}_n$ za koji važi: $a_0 = 0$, $a_{n+1} = 2a_n + 1$
- $G(a) = \sum_{n=0}^{\infty} a_n \cdot x^n$.
- pomnožiti obe strane rekurentne relacije sa x^n:
  - $\sum_{n\geq 0} a_{n+1}x^n = \frac{1}{x}[(a_0 + a_1x + a_2x + \cdots) - a_0] = \frac{G(a)}{x}$ $(a_0 = 0)$
  - $\sum_{n\geq 0}(2a_n + 1)x^n = 2G(a) + \sum_{n\geq 0} x^n = 2G(a) + \frac{1}{1-x}$
- $\frac{G(a)}{x} = 2G(a) + \frac{1}{1-x}$
- $G(a) = \frac{x}{(1-x)(1-2x)}$
- $G(a) = x\left(\frac{2}{1-2x} - \frac{1}{1-x}\right) =$
  $(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots) - (1 + x + x^2 + x^3 + \cdots)$
- $a_n = 2^n - 1$

Generatorne funkcije - metoda

Example

- niz $\{a_n\}_n$ za koji važi: $a_0 = 0$, $a_{n+1} = 2a_n + 1$
- $G(a) = \sum_{n=0}^{\infty} a_n \cdot x^n$.
- pomnožiti obe strane rekurentne relacije sa x^n:
  - $\sum_{n\geq 0} a_{n+1}x^n = \frac{1}{x}[(a_0 + a_1x + a_2x + \cdots) - a_0] = \frac{G(a)}{x}$ $(a_0 = 0)$
  - $\sum_{n\geq 0}(2a_n + 1)x^n = 2G(a) + \sum_{n\geq 0} x^n = 2G(a) + \frac{1}{1-x}$
- $\frac{G(a)}{x} = 2G(a) + \frac{1}{1-x}$
- $G(a) = \frac{x}{(1-x)(1-2x)}$
- $G(a) = x\left(\frac{2}{1-2x} - \frac{1}{1-x}\right) =$
  $(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots) - (1 + x + x^2 + x^3 + \cdots)$
- $a_n = 2^n - 1$

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ oblika $\langle 1, c, c^2, \ldots \rangle$, tj. dat sa $a_n = c^n$, za $n \geq 0$ i neku konstantu c, onda je za generatornu funkciju:

- $G(a) = 1 + c \cdot x + c^2 \cdot x^2 + \cdots + c^n \cdot x^n + \cdots$ zatvorena forma izraz

$$\frac{1}{1 - c \cdot x}$$

Ako je niz $\{a_n\}_n$ oblika $\langle 1, -1, 1, \ldots \rangle$, tj. dat sa $a_n = (-1)^n$ za $n \geq 0$, onda je za generatornu funkciju:

- $G(a) = 1 - x + x^2 - x^3 + x^4 - \cdots$ zatvorena forma izraz

$$\frac{1}{1 + x}$$

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ oblika $\langle 1, 0, 1, 0, \ldots \rangle$, tj. dat sa $a_{2n} = 1$ i $a_{2n+1} = 0$ za $n \geq 0$, onda je za generatornu funkciju:

- $G(a) = 1 + x^2 + x^4 + \cdots$ zatvorena forma izraz

$$\frac{1}{1 - x^2}$$

Ako je niz $\{a_n\}_n$ dat sa $a_n = \frac{1}{n!}$ za $n \geq 0$, onda je za generatornu funkciju:

- $G(a) = 1 + x + \frac{1}{2}x^2 + \cdots$ zatvorena forma izraz

$$e^x$$

Generatorne funkcije

Example

Ako je niz $\{a_n\}_n$ dat sa $a_i = \binom{k}{i}$ za neko fiksirano k i $i = 0, 1, \ldots, k$, a $a_i = 0$ za $i > k$, odnosno

$$a = \left\langle \binom{k}{0}, \binom{k}{1}, \ldots, \binom{k}{k-1}, \binom{k}{k}, 0, 0, \ldots \right\rangle,$$

onda je za generatornu funkciju:

- $G(a) = \binom{k}{0} + \binom{k}{1}x + \ldots + \binom{k}{k}x^k$ zatvorena forma izraz

$$(1+x)^k$$

Generatorne funkcije

Sa generatornim funkcijama i njihovim zatvorenim formama radi se formalno, ne razmatrajući konvergenciju.

Definition

Generatorne funkcije $G(a)$ i $G(b)$ nizova $\{a_n\}_n$ i $\{b_n\}_n$ su jednake ako su jednaki odgovarajući nizovi, tj. ako je za svako $n \in \mathbb{N}$, $a_n = b_n$. ■

Operacije na generatornim funkcijama

- $G(a)$, $G(b)$ generatorne funkcija nizova $\{a_n\}_n$ i $\{b_n\}_n$

- Skaliranje: $G(c \cdot a) = c \cdot G(a)$, za niz $\{c \cdot a_n\}_n$
- Sabiranje: $G(a \pm b) = G(a) \pm G(b)$, za niz $\{a_n \pm b_n\}_n$
- Proizvod: $G(a \cdot b) = \sum_{n=0}^{\infty}(\sum_{k=0}^{n} a_k \cdot b_{n-k}) \cdot x^n$
- Pomeranja: $b_0 = \ldots = b_{k-1} = 0$, a $b_{k+i} = a_i$, za $i \geq 0$
  $G(b) = x^k G(a)$
- Diferenciranje: $b_n = (n+1)a_{n+1}$
  $G(b) = G'(a)$ je izvod od $G(a)$.

Operacije na generatornim funkcijama

Pravilo skaliranja: $G(c \cdot a) = c \cdot G(a)$

Example

- $G(a) = 1$, za $a = \langle 1, 0, 0, \ldots \rangle$,
  $G(c \cdot a) = c$, za $c \cdot a = \langle c, 0, 0, \ldots \rangle$

- $G(a) = 1 + x^2 + x^4 + \cdots = \dfrac{1}{1 - x^2}$, za $a = \langle 1, 0, 1, 0, \ldots \rangle$

  $G(a) = 2 + 2x^2 + 2x^4 + \cdots = \dfrac{2}{1 - x^2}$, za $2 \cdot a = \langle 2, 0, 2, 0, \ldots \rangle$

Operacije na generatornim funkcijama

Pravilo sabiranja: $G(a+b) = G(a) + G(b)$

Example

- $G(a) = 1 + x + x^2 + x^3 + x^4 + \cdots = \frac{1}{1-x}$, za $a = \langle 1, 1, 1, 1, \ldots \rangle$
- $G(b) = 1 - x + x^2 - x^3 + x^4 - \cdots = \frac{1}{1+x}$, za $b = \langle 1, -1, 1, -1, \ldots \rangle$

- za $a + b = \langle 2, 0, 2, 0, \ldots \rangle$ je

$$G(a+b) = 2 + 2 \cdot x^2 + 2 \cdot x^4 + \cdots = \frac{1}{1-x} + \frac{1}{1+x} = \frac{2}{1-x^2}$$

Operacije na generatornim funkcijama

Pravilo pomeranja: $b_0 = \ldots = b_{k-1} = 0$, a $b_{k+i} = a_i$, za $i \geq 0$
$G(b) = x^k G(a)$

Example

- $G(a) = 1 + x + x^2 + x^3 + x^4 + \cdots = \frac{1}{1-x}$, za $a = \langle 1, 1, 1, 1, \ldots \rangle$
- $b = \langle \underbrace{0, \ldots 0}_{k}, 1, 1, \ldots \rangle$
- $G(b) = x^k + x^{k+1} + \cdots = \frac{x^k}{1-x}$

Operacije na generatornim funkcijama

Pravilo proizvoda:
$G(a \cdot b) = \sum_{n=0}^{\infty}(\sum_{k=0}^{n} a_k \cdot b_{n-k}) \cdot x^n = a_0 \cdot b_0 + (a_0 \cdot b_1 + b_0 \cdot a_1)x + \cdots$

Example

- $(1 - x)(1 + x + x^2 = x^3 + \cdots) = 1$
- stepeni red čiji su koeficijenti $a_0 = 1$, $a_1 = -1$, $a_k = 0$, za $k \geq 2$ je *inverzan* stepenom redu sa koeficijentima određenim nizom $b = \langle 1, 1, 1, 1, \ldots \rangle$

Operacije na generatornim funkcijama

Pravilo diferenciranja: $\{a_n\}_n$, $\{b_n\}_n$: $b_i = (i+1)a_{i+1}$
$G(b) = G'(a)$

Example

- $G(a) = 1 + x + x^2 + x^3 + x^4 + \cdots = \frac{1}{1-x}$, za $a = \langle 1, 1, 1, 1, \ldots \rangle$
- $\frac{d}{dx}\left(\frac{1}{1-x}\right) = \frac{1}{(1-x)^2}$
- $G(b) = 1 + 2 \cdot x + 3 \cdot x^2 + \cdots = \frac{1}{(1-x)^2}$, za $b = \langle 1, 2, 3, \ldots \rangle$

Izračunavanje zatvorene forme generatorne funkcije

- Fibonačijev niz: $F = \langle 0, 1, 1, 2, 3, 5, \ldots \rangle$
- $G(F) = 0 + 1 \cdot x + 1 \cdot x^2 + 2 \cdot x^3 + 3 \cdot x^4 + 5 \cdot x^5 + \ldots$
- $F_0 = 0$, $F_1 = 1$, $F_2 = F_1 + F_0 = 1$, $F_3 = F_2 + F_1 = 2$, $F_4 = F_3 + F_2 = 3$, $F_5 = F_4 + F_3 = 5$
- $\langle 0, 1 + F_0, F_0 + F_1, F_1 + F_2, F_2 + F_3, F_3 + F_4, \ldots \rangle$,
- $G(F) = 0 + (F_0 + 1)x + (F_0 + F_1)x^2 + (F_1 + F_2)x^3 + (F_2 + F_3)x^4 + (F_3 + F_4)x^5 + \ldots$

Izračunavanje zatvorene forme generatorne funkcije

- Fibonačijev niz: $F = \langle 0, 1, 1, 2, 3, 5, \ldots \rangle$
- $G(F) = 0 + 1 \cdot x + 1 \cdot x^2 + 2 \cdot x^3 + 3 \cdot x^4 + 5 \cdot x^5 + \ldots$

- $F_0 = 0,\ F_1 = 1,\ F_2 = F_1 + F_0 = 1,\ F_3 = F_2 + F_1 = 2,$
  $F_4 = F_3 + F_2 = 3,\ F_5 = F_4 + F_3 = 5$
- $\langle 0, 1 + F_0, F_0 + F_1, F_1 + F_2, F_2 + F_3, F_3 + F_4, \ldots \rangle,$

- $G(F) =$
  $0+(F_0+1)x+(F_0+F_1)x^2+(F_1+F_2)x^3+(F_2+F_3)x^4+(F_3+F_4)x^5+\ldots$

Izračunavanje zatvorene forme generatorne funkcije

$$G(F) = 0+(F_0+1)x+(F_0+F_1)x^2+(F_1+F_2)x^3+(F_2+F_3)x^4+(F_3+F_4)x^5+\ldots$$

se prikazuje pomoću jednostavnijih generatorskih funkcija za koje su već određene zatvorene forme:

$$\begin{array}{cccccccc}
 & \langle & 0, & 1, & 0, & 0, & \ldots\rangle & x \\
 & \langle & 0, & F_0, & F_1, & F_2, & \ldots\rangle & x\cdot G(F) \\
+ & \langle & 0, & 0, & F_0, & F_1, & \ldots\rangle & x^2\cdot G(F) \\
\hline
 & \langle & 0, & 1+F_0, & F_0+F_1, & F_1+F_2, & \ldots\rangle & x+x\cdot G(F)+x^2\cdot G(F)
\end{array}$$

Izračunavanje zatvorene forme generatorne funkcije

- $G(F) = x + x \cdot G(F) + x^2 \cdot G(F)$
- zatvorena forma generatorne funkcije Fibonačijevog niza brojeva je *racionalna funkcija*

$$G(F) = \frac{x}{1 - x - x^2}$$

Generatorne funkcije

Theorem

Neka su dati niz $\{a_n\}_n$ i konstante $c_1, \ldots c_k$. Tada je ekvivalentno:

1. *Niz $\{a_n\}_n$ je rešenje linearne rekuretne relacije,*

$$a_n = \sum_{i=1}^{k} c_i \cdot a_{n-i}.$$

2. *Zatvorena forma generatorne funkcije niza $\{a_n\}_n$ je racionalna funkcija oblika*

$$G(a) = \frac{g(x)}{1 - \sum_{i=1}^{k} c_i \cdot x^i}$$

gde je $g(x)$ polinom stepena najviše $k-1$.

Generatorne funkcije i prebrojavanje

- određivanje zatvorenih formi generatornih funkcija ima primena u prebrojavanju, jer polazeći od neke zatvorene forme mogu se odrediti koeficijento odgovarajućih stepenih redova (generatornih funkcija), odnosno članovi njima odgovarajućih nizova
- prebrojavanje načina izbora elemenata nekog skupa, koeficijent uz stepen x^k odgovara broju načina na koji je moguće birati k elemenata
- jednočlani skup $\{a_1\}$
- generatorna funkcija za izbor k elemenata iz tog skupa je $1 + x$:
  - 1 način za izbor 0 elemenata skupa
  - 1 način za izbor 1 elementa skupa
  - 0 načina za izbor više od jednog elementa

Generatorne funkcije i prebrojavanje

- određivanje zatvorenih formi generatornih funkcija ima primena u prebrojavanju, jer polazeći od neke zatvorene forme mogu se odrediti koeficijento odgovarajućih stepenih redova (generatornih funkcija), odnosno članovi njima odgovarajućih nizova
- prebrojavanje načina izbora elemenata nekog skupa, koeficijent uz stepen x^k odgovara broju načina na koji je moguće birati k elemenata
- jednočlani skup $\{a_1\}$
- generatorna funkcija za izbor k elemenata iz tog skupa je $1 + x$:
  - 1 način za izbor 0 elemenata skupa
  - 1 način za izbor 1 elementa skupa
  - 0 načina za izbor više od jednog elementa

Generatorne funkcije i prebrojavanje

- $\{a_1, a_2, a_3\}$
  $(1 + a_1x)(1 + a_2x)(1 + a_3x) =$
  $1 + (a_1 + a_2 + a_3)x + (a_1a_2 + a_1a_3 + a_2a_3)x^2 + (a_1a_2a_3)x^3$
- koeficijent uz x zapis svih mogućih 1-kombinacija,
- koeficijent uz x^2 zapis svih mogućih 2-kombinacija i
- koeficijent uz x^3 zapis svih mogućih 3-kombinacija
- Brojevi 1, 2 i 3-kombinacija: $\binom{3}{1} = 3$, $\binom{3}{2} = 3$ i $\binom{3}{3} = 1$
- brojanje sabiraka uz stepen x^i,
- ili zamenom $a_1 = a_2 = a_3 = 1$: $(1 + x)(1 + x)(1 + x)$
- $(1 + x)^3$ zatvorena forma generatorne funkcije brojanja kombinacija 3 objekta

Generatorne funkcije i prebrojavanje

- $\{a_1, a_2, a_3\}$
  $(1 + a_1x)(1 + a_2x)(1 + a_3x) =$
  $1 + (a_1 + a_2 + a_3)x + (a_1a_2 + a_1a_3 + a_2a_3)x^2 + (a_1a_2a_3)x^3$
- koeficijent uz x zapis svih mogućih 1-kombinacija,
- koeficijent uz x^2 zapis svih mogućih 2-kombinacija i
- koeficijent uz x^3 zapis svih mogućih 3-kombinacija
- Brojevi 1, 2 i 3-kombinacija: $\binom{3}{1} = 3$, $\binom{3}{2} = 3$ i $\binom{3}{3} = 1$
- brojanje sabiraka uz stepen x^i,
- ili zamenom $a_1 = a_2 = a_3 = 1$: $(1 + x)(1 + x)(1 + x)$
- $(1 + x)^3$ zatvorena forma generatorne funkcije brojanja kombinacija 3 objekta

Generatorne funkcije i prebrojavanje

- $\{a_1, a_2, a_3\}$
  $(1 + a_1x)(1 + a_2x)(1 + a_3x) =$
  $1 + (a_1 + a_2 + a_3)x + (a_1a_2 + a_1a_3 + a_2a_3)x^2 + (a_1a_2a_3)x^3$
- koeficijent uz x zapis svih mogućih 1-kombinacija,
- koeficijent uz x^2 zapis svih mogućih 2-kombinacija i
- koeficijent uz x^3 zapis svih mogućih 3-kombinacija
- Brojevi 1, 2 i 3-kombinacija: $\binom{3}{1} = 3$, $\binom{3}{2} = 3$ i $\binom{3}{3} = 1$
- brojanje sabiraka uz stepen x^i,
- ili zamenom $a_1 = a_2 = a_3 = 1$: $(1 + x)(1 + x)(1 + x)$
- $(1 + x)^3$ zatvorena forma generatorne funkcije brojanja kombinacija 3 objekta

Generatorne funkcije i prebrojavanje

- $(1+x)^k$ je zatvorena forma generatorne funkcije brojanja kombinacija bez ponavljanja skupa sa k elemenata
- $G(a) = \binom{k}{0} + \binom{k}{1}x + \cdots + \binom{k}{k}x^k$
- odgovarajući niz je

$$a = \left\langle \binom{k}{0}, \binom{k}{1}, \ldots, \binom{k}{k}, 0, 0, \ldots \right\rangle$$

- koeficijent $\binom{k}{i}$ uz x^i u $G(a)$ je jednak broju i-kombinacija bez ponavljanja skupa od k elemenata.

Generatorne funkcije i prebrojavanje

Generatorna funkcija za kombinacije sa ponavljanjem:

- za jednočlani skup $\{a_1\}$ je $G(a) = 1 + x + x^2 + \ldots = \frac{1}{1-x}$, jer postoji samo jedan način za izbor k elemenata iz tog skupa
- zatvorena forma generatorne funkcije broja i-kombinacija sa ponavljanjem od n objekata (kojih imamo na raspolaganju neograničeni broj):

$$\frac{1}{(1-x)^n} = \prod_{i=1}^{n} \frac{1}{1-x}$$

- gde je $\frac{1}{1-x}$ zatvorena forma generatorne funkcije kombinacija sa ponavljanjem za 1 objekt.

Generatorne funkcije i prebrojavanje

Generatorna funkcija za kombinacije sa ponavljanjem:

- za jednočlani skup $\{a_1\}$ je $G(a) = 1 + x + x^2 + \ldots = \frac{1}{1-x}$, jer postoji samo jedan način za izbor k elemenata iz tog skupa
- zatvorena forma generatorne funkcije broja i-kombinacija sa ponavljanjem od n objekata (kojih imamo na raspolaganju neograničeni broj):

$$\frac{1}{(1-x)^n} = \prod_{i=1}^{n} \frac{1}{1-x}$$

- gde je $\frac{1}{1-x}$ zatvorena forma generatorne funkcije kombinacija sa ponavljanjem za 1 objekt.

Generatorne funkcije i prebrojavanje

Generatorna funkcija za kombinacije sa ponavljanjem:

- za jednočlani skup $\{a_1\}$ je $G(a) = 1 + x + x^2 + \ldots = \frac{1}{1-x}$, jer postoji samo jedan način za izbor k elemenata iz tog skupa
- zatvorena forma generatorne funkcije broja i-kombinacija sa ponavljanjem od n objekata (kojih imamo na raspolaganju neograničeni broj):

$$\frac{1}{(1-x)^n} = \prod_{i=1}^{n} \frac{1}{1-x}$$

- gde je $\frac{1}{1-x}$ zatvorena forma generatorne funkcije kombinacija sa ponavljanjem za 1 objekt.

Generatorne funkcije i prebrojavanje

Pravilo konvolucije:
Neka su $G(a)$ i $G(b)$ generatorne funkcije nizova $\{a_n\}_n$ i $\{b_n\}_n$ koji predstavljaju broj kombinacija elemenata skupa A, odnosno B i neka je $A \cap B = \emptyset$. Tada je

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

generatorna funkcija niza $\{c_n\}_n$ koji predstavlja broj kombinacija elemenata skupa $A \cup B$.

Nije preciziran tip kombinacija: sa ili bez ponavljanja.

Generatorne funkcije i prebrojavanje

Pravilo konvolucije:
Neka su $G(a)$ i $G(b)$ generatorne funkcije nizova $\{a_n\}_n$ i $\{b_n\}_n$ koji predstavljaju broj kombinacija elemenata skupa A, odnosno B i neka je $A \cap B = \emptyset$. Tada je

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

generatorna funkcija niza $\{c_n\}_n$ koji predstavlja broj kombinacija elemenata skupa $A \cup B$.

Nije preciziran tip kombinacija: sa ili bez ponavljanja.

Generatorne funkcije i prebrojavanje

Example

- majica se prodaje u tri boje: plavoj, sivoj i beloj; kupac želi 3 komada: S i B do 1 komad, P do 3
- na koliko načina se ova kupovina može ostvariti?
- pravilo konvolucije

  $(1 + x + x^2 + x^3)(1 + x)(1 + x) = 1 + 3x + 4x^2 + 4x^3 + \ldots$
- prvi faktor: 0–3 plave majice, druga dva za 0 ili 1 sivu/belu majicu
- traženi broj kombinacija sa ponavljanjem je koeficijent uz x^3, jednak je 4 i odgovara sledećim kobinacijama: PPP, PPS, PPB, PBS.

Generatorne funkcije i prebrojavanje

Example

- majica se prodaje u tri boje: plavoj, sivoj i beloj; kupac želi 3 komada: S i B do 1 komad, P do 3
- na koliko načina se ova kupovina može ostvariti?
- pravilo konvolucije

  $(1 + x + x^2 + x^3)(1 + x)(1 + x) = 1 + 3x + 4x^2 + 4x^3 + \ldots$
- prvi faktor: 0–3 plave majice, druga dva za 0 ili 1 sivu/belu majicu
- traženi broj kombinacija sa ponavljanjem je koeficijent uz x^3, jednak je 4 i odgovara sledećim kobinacijama: PPP, PPS, PPB, PBS.

Generatorne funkcije i prebrojavanje

Example

- majica se prodaje u tri boje: plavoj, sivoj i beloj; kupac želi 3 komada: S i B do 1 komad, P do 3
- na koliko načina se ova kupovina može ostvariti?
- pravilo konvolucije

  $(1 + x + x^2 + x^3)(1 + x)(1 + x) = 1 + 3x + 4x^2 + 4x^3 + \ldots$
- prvi faktor: 0–3 plave majice, druga dva za 0 ili 1 sivu/belu majicu
- traženi broj kombinacija sa ponavljanjem je koeficijent uz x^3, jednak je 4 i odgovara sledećim kobinacijama: PPP, PPS, PPB, PBS.

Generatorne funkcije i prebrojavanje

Example

- na koliko načina se može spakovati n komada odeće ako:
  - broj majica mora biti paran,
  - broj košulja mora biti oblika $3k$,
  - broj džempera je najviše 2 i
  - broj šalova je najviše 1,
- kombinacije sa ponavljanjem jednočlanih skupova

Generatorne funkcije i prebrojavanje

Example

- na koliko načina se može spakovati n komada odeće ako:
  - broj majica mora biti paran,
  - broj košulja mora biti oblika $3k$,
  - broj džempera je najviše 2 i
  - broj šalova je najviše 1,
- kombinacije sa ponavljanjem jednočlanih skupova

Generatorne funkcije i prebrojavanje

Nastavak primera:

- Odgovarajući nizovi kombinacija jednočlanih skupova:
  - paran broj majica: $M = \langle 1, 0, 1, 0, \ldots \rangle$,
  - $3k$ košulja: $K = \langle 1, 0, 0, 1, 0, 0, 1 \ldots \rangle$,
  - 2 džempera: $D = \langle 1, 1, 1, 0, 0 \ldots \rangle$,
  - 0 ili 1 šalova: $S = \langle 1, 1, 0, 0 \ldots \rangle$
- zatvorene forme generatornih funkcija:
  - $1 + x^2 + x^4 + \ldots = \dfrac{1}{1 - x^2} = G(M)$,
  - $1 + x^3 + x^6 + \ldots = \dfrac{1}{1 - x^3} = G(K)$,
  - $1 + x + x^2 = \dfrac{1 - x^3}{1 - x} = G(D)$ i
  - $1 + x = G(S)$.

Generatorne funkcije i prebrojavanje

Nastavak primera:

- Odgovarajući nizovi kombinacija jednočlanih skupova:
  - paran broj majica: $M = \langle 1, 0, 1, 0, \ldots \rangle$,
  - $3k$ košulja: $K = \langle 1, 0, 0, 1, 0, 0, 1 \ldots \rangle$,
  - 2 džempera: $D = \langle 1, 1, 1, 0, 0 \ldots \rangle$,
  - 0 ili 1 šalova: $S = \langle 1, 1, 0, 0 \ldots \rangle$
- zatvorene forme generatornih funkcija:
  - $1 + x^2 + x^4 + \ldots = \dfrac{1}{1 - x^2} = G(M)$,
  - $1 + x^3 + x^6 + \ldots = \dfrac{1}{1 - x^3} = G(K)$,
  - $1 + x + x^2 = \dfrac{1 - x^3}{1 - x} = G(D)$ i
  - $1 + x = G(S)$.

Generatorne funkcije i prebrojavanje

Nastavak primera (2):

Prema pravilu konvolucije posmatramo proizvod zatvorenih formi generatornih funkcija:

$$\frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdot \frac{1-x^3}{1-x} \cdot (1+x) = \frac{1}{(1-x)^2}$$

- $\frac{1}{(1-x)^2}$ je zatvorena forma stepenog reda $\sum_{i=0}^{\infty}(i+1)x^i$
- koeficijent uz x^n uvek $n+1$
- broj načina pakovanja n komada odeće uz data ograničenja je uvek $n+1$.

Generatorne funkcije i prebrojavanje

Nastavak primera (2):

Prema pravilu konvolucije posmatramo proizvod zatvorenih formi generatornih funkcija:

$$\frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdot \frac{1-x^3}{1-x} \cdot (1+x) = \frac{1}{(1-x)^2}$$

- $\frac{1}{(1-x)^2}$ je zatvorena forma stepenog reda $\sum_{i=0}^{\infty}(i+1)x^i$
- koeficijent uz x^n uvek $n+1$
- broj načina pakovanja n komada odeće uz data ograničenja je uvek $n+1$.

Algebarske strukture

Definition

Algebarska struktura je uređena n-torka

$$\langle A, f_1, \ldots, f_k, c_1, \ldots, c_m \rangle$$

gde su:

- $n = 1 + k + m$,
- A neprazan skup, *domen*,
- $f_1, \ldots, f_k$ operacije domena A i
- $c_1, \ldots, c_m \in A$ konstante.

- grupe
- prsteni i polja i
- Bulove algebre

Grupe

Definition

Grupa je algebarska struktura $\langle A, \cdot, ^{-1}, 1\rangle$ za koju važi:

- $\cdot$ je binarna, a $^{-1}$ unarna operacija,
- zakon asocijativnosti, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- 1 je neutral za operaciju $\cdot$, $x \cdot 1 = x$, $1 \cdot x = x$ i
- $x \cdot x^{-1} = 1$ i $x^{-1} \cdot x = 1$.

Grupa je *komutativna* ili *Abelova* ako za nju važi:

- $x \cdot y = y \cdot x$.

Red grupe $G = \langle A, \cdot, ^{-1}, 1\rangle$, u oznaci $|G|$ je kardinalnost skupa A.

Évariste Galois, 1811 – 1832

Francuski matematičar. Prvi je upotrebio termin *grupa* za grupe permutacija. Postavio je temelje apstraktne algebre. Bio je radikalni republikanac. Preminuo je od posledica ranjavanja u dvoboju do koga je došlo pod sumnjivim okolnostima u vreme vladavine kralja Louis-Philippe I.

Niels Henrik Abel, 1802 – 1829

Norveški matematičar. U 19. godini je dokazao da u opštem slučaju ne postoji algebarsko rešenje (dobijeno od koeficijenata i racionalnih konstanti primenom zbira, razlike, proizvoda, količnika i korenovanja) za korene polinomijalnih jednačina stepena većeg od 4. Za potrebe tog dokaza je, nezavisno od Galois-a, razvio teoriju grupa. U znak sećanja 2002. godine je ustanovljena Abelova nagrada, kao matematičarski pandan Nobelovoj nagradi.

Grupe

Example

Primer komutativne grupe je struktura $\langle \mathbb{Z}, +, -, 0 \rangle$ u kojoj je sabiranje komutativno i asocijativno, 0 je neutral, a $-x$ je inverzni element za x.

Grupe

Example

Neka je A konačan neprazan skup simbola koji nazivamo azbuka. Reč je konačan niz simbola. Prazna reč, u oznaci ϵ, ne sadrži ni jedan simbol. A^* je skup svih reči azbuke A. Binarnom operacijom nadovezivanja od reči $x, y \in A^*$ dobija se:

$$x * y = xy.$$

Operacija $*$ je asocijativna. Prazna reč je neutral: $\epsilon * x = x * \epsilon = x$.
U opčtem slučaju $*$ nije komutativna (sem za jednočlanu azbuku). Na primer $a * b \neq b * a$. Takođe, sem prazne reči ϵ za koju je $\epsilon * \epsilon = \epsilon$, reči iz A^* nemaju inverzne elemente.
$\langle A^*, *, \epsilon \rangle$ nije grupa.

Grupe

Example

Neka je $A = \{1, 2, 3\}$. S_3 je skup svih 6 permutacija skupa A:

$$p_1 = \langle 1, 2, 3 \rangle \quad , \quad p_2 = \langle 1, 3, 2 \rangle,$$
$$p_3 = \langle 2, 1, 3 \rangle \quad , \quad p_4 = \langle 2, 3, 1 \rangle,$$
$$p_5 = \langle 3, 1, 2 \rangle \quad , \quad p_6 = \langle 3, 2, 1 \rangle.$$

Permutacije možemo shvatiti i kao bijektivne funkcije koje redom elemente 1, 2 i 3 preslikavaju u elemente navedene malopre.
Na primer $p_6(1) = 3$, a $p_2(3) = 2$.
Definišimo operaciju na skupu permutacija tako da je $p_i * p_j$ permutacija za koju važi:

$$p_i * p_j(x) = p_j(p_i(x)), \text{ za } x \in A.$$

Sada je $p_6 * p_2(1) = p_2(p_6(1)) = p_2(3) = 2$.

Grupe

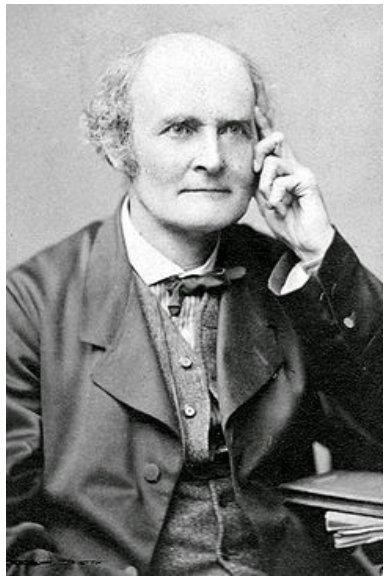
Nastavak primera (2):

Pošto su permutacije bijektivne funkcije, to su i njihove kompozicije. Tabela opisuje operaciju $*$ u S_3:

$*$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_2	p_5	p_1	p_3
p_5	p_5	p_3	p_6	p_1	p_4	p_2
p_6	p_6	p_4	p_5	p_2	p_3	p_1

Pemutacija p_1 je neutral operacije $*$. Kompozicija je asocijativna operacija. Svaka od permutacija ima i inverz u odnosu na $*$ ($p_6 * p_6 = p_1$). Struktura $\mathbb{S}_3 = \langle S_3, *, ^{-1}, p_1 \rangle$ je grupa koja nije komutativna. Za proizvoljno $n \in \mathbb{N}$, $n > 0$, $\mathbb{S}_n$ je grupa.

Arthur Cayley, 1821 – 1895



Engleski matematičar. Jedan od pionira moderne (čiste) matematike. Prvi je definisao koncept grupe kao algebarske strukture koja se sastoji od skupa i binarne operacije koja zadovoljava odgovarajuće zakone. Dao je veliku podršku uključivanju žena u univerzitetsko obrazovanje.

Grupe

Theorem

U grupi $\langle A, \cdot, ^{-1}, 1\rangle$

1. *jednačina* $a \cdot x = b$ *ima jedinstveno rešenje* $x = a^{-1} \cdot b$ *i*
2. *jednačina* $y \cdot a = b$ *ima jedinstveno rešenje* $x = b \cdot a^{-1}$.

Proof.

(1) Pošto je reč o grupi, za a postoji jedinstveni inverz a^{-1}. Za $x = a^{-1} \cdot b$ tada važi $a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = b$, pa je $a^{-1} \cdot b$ jedno rešenje polazne jednačine.
Ako su x_1 i x_2 dva rešenja polazne jednačine, tada važi $a \cdot x_1 = b$ i $a \cdot x_2 = b$, pa je $a \cdot x_1 = a \cdot x_2$. Tada je i $a^{-1} \cdot a \cdot x_1 = a^{-1} \cdot a \cdot x_2$, odnosno $x_1 = x_2$, odakle sledi jedinstvenost rešenja. □

Grupe

Corollary

U Kejlijevoj tabeli koja odgovara operaciji grupe u svakom redu, odnosno u svakoj koloni, svaki od elemenata grupe se pojavljuje tačno jednom.

$\cdot$	$\ldots$	c	$\ldots$
$\vdots$		$\vdots$	
a	$\ldots$	b	$\ldots$
$\vdots$		$\vdots$	

b se pojavljuje u redu u kome je a u onoj koloni u čijem zaglavlju se nalazi c ako i samo ako je c rešenje jednačine $a \cdot x = b$. Rešenje jednačine je jedinstveno, b se može u redu u kome je a javiti samo jednom, u koloni koja odgovara jedinstvenom rešenju.
Utvrđivanja da neka algebarska struktura nije grupa: ako se u nekom redu (koloni) bar jedan element javlja bar dva puta. Obrat ne važi.

Korektivni kodovi

Prilikom prenosa podataka (binarnih reči), dolazi do grešaka zbog:

- nepouzdanosti samog kanala preko koga se prenos vrši i
- uticaja spoljnih izvora, takozvanog šuma.

Pretpostavke:

- greške prenosa su: prelazak 0 u 1, ili 1 u 0,
- obe konverzije su podjednako veovatne,
- pogreške na pojedinačnim bitovima su međusobno nezavisne i
- podjednako su verovatne greške na svim bitovima.

Poslednje dve pretpostavke znače da je verovatnije da se dogodi manje, nego više, grešaka, pa je najverovatniji broj grešaka 1.

Korektivni kodovi

Zadaci:

- otkrivanje da je došlo do greške, tj. *detekcija*, i
- ispravljanje otkrivene greške, tj. *korekcija*.

Korektivni kodovi

Oznake:

- B^n - skup binarnih reči dužine n
- $B^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
- *težina* binarne reči a, $w(a)$, broj bitova jednakih 1 u a
- Sabiranje binarnih reči - *ekskluzivno ili*, $\veebar$, (sabiranja po modulu 2)

$\veebar$	0	1
0	0	1
1	1	0

Na primer:

$$\begin{array}{rr} & 1011001 \\ + & 1000111 \\ \hline & 0011110 \end{array}$$

Korektivni kodovi

Example

- prenos binarnih reči iz skupa B^3
- neka je poslata reč 010
- neka je primljena reč 011
- pošto je primljena reč u skupu reči koje se prenose, nije moguće detektovati grešku.

Korektivni kodovi

Example

- prenos binarnih reči iz skupa $\{001, 010, 100, 111\}$
- neka je primljena reč 011, detektuje se greška
- na osnovu pretpostavke da je najverovatnija greška na samo jednom bitu, kandidati za reč koja je mogla biti poslata: 001, 010 i 111
- korekciju je nemoguće izvesti

Korektivni kodovi

- neophodna osobina koju komunikacioni sistem treba da poseduje: da bi se ostvarila detekcija greške, nekorektno preneta reč ne sme pripadati skupu reči koje se očekuju na prijemu,
- reči koje se šalju, odnosno, koje se očekuju na prijemu, moraju biti dovoljno *udaljene*, tj. različite, kako bi greška prilikom prenosa dovela do prijema reči koja ne pripada očekivanom skupu
- korekcija je teži problem nego detekcija greške i postoje situacije u kojima, iako je poznato da je došlo do greške prenosa, tu grešku nije moguće ispraviti.

Korektivni kodovi

Example

- prenos binarnih reči iz skupa $\{000, 111\}$
- primljena reč je 011
- detekcija greška je laka
- poštujući pretpostavku da je najverovatnija greška na samo jednom bitu, vršimo korekciju zaključujući da je poslata reč 111
- ako je došlo do 2 greške prilikom prenosa reči 000, a primljena reč je 011, na osnovu pretpostavke o verovatnoći broja grešaka, korekcija će biti nekorektna

Korektivni kodovi

Definition

Hamingovo rastojanje binarnih reči a i b dužine n, u oznaci $d(a, b)$ je broj bitova na kojima se a i b razlikuju.

$$d(a, b) = w(a + b)$$

gde je $+$ operacija sabiranja reči, a $w()$ je težina binarne reči.

Korektivni kodovi

Example

Reči $x = 1011001$ i $y = 1000111$ se razllikuju na 4 mesta, pa je $d(x, y) = 4$. Analogno, pošto je

$$\begin{array}{rr} & 1011001 \\ + & 1000111 \\ & 0011110 \end{array}$$

i $w(0011110) = 4$, ponovo dobijamo $d(x, y) = 4$.

(m, n)-blok kodiranje

(m, n)-*blok kodiranje*:

- primenjuje se u realnim komunikacionim sistemima
- binarne reči se kodiraju pre prenosa dodavanjem izvesnog broja bitova koji kasnije olakšavaju detekciju i korekciju grešaka
- prenose se binarne reči čijih m bitova sadrže informacije, a preostalih r bitova se koriste prilikom detekcije i korekcije grešaka
- $n = m + r$
- kodiranje se vrši funkcijom:

$$E : B^m \mapsto B^n$$

(m, n)-blok kodiranje

- *Kodne reči* su elementi slike funkcije E, $Im(E)$
- E mora biti injektivna, tj. različite reči moraju imati različite kodove, kako bi bilo moguće sprovesti obrnuti proces
- dekodiranje

$$D : B^n \mapsto B^m \cup \{e\}$$

- e označava grešku
- ako je primljena reč $y \in B^n \setminus Im(E)$, detektuje se greška
- ako je moguća korekcija, onda je $D(y) = D(x)$, gde je x kodna reč koja je najbliža reči y
- ako ne postoji jedinstvena najbliža reč, javlja se greška, $D(y) = e$

(m, n)-blok kodiranje

Example

Kodirajuća funkcija za proveru parnosti (odnosno neparnosti) je oblika

$$E : B^m \mapsto B^{m+1}$$

za koju je $m+1$. bit slike takav da $E(x)$ ima paran (odnosno neparan) broj bitova 1.

(m, n)-blok kodiranje

- (m, n)-blok kodiranje je *sistematsko* ako su za svako $x \in B^m$, prvih m bitova u $E(x)$ jednaki x
- kodiranje je *k-detektibilno*: moguće je detektovati bilo koju kombinaciju od k ili manje grešaka
- kodiranje je *k-korektibilno*: moguće je korigovati bilo koju kombinaciju od k ili manje grešaka
- *Minimalna distanca* za neko kodiranje je

$$\min\{d(x, y) : x, y \in Im(E)\}$$

(m, n)-blok kodiranje

Theorem

Kodiranje je:

- *k-detektibilno ako i samo ako je minimalna distanca kodiranje bar $k + 1$ i*
- *k-korektibilno ako i samo ako je minimalna distanca kodiranje bar $2k + 1$.*

(m, n)-blok kodiranje

Example

Pošto kodiranje $E : B^2 \mapsto B^6$, definisano sa:

- $E(00) = 001000$,
- $E(01) = 010100$,
- $E(10) = 100010$ i
- $E(11) = 110001$,

kao minimalnu distancu ima 3, to je ono 2-detektibilno i 1-korektibilno.

(m, n)-blok kodiranje

Example

Pošto kodiranje $E : B^2 \mapsto B^6$, definisano sa:

- $E(00) = 001000$,
- $E(01) = 010100$,
- $E(10) = 100010$ i
- $E(11) = 110001$,

kao minimalnu distancu ima 3, to je ono 2-detektibilno i 1-korektibilno.

(m, n)-blok kodiranje

- funkcija kodiranja $E : B^m \mapsto B^n$ pri kojoj se na reč koja se kodira nadovezuju bitovi za proveru, pogodno se prikazuje *generatornom matricom* G koja sadrži samo 0 i 1
- kodiranje se obavlja matričnim množenjem u kome se operacije sabiranja i množenja vrše u binarnom brojnom sistemu

(m, n)-blok kodiranje

Example

Neka je kodiranje $E : B^3 \mapsto B^6$ definisano sa $E(x) = x \times G$, gde je generatorna matrica:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{3\times 6}$$

Reč oblika $x_1x_2x_3$ se kodira na sledeći način:

$$\begin{aligned} E(x_1x_2x_3) &= \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} x_1 & x_2 & x_3 & x_1 + x_2 & x_2 + x_3 & x_1 + x_3 \end{bmatrix} \end{aligned}$$

$E(011) = 011101.$

(m, n)-blok kodiranje

Example

Neka je kodiranje $E : B^3 \mapsto B^6$ definisano sa $E(x) = x \times G$, gde je generatorna matrica:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{3\times 6}$$

Reč oblika $x_1x_2x_3$ se kodira na sledeći način:

$$\begin{aligned} E(x_1x_2x_3) &= \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} x_1 & x_2 & x_3 & x_1 + x_2 & x_2 + x_3 & x_1 + x_3 \end{bmatrix} \end{aligned}$$

$E(011) = 011101.$

(m, n)-blok kodiranje

Nastavak primera (1):

- E je sistematsko kodiranje, prva tri bita kodne reči su zapravo reč koja se kodira, jer je levi blok generatorne matrice G jedinična matrica $I_{3\times 3}$
- preostala 3 bita služe za proveru parnosti parova bita originalne reči
- svaka greška pri prenosu jednog bita se jednoznačno određuje vrednostima kodne reči
- greška u prenosu na jednom od prva tri bita vidi se na dva od tri poslednja bita: $x_1 + x_2$, $x_2 + x_3$ i $x_1 + x_3$
- greška na bitu 2 će biti uočena na bitovima 4 i 5: $x_1 + x_2$, $x_2 + x_3$
- ako se greška pojavi na bitu 4, $x_1 + x_2$, ona će biti vidljiva samo tu

(m, n)-blok kodiranje

Nastavak primera (2):

- prenosom 011 dobijena je reč $w_1 w_2 w_3 w_4 w_5 w_6 = 001101$,
- $w_1 + w_2 = 0 \neq w_4$ i $w_2 + w_3 = 1 \neq w_5$,
- neslaganje se javlja na bitovima 4 i 5, pa je bit w_2 loše prenet
- prenosom 011 dobijena je reč $w_1 w_2 w_3 w_4 w_5 w_6 = 011001$,
- $w_1 + w_2 = 1 \neq w_4$, $w_2 + w_3 = 0 = w_5$ i $w_1 + w_3 = 1 = w_6$,
- bit w_4 je loše prenet.

(m, n)-blok kodiranje

Nastavak primera (3):

Generatorna matrica G je oblika $[IF]$, gde je I jedinična matrica $I_{3\times 3}$

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{3\times 6}$$

- $H = \left[F^T I\right]_{3\times 6}$ je *matrice provere parnosti*
- Za H i svaku kodnu reč $w \in B^6$ važi da je

$$H \times w^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

gde su F^T i w^T transponovane matrice.

(m, n)-blok kodiranje

Theorem

Neka je generatorna matrica G oblika $[I_{m\times m}F_{m\times r}]_{m\times n}$, gde je $n = m + r$, i neka je matrica provere parnosti $H = \left[F^T_{m\times r}I_{r\times r}\right]_{r\times n}$.
Ako je funkcija kodiranja $E : B^m \mapsto B^n$ definisana sa $E(x) = x \times G$, onda za svaku kodnu reč $w \in B^n$ važi:

$$H \times w^T = 0_{r\times 1}$$

Theorem

Ako je funkcija kodiranja $E : B^m \mapsto B^n$ definisana sa $E(x) = x \times G$, gde je G generatorna matrica, onda skup kodnih reči $Im(E) \subset B^n$ čini grupu u odnosu na sabiranje reči koje se realizuje primenom logičke operacije ekskluzivno ili na bitovima reči.

(m, n)-blok kodiranje

- kodiranje za koje $Im(E)$ u odnosu na operaciju sabiranja binarnih reči čini grupu, naziva se *grupovno kodiranje*
- za pronalaženje minimalne distance proizvoljnog kodiranja moraju uporediti svi parovi reči
- ovde je to lakše:

Theorem

Minimalna distanca grupovnog kodiranja je minimalna težina kodnih reči kod kojih svi bitovi nisu 0.

(m, n)-blok kodiranje

Za ovakva kodiranja:

- prilikom detekcije grešaka proverava se proizvod $H \times w^T$
- ako je dobijena 0-matricu, razumno je pretpostaviti da je w korektno preneta, a dekodiranje se sprovodi izdvajanjem početnih bitova reči w
- ako je $H \times w^T \neq 0$, došlo je do greške prenosa.

(m, n)-blok kodiranje

Pozicija greške se određuje na sledeći način:

- neka je w_p kodna reč čijim prenosom je dobijena reč w (w_p i w se razlikuju samo na jednom bitu, recimo na poziciji i)
- tada je $w_p = w + e_i$, gde je e_i binarna reč koja se sastoji od bitova 0 i samo jednog bita 1, na poziciji i,
- $H \times w^T = H \times (w_p + e_i)^T = H \times (w_p^T + e_i^T) = (H \times w_p^T) + (H \times e_i^T) = 0 + H \times e_i^T = H \times e_i^T$
- $H \times e_i^T = h_i$, gde je h_i i-ta kolona matrice H, a i pozicija bita na kome se pojavila greška.
- poređenjem $H \times w^T$ sa kolonama matrice H detektuje se pozicija greške koja se potom lako koriguje promenom vrednosti odgovarajućeg bita u reči w
- Ako $H \times w^T \neq 0$, ali $H \times w^T$ nije jednako ni jednoj od kolona matrice H, pojavilo se više od jedne greške (za pouzdano korigovanje postoje složenije metode)

(m, n)-blok kodiranje

Pozicija greške se određuje na sledeći način:

- neka je w_p kodna reč čijim prenosom je dobijena reč w (w_p i w se razlikuju samo na jednom bitu, recimo na poziciji i)
- tada je $w_p = w + e_i$, gde je e_i binarna reč koja se sastoji od bitova 0 i samo jednog bita 1, na poziciji i,
- $H \times w^T = H \times (w_p + e_i)^T = H \times (w_p^T + e_i^T) = (H \times w_p^T) + (H \times e_i^T) = 0 + H \times e_i^T = H \times e_i^T$
- $H \times e_i^T = h_i$, gde je h_i i-ta kolona matrice H, a i pozicija bita na kome se pojavila greška.
- poređenjem $H \times w^T$ sa kolonama matrice H detektuje se pozicija greške koja se potom lako koriguje promenom vrednosti odgovarajućeg bita u reči w
- Ako $H \times w^T \neq 0$, ali $H \times w^T$ nije jednako ni jednoj od kolona matrice H, pojavilo se više od jedne greške (za pouzdano korigovanje postoje složenije metode)

(m, n)-blok kodiranje

Example

Neka je kodiranje $E : B^3 \mapsto B^6$ definisano sa $E(x) = x \times G$:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{3\times 6}$$

Neka je prenosom dobijeno $w = 100100$. Tada je:

$$H \times w^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

(m, n)-blok kodiranje

Nastavak primera:
Rezultat nije 0-matrica, pa w nije kodna reč. Pošto se

$$H \times w^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

poklapa sa kolonom h_6 matrice H, to je greška nastala u prenosu poslednjeg bita reči, pa je poslata reč bila

$$w_p = 100101$$

Prsteni i polja

Definition

Prsten je algebarska struktura $\langle A, +, \cdot, -, 0, 1\rangle$ za koju važi:

- $+$ i $\cdot$ su binarne operacije, a $-$ je unarna operacija,
- $\langle A, +, -, 0\rangle$ je komutativna grupa,
- zakon asocijativnosti, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- zakon distributivnosti, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ i $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Element a prstena koji je različit od 0 je *levi (desni) delilac nule* ako postoji ne-nulti element prstena b tako da je $a \cdot b = 0$ $(b \cdot a = 0)$.

Prsteni i polja

Definition

Prsten je *komutativan sa jedinicom* ako važi:

- $x \cdot y = y \cdot x$ i
- $x \cdot 1 = x$.

Komutativni prsten sa jedinicom je *polje* ako važi:

- za svaki $x \in A$, ako je $x \neq 0$, onda postoji njegov inverz $x^{-1} \in A$, tako da je $x \cdot x^{-1} = 1$.

Kongruencija po modulu

- $n \in \mathbb{N}$, $n > 0$
- relacija *kongruencije po modulu* n, u oznaci $x \equiv_n y$ ili $x \equiv y \pmod{n}$, na skupu celih brojeva $\mathbb{Z}$:

$$x \equiv_n y \text{ ako i samo ako } x - y = k \cdot n, \text{ za neki } k \in \mathbb{Z}.$$

- relacija ekvivalencije

Example

- Pretpostavimo da je trenutno ponoć
- Koliko sati će biti za 50 sati?
- Vreme se broji u 24-voro satnim ciklusima, posmatramo relaciju $\equiv_{24}$
- Pošto je $50 \equiv_{24} 2$, odgovor je: biće 2 sata ujutro.

Kongruencija po modulu

- $n \in \mathbb{N}$, $n > 0$
- relacija *kongruencije po modulu* n, u oznaci $x \equiv_n y$ ili $x \equiv y \pmod{n}$, na skupu celih brojeva $\mathbb{Z}$:

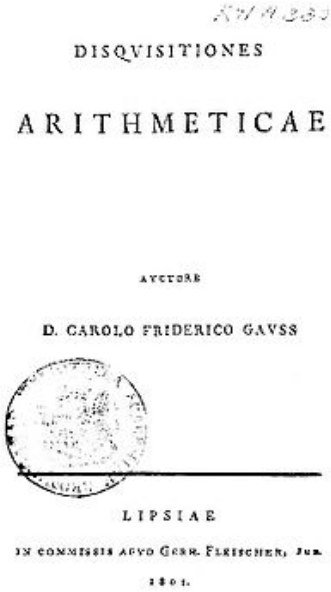
$$x \equiv_n y \text{ ako i samo ako } x - y = k \cdot n, \text{ za neki } k \in \mathbb{Z}.$$

- relacija ekvivalencije

Example

- Pretpostavimo da je trenutno ponoć
- Koliko sati će biti za 50 sati?
- Vreme se broji u 24-voro satnim ciklusima, posmatramo relaciju $\equiv_{24}$
- Pošto je $50 \equiv_{24} 2$, odgovor je: biće 2 sata ujutro.

Leonhard Euler 1707 – 1783, Johann Carl Friedrich Gauss, 1777 – 1855


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

Relaciju kongruencije su prvi proučavali Euler (levo) koji ju je eksplicitno uveo i Gauss (sredina) koji je u knjizi "Disquisitiones Arithmeticae" iz 1801. godine (desno) uveo simbol $\equiv$ za kongruenciju i precizno predstavio modularnu aritmetiku. Eulerov rad iz 1736. godine je prvi koji se bavi onim što se danas naziva teorija grafova.

Kongruencija po modulu

Alternativna karakterizacija kongruencija po modulu.

Theorem

Za $x, y \in \mathbb{Z}$ je $x \equiv_n y$ ako i samo ako x i y imaju iste ostatke pri deljenju sa n.

Proof.

($\Leftarrow$) Ako važi $x = k_x n + r$ i $y = k_y n + r$, onda je $x - y = (k_x - k_y)n$, pa je $x \equiv_n y$.

($\Rightarrow$) Neka je $x \equiv_n y$, $x = k_x n + r_x$ i $y = k_y n + r_y$. Tada je $x - y$ deljivo sa n, pa je i

$$r_x - r_y = (x - y) + (k_y - k_x)n$$

deljivo sa n. Pošto su r_x, $r_y \in \{0, \ldots n-1\}$, sledi da je $r_x - r_y = 0$, tj. $r_x = r_y$.

Kongruencija po modulu

Alternativna karakterizacija kongruencija po modulu.

Theorem

Za $x, y \in \mathbb{Z}$ je $x \equiv_n y$ ako i samo ako x i y imaju iste ostatke pri deljenju sa n.

Proof.

($\Leftarrow$) Ako važi $x = k_x n + r$ i $y = k_y n + r$, onda je $x - y = (k_x - k_y)n$, pa je $x \equiv_n y$.

($\Rightarrow$) Neka je $x \equiv_n y$, $x = k_x n + r_x$ i $y = k_y n + r_y$. Tada je $x - y$ deljivo sa n, pa je i

$$r_x - r_y = (x - y) + (k_y - k_x)n$$

deljivo sa n. Pošto su r_x, $r_y \in \{0, \ldots n-1\}$, sledi da je $r_x - r_y = 0$, tj. $r_x = r_y$.

Kongruencija po modulu

Example

- $17 - 5 = 12$ i 6 deli 12, važi $17 \equiv_6 5$
- isto: $17 = 2 \cdot 6 + 5$ i $5 = 0 \cdot 6 + 5$.

Kongruencija po modulu

Theorem

Za $x, x', y, y' \in \mathbb{Z}$, *ako je* $x \equiv_n x'$ *i* $y \equiv_n y'$ *onda važi:*

1. $x + y \equiv_n x' + y'$,
2. $x - y \equiv_n x' - y'$,
3. $x \cdot y \equiv_n x' \cdot y'$ *i*
4. $x^k \equiv_n x'^k$ *za* $k \in \mathbb{N}$.

Proof.

(1),(2) Pošto n deli i $x - x'$ i $y - y'$ tada je desna strana jednakosti:

$$(x + y) - (x' + y') = (x - x') + (y - y')$$

zapravo zbir dva broja deljiva sa n, pa je $x + y \equiv_n x' + y'$ i dobija se tvrđenje (1). □

Kongruencija po modulu

Nastavak dokaza:

Takođe je

$$(x-y)-(x'-y')=(x-x')+(y'-y)$$

i uz isto obrazloženje sledi tvrđenje (2).
(3) Slično,

$$(x\cdot y)-(x'\cdot y')=(x\cdot y)-(x\cdot y')+(x\cdot y')-(x'\cdot y')=x(y-y')+y'(x-x')$$

i poslednji zbir čine dva sabirka deljiva sa n, pa je to slučaj i sa $(x\cdot y)-(x'\cdot y')$, odnosno važi $x\cdot y\equiv_n x'\cdot y'$.
(4) Direktna posledica od (3) za $x=y$ i $x'=y'$.

Kongruencija po modulu

Na osnovu prethodne teoreme:

- ako u nekom aritmetičkom izrazu koji uključuje cele brojeve, sabiranje, oduzimanje i množenje (ali ne i deljenje!) zamenimo brojeve koji su međusobno kongruenti
- rezultati polaznog i izraza dobijenog zamenom (možda neće biti jednaki, ali) će biti kongruentni
- na ovaj način se može efikasnije računati

Kongruencija po modulu

Example

Neka je:

- $n = 113 \cdot (167 + 484) + 192 \cdot 145$

i neka treba pronaći kojoj klasi ekvivalencije relacije $\equiv_{21}$ pripada n. Direktan način je izračunati $n = 113 \cdot (167 + 484) + 192 \cdot 145 = 101403$, i nakon delenja sa 21 dobiti ostatak 15, tako da je $n \equiv_{21} 15$. Međutim, problem će efikasnije biti rešen ako se uoči da je:

- $113 \equiv_{21} 8$, $167 \equiv_{21} 20$, $484 \equiv_{21} 1$, $192 \equiv_{21} 3$ i $145 \equiv_{21} 19$,

pa se odgovarajućom zamenom dobija izraz $8(20 + 1) + 3 \cdot 19$. Pošto je $8(20 + 1) \equiv_{21} 0$, izraz se redukuje na $3 \cdot 19 = 57$, pa kako se deljenjem 57 sa 21 dobija se ostatak 15, to je, prema očekivanju, $n \equiv_{21} 15$.

Kongruencija po modulu

Nastavak primera (1):

Čemu je kongruentno 9^{342}, u odnosu na relaciju $\equiv_{10}$:

- $9^2 \equiv_{10} 1$,
- $9^{342} = (9^2)^{171} \equiv_{10} 1^{171} \equiv_{10} 1$.

Kongruencija po modulu

Nastavak primera (2):

Čemu je kongruentno 5^8 u odnosu na relaciju $\equiv_{16}$:

- $5 \equiv_{16} 5$,
- $5^2 \equiv_{16} 25 \equiv_{16} 9$,
- $5^4 \equiv_{16} 5^2 \cdot 5^2 \equiv_{16} 9 \cdot 9 \equiv_{16} 81 \equiv_{16} 1$ i
- $5^8 \equiv_{16} 5^4 \cdot 5^4 \equiv_{16} 1 \cdot 1 \equiv_{16} 1$.

Kongruencija po modulu

Example

- $484 \equiv_{21} 1$
- $22 \equiv_{21} 1$
- $484/21$ nije ceo broj i ne važi da je:
- $484/21 \equiv_{21} 1/1$

Modularna aritmetika

Aritmetičke operacije na količničkom skupu $\mathbb{Z}_{/\equiv_n}$:

- $[i] + [j] = [i + j]$,
- $[i] - [j] = [i - j]$ i
- $[i] \cdot [j] = [i \cdot j]$.

Modularna aritmetika

Example

- $n = 4$, $\mathbb{Z}_{/\equiv_n} = \{[0], [1], [2], [3]\}$
- $[3] + [2] = [5]$
- $5 \equiv_4 1$
- $[3] + [2] = [1]$
- Slično, pošto je $[3] \cdot [2] = [6]$ i $6 \equiv_4 2$, onda je $[3] \cdot [2] = [2]$.

Modularna aritmetika

- $\mathbb{Z}_{/\equiv_n}$ se poistovećuje $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- $\langle \mathbb{Z}_n, +, \cdot, -, 0, 1 \rangle$ je komutativni prsten sa jedinicom
- Ako n nije prost broj, jasno je da uvek postoje prirodni brojevi x i y takvi da važi:
  - $1 < x < n$, $1 < y < n$ i
  - $x \cdot y = n$, odnosno $x \cdot y \equiv_n 0$.
- ako n nije prost broj, $\mathbb{Z}_n$ ima delioce nule
- $\langle \mathbb{Z}_n, +, \cdot, -, 0, 1 \rangle$ neće biti polje

- ako p jeste prost broj, $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$ jeste polje

Modularna aritmetika

- $\mathbb{Z}_{/\equiv_n}$ se poistovećuje $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
- $\langle \mathbb{Z}_n, +, \cdot, -, 0, 1 \rangle$ je komutativni prsten sa jedinicom
- Ako n nije prost broj, jasno je da uvek postoje prirodni brojevi x i y takvi da važi:
  - $1 < x < n$, $1 < y < n$ i
  - $x \cdot y = n$, odnosno $x \cdot y \equiv_n 0$.
- ako n nije prost broj, $\mathbb{Z}_n$ ima delioce nule
- $\langle \mathbb{Z}_n, +, \cdot, -, 0, 1 \rangle$ neće biti polje

- ako p jeste prost broj, $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$ jeste polje

Mala Fermaova teorema

Theorem

Ako su p prost broj i a prirodan broj, onda p deli $a^p - a$, odnosno

$$a^p - a = k \cdot p,$$

za neki ceo broj k.

Proof.

- ako je p prost broj i l prirodan broj, $0 < l < p$, onda je $p \mid \binom{p}{l}$
  - $\binom{p}{l} = \frac{p!}{l!(p-l)!}$, pa je $p! = \binom{p}{l} \cdot l! \cdot (p-l)!$.
- $p \mid p!$
- $p \nmid l!$, $p \nmid (p-l)!$, p prost broj, $l, p-l < p$
- sledi $p \mid \binom{p}{l}$

Mala Fermaova teorema

Theorem

Ako su p prost broj i a prirodan broj, onda p deli $a^p - a$, odnosno

$$a^p - a = k \cdot p,$$

za neki ceo broj k.

Proof.

- ako je p prost broj i l prirodan broj, $0 < l < p$, onda je $p \mid \binom{p}{l}$
  - $\binom{p}{l} = \frac{p!}{l!(p-l)!}$, pa je $p! = \binom{p}{l} \cdot l! \cdot (p-l)!$.
- $p \mid p!$
- $p \nmid l!$, $p \nmid (p-l)!$, p prost broj, $l, p-l < p$
- sledi $p \mid \binom{p}{l}$

Mala Fermaova teorema

Theorem

Ako su p prost broj i a prirodan broj, onda p deli $a^p - a$, odnosno

$$a^p - a = k \cdot p,$$

za neki ceo broj k.

Proof.

- ako je p prost broj i l prirodan broj, $0 < l < p$, onda je $p \mid \binom{p}{l}$
  - $\binom{p}{l} = \frac{p!}{l!(p-l)!}$, pa je $p! = \binom{p}{l} \cdot l! \cdot (p-l)!$.
- $p \mid p!$
- $p \nmid l!$, $p \nmid (p-l)!$, p prost broj, $l, p-l < p$
- sledi $p \mid \binom{p}{l}$

Mala Fermaova teorema

Theorem

Ako su p prost broj i a prirodan broj, onda p deli $a^p - a$, odnosno

$$a^p - a = k \cdot p,$$

za neki ceo broj k.

Proof.

- ako je p prost broj i l prirodan broj, $0 < l < p$, onda je $p \mid \binom{p}{l}$
  - $\binom{p}{l} = \frac{p!}{l!(p-l)!}$, pa je $p! = \binom{p}{l} \cdot l! \cdot (p-l)!$.
- $p \mid p!$
- $p \nmid l!$, $p \nmid (p-l)!$, p prost broj, $l, p-l < p$
- sledi $p \mid \binom{p}{l}$

Mala Fermaova teorema

Theorem

Ako su p prost broj i a prirodan broj, onda p deli $a^p - a$, odnosno

$$a^p - a = k \cdot p,$$

za neki ceo broj k.

Proof.

- ako je p prost broj i l prirodan broj, $0 < l < p$, onda je $p \mid \binom{p}{l}$
  - $\binom{p}{l} = \frac{p!}{l!(p-l)!}$, pa je $p! = \binom{p}{l} \cdot l! \cdot (p-l)!$.
- $p \mid p!$
- $p \nmid l!$, $p \nmid (p-l)!$, p prost broj, $l, p-l < p$
- sledi $p \mid \binom{p}{l}$

Mala Fermaova teorema

Theorem

Ako su p prost broj i a prirodan broj, onda p deli $a^p - a$, odnosno

$$a^p - a = k \cdot p,$$

za neki ceo broj k.

Proof.

- ako je p prost broj i l prirodan broj, $0 < l < p$, onda je $p \mid \binom{p}{l}$
  - $\binom{p}{l} = \frac{p!}{l!(p-l)!}$, pa je $p! = \binom{p}{l} \cdot l! \cdot (p-l)!$.
- $p \mid p!$
- $p \nmid l!$, $p \nmid (p-l)!$, p prost broj, $l, p-l < p$
- sledi $p \mid \binom{p}{l}$

Mala Fermaova teorema

Nastavak dokaza za $a^p - a = k \cdot p$, indukcijom po a:

- za $a = 0$, tvrđenje trivijalno važi
- $a = b + 1$, $p | b^{p-1} - 1$.
- $a^p - a = (b+1)^p - (b+1)$
  $= b^p + \left(\sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}\right) + 1 - b - 1$
  $= b(b^{p-1} - 1) + \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$
- $p | b^p - b = b(b^{p-1} - 1)$, $p | \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$, pa
- $p | a^p - a$

Mala Fermaova teorema

Nastavak dokaza za $a^p - a = k \cdot p$, indukcijom po a:

- za $a = 0$, tvrđenje trivijalno važi
- $a = b + 1$, $p | b^{p-1} - 1$.
- $a^p - a = (b+1)^p - (b+1)$
  $= b^p + \left(\sum_{l=1}^{p-1} \binom{p}{l} b^{p-l} \right) + 1 - b - 1$
  $= b(b^{p-1} - 1) + \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$
- $p | b^p - b = b(b^{p-1} - 1)$, $p | \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$, pa
- $p | a^p - a$

Mala Fermaova teorema

Nastavak dokaza za $a^p - a = k \cdot p$, indukcijom po a:

- za $a = 0$, tvrđenje trivijalno važi
- $a = b + 1$, $p | b^{p-1} - 1$.
- $a^p - a = (b+1)^p - (b+1)$
  $= b^p + \left(\sum_{l=1}^{p-1} \binom{p}{l} b^{p-l} \right) + 1 - b - 1$
  $= b(b^{p-1} - 1) + \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$
- $p | b^p - b = b(b^{p-1} - 1)$, $p | \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$, pa
- $p | a^p - a$

Mala Fermaova teorema

Nastavak dokaza za $a^p - a = k \cdot p$, indukcijom po a:

- za $a = 0$, tvrđenje trivijalno važi
- $a = b + 1$, $p | b^{p-1} - 1$.
- $a^p - a = (b+1)^p - (b+1)$
  $= b^p + \left(\sum_{l=1}^{p-1} \binom{p}{l} b^{p-l} \right) + 1 - b - 1$
  $= b(b^{p-1} - 1) + \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$
- $p | b^p - b = b(b^{p-1} - 1)$, $p | \sum_{l=1}^{p-1} \binom{p}{l} b^{p-l}$, pa
- $p | a^p - a$

Pierre de Fermat, 1601 (ili 1607/8) – 1665

Francuski advokat i pasionirani matematičar. Glavni rezultati: početni razvoj infinitezimalnog računa, teorija brojeva, verovatnoća itd. Najpoznatiji je po Fermaovoj poslednjoj (ili velikoj) teoremi zabeleženoj na margini Diofantove aritmetike u kojoj se tvrdi da ne postoje ne-nulti prirodni brojevi a, b i c koji za $n > 2$ zadovoljavaju jednačinu $a^n + b^n = c^n$. Dokaz teoreme je tek 1995. godine dao A. Wiles.

Mala Fermaova teorema

- teorema se može formulisati za $0 < a < p$):
  - $a^{p-1} - 1 = k \cdot p$,
  - $a^{p-1} \equiv_p 1$
  - $a \cdot a^{p-2} \equiv_p 1$
- za prost broj p i a takav da je $0 < a < p$, $a^{-1} \equiv_p a^{p-2}$ je inverz od a u $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$
- $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$ jeste polje

Mala Fermaova teorema

- teorema se može formulisati za $0 < a < p$):
  - $a^{p-1} - 1 = k \cdot p$,
  - $a^{p-1} \equiv_p 1$
  - $a \cdot a^{p-2} \equiv_p 1$
- za prost broj p i a takav da je $0 < a < p$, $a^{-1} \equiv_p a^{p-2}$ je inverz od a u $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$
- $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$ jeste polje

Mala Fermaova teorema

- teorema se može formulisati za $0 < a < p$):
  - $a^{p-1} - 1 = k \cdot p$,
  - $a^{p-1} \equiv_p 1$
  - $a \cdot a^{p-2} \equiv_p 1$
- za prost broj p i a takav da je $0 < a < p$, $a^{-1} \equiv_p a^{p-2}$ je inverz od a u $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$
- $\langle \mathbb{Z}_p, +, \cdot, -, 0, 1 \rangle$ jeste polje

Modularna aritmetika

Example

Inverzni elementi za 2, 3 i 4 u $\mathbb{Z}_5$ su redom:

- pošto je $2^{5-2} = 2^3 = 8$ i $8 \equiv_5 3$, to je $2^{-1} \equiv_5 3$,
- pošto je $3^{5-2} = 3^3 = 27$ i $27 \equiv_5 2$, to je $3^{-1} \equiv_5 2$ i
- pošto je $4^{5-2} = 4^3 = 64$ i $64 \equiv_5 4$, to je $4^{-1} \equiv_5 4$.

Modularna aritmetika

Example

Sledećim tabelama

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

definisane su operacije $+$ i $\cdot$ u polju $\langle \mathbb{Z}_2, +, \cdot, -, 0, 1 \rangle$.
Za oduzimanje u ovom polju se lako vidi da je $x + y = x - y$.
U ovom slučaju je lako odrediti i rezultat deljenja: deljenje sa 0 nije definisano, dok deljenje 1 ne menja deljenik.

Modularna aritmetika

Problem deljenja se svodi na problem nalaženja inverza:

- neka se traži vrednost $c \equiv_p \frac{a}{b}$,
- ako možemo naći d takav da je $b \cdot d \equiv_p 1$, tj. $d = b^{-1}$, tada je $\frac{1}{b} \equiv_p d$ i
- $c \equiv_p \frac{a}{b} \equiv_p a \cdot \frac{1}{b} \equiv_p a \cdot d$.

Nalaženja inverza preko Male Fermaove teoreme nije efikasno.
Korsti se Euklidov algoritam za izračunavanje najvećeg zajedničkog delioca.

Modularna aritmetika

Problem deljenja se svodi na problem nalaženja inverza:

- neka se traži vrednost $c \equiv_p \frac{a}{b}$,
- ako možemo naći d takav da je $b \cdot d \equiv_p 1$, tj. $d = b^{-1}$, tada je $\frac{1}{b} \equiv_p d$ i
- $c \equiv_p \frac{a}{b} \equiv_p a \cdot \frac{1}{b} \equiv_p a \cdot d$.

Nalaženja inverza preko Male Fermaove teoreme nije efikasno.
Korsti se Euklidov algoritam za izračunavanje najvećeg zajedničkog delioca.

Euklidov algoritam za NZD

Definition

Najveći zajednički delilac prirodnih brojeva x i y (koji nisu oba jednaka 0), u oznaci $\gcd(x, y)$ je najveći prirodni broj koji deli i x i y.
Dva prirodna broja x i y su *uzajamno prosti* ako je $\gcd(x, y) = 1$.

Example

Lako se proverava da važi:

- $\gcd(1, 6) = 1$, $\gcd(2, 6) = 2$,
- $\gcd(4, 6) = 2$, $\gcd(5, 6) = 1$, $\gcd(6, 6) = 1$.

Euklidov algoritam za NZD

Theorem

Svaki prirodan broj veći od 1 *se na jedinstven način može prikazati kao proizvod nekih stepenova nekih prostih brojeva.*

- $x = p_1^{a_1} \cdots p_k^{a_k}$ (gde neki od a_i mogu biti jednaki 0) i
- $y = p_1^{b_1} \cdots p_k^{b_k}$ (gde neki od b_i mogu biti jednaki 0), pa je
- $\gcd(x, y) = p_1^{\min(a_1, b_1)} \cdots p_k^{\min(a_k, b_k)}$.

Euklidov algoritam za NZD

Example

Kako je:

- $24 = 2^3 \cdot 3$ i
- $36 = 2^2 \cdot 3^2$, to je
- $\gcd(24, 36) = 2^2 \cdot 3 = 12$.

Mana: potreba da se pronađu svi faktori brojeva čiji se najveći zajednički delilac traži.
Neefiksno.

Euklidov algoritam za NZD

Example

Kako je:

- $24 = 2^3 \cdot 3$ i
- $36 = 2^2 \cdot 3^2$, to je
- $\gcd(24, 36) = 2^2 \cdot 3 = 12$.

Mana: potreba da se pronađu svi faktori brojeva čiji se najveći zajednički delilac traži.
Neefiksno.

Euklidov algoritam za NZD

Algoritam, uz pretpostavke da važi $x, y > 0$ i $x < y$):

1. $y = q_0 \cdot x + r_0$, gde su $q_0, r_0 \in \mathbb{N}$, $r_0 < x$,
2. ako je $r_0 = 0$, $\gcd(x, y) = x$, inače
3. $i = 1$,
   $x = q_1 \cdot r_0 + r_1$,
   gde su $q_1, r_1 \in \mathbb{N}$, $r_1 < r_0$,
4. ako je $r_i = 0$, $\gcd(x, y) = r_{i-1}$, inače
5. $i = i + 1$,
   $r_{i-2} = q_i \cdot r_{i-1} + r_i$,
   $q_i, r_i \in \mathbb{N}$, $r_i < r_{i-1}$
   preći na korak (4).

Euklidov algoritam za NZD

Example

Izračunavanje $\gcd(91, 287)$:

- $287 = 3 \cdot 91 + 14$, pa je $r_0 = 14$
- $91 = 6 \cdot 14 + 7$, pa je $r_1 = 7$, $i = 1$
- $i = 2$, $14 = 2 \cdot 7$, pa je $r_2 = 0$

$\gcd(91, 287) = r_1 = 7$.

Euklidov algoritam za NZD

- Euklidov algoritam uvek završava: vrednosti r_i opadaju i uvek su nenegativne
- Euklidov algoritam izračunava $\gcd(x, y)$
- poslednji korak: $r_k = q_{k+2} \cdot r_{k+1}$, tj. ostatak $r_{k+2} = 0$, $r_{k+1} | r_k$
- pretposlednji korak: $r_{k-1} = q_{k+1} r_k + r_{k+1}$, r_{k+1} deli desnu stranu, pa $r_{k+1} | r_{k-1}$, $\ldots$
- ponavljajući postupak: $r_{k+1} | r_0, r_1$, pa $r_{k+1} | x$ i $r_{k+1} | y$
- r_{k+1} je najveći delilac: za svaki drugi delilac c mora biti $c | r_0$, jer je $y = q_0 \cdot x + r_0$, a zatim i $c | r_1$, jer $x = q_1 \cdot r_0 + r_1$, $c | r_2, \ldots, c | r_{k+1}$

Euklidov algoritam za NZD

- Euklidov algoritam uvek završava: vrednosti r_i opadaju i uvek su nenegativne
- Euklidov algoritam izračunava $\gcd(x, y)$
- poslednji korak: $r_k = q_{k+2} \cdot r_{k+1}$, tj. ostatak $r_{k+2} = 0$, $r_{k+1} | r_k$
- pretposlednji korak: $r_{k-1} = q_{k+1} r_k + r_{k+1}$, r_{k+1} deli desnu stranu, pa $r_{k+1} | r_{k-1}$, $\ldots$
- ponavljajući postupak: $r_{k+1} | r_0, r_1$, pa $r_{k+1} | x$ i $r_{k+1} | y$
- r_{k+1} je najveći delilac: za svaki drugi delilac c mora biti $c | r_0$, jer je $y = q_0 \cdot x + r_0$, a zatim i $c | r_1$, jer $x = q_1 \cdot r_0 + r_1$, $c | r_2, \ldots, c | r_{k+1}$

Euklidov algoritam za NZD

- Euklidov algoritam uvek završava: vrednosti r_i opadaju i uvek su nenegativne
- Euklidov algoritam izračunava $\gcd(x, y)$
- poslednji korak: $r_k = q_{k+2} \cdot r_{k+1}$, tj. ostatak $r_{k+2} = 0$, $r_{k+1} | r_k$
- pretposlednji korak: $r_{k-1} = q_{k+1} r_k + r_{k+1}$, r_{k+1} deli desnu stranu, pa $r_{k+1} | r_{k-1}$, ...
- ponavljajući postupak: $r_{k+1} | r_0, r_1$, pa $r_{k+1} | x$ i $r_{k+1} | y$
- r_{k+1} je najveći delilac: za svaki drugi delilac c mora biti $c | r_0$, jer je $y = q_0 \cdot x + r_0$, a zatim i $c | r_1$, jer $x = q_1 \cdot r_0 + r_1$, $c | r_2, \ldots, c | r_{k+1}$

Euklidov algoritam za NZD

- Euklidov algoritam uvek završava: vrednosti r_i opadaju i uvek su nenegativne
- Euklidov algoritam izračunava $\gcd(x, y)$
- poslednji korak: $r_k = q_{k+2} \cdot r_{k+1}$, tj. ostatak $r_{k+2} = 0$, $r_{k+1} | r_k$
- pretposlednji korak: $r_{k-1} = q_{k+1} r_k + r_{k+1}$, r_{k+1} deli desnu stranu, pa $r_{k+1} | r_{k-1}$, ...
- ponavljajući postupak: $r_{k+1} | r_0, r_1$, pa $r_{k+1} | x$ i $r_{k+1} | y$
- r_{k+1} je najveći delilac: za svaki drugi delilac c mora biti $c | r_0$, jer je $y = q_0 \cdot x + r_0$, a zatim i $c | r_1$, jer $x = q_1 \cdot r_0 + r_1$, $c | r_2$, ..., $c | r_{k+1}$

Euklidov algoritam za NZD

Theorem

Neka je $d = \gcd(x, y)$. *Tada je za neke* $m, n \in \mathbb{Z}$

$$d = m \cdot x + n \cdot y$$

Proof.

- svaki $r_i = a \cdot x + b \cdot y$, $y = q_0 \cdot x + r_0$ i $x = q_1 \cdot r_0 + r_1$
- $r_0 = y - q_0 \cdot x$ i
- $r_1 = x - q_1 \cdot r_0 = x - q_1(y - q_0 \cdot x) = -q_1 \cdot y + (1 - q_1 \cdot q_0)x, \ldots$
- neka $r_{i-2} = m' \cdot x + n' \cdot y$ i $r_{i-1} = m'' \cdot x + n'' \cdot y$
- $r_{i-2} = q_i \cdot r_{i-1} + r_i$, pa je
- $r_i = r_{i-2} - q_i \cdot r_{i-1} = (m' \cdot x + n' \cdot y) - q_i(m'' \cdot x + n'' \cdot y) = (m' - q_i \cdot m'')x + (n' - q_i n'')y$,

Euklidov algoritam za NZD

Theorem

Neka je $d = \gcd(x, y)$. *Tada je za neke* $m, n \in \mathbb{Z}$

$$d = m \cdot x + n \cdot y$$

Proof.

- svaki $r_i = a \cdot x + b \cdot y$, $y = q_0 \cdot x + r_0$ i $x = q_1 \cdot r_0 + r_1$
- $r_0 = y - q_0 \cdot x$ i
- $r_1 = x - q_1 \cdot r_0 = x - q_1(y - q_0 \cdot x) = -q_1 \cdot y + (1 - q_1 \cdot q_0)x$, ...
- neka $r_{i-2} = m' \cdot x + n' \cdot y$ i $r_{i-1} = m'' \cdot x + n'' \cdot y$
- $r_{i-2} = q_i \cdot r_{i-1} + r_i$, pa je
- $r_i = r_{i-2} - q_i \cdot r_{i-1} = (m' \cdot x + n' \cdot y) - q_i(m'' \cdot x + n'' \cdot y) = (m' - q_i \cdot m'')x + (n' - q_i n'')y$,

Euklidov algoritam za NZD

Theorem

Neka je $d = \gcd(x, y)$. *Tada je za neke* $m, n \in \mathbb{Z}$

$$d = m \cdot x + n \cdot y$$

Proof.

- svaki $r_i = a \cdot x + b \cdot y$, $y = q_0 \cdot x + r_0$ i $x = q_1 \cdot r_0 + r_1$
- $r_0 = y - q_0 \cdot x$ i
- $r_1 = x - q_1 \cdot r_0 = x - q_1(y - q_0 \cdot x) = -q_1 \cdot y + (1 - q_1 \cdot q_0)x, \ldots$
- neka $r_{i-2} = m' \cdot x + n' \cdot y$ i $r_{i-1} = m'' \cdot x + n'' \cdot y$
- $r_{i-2} = q_i \cdot r_{i-1} + r_i$, pa je
- $r_i = r_{i-2} - q_i \cdot r_{i-1} = (m' \cdot x + n' \cdot y) - q_i(m'' \cdot x + n'' \cdot y) = (m' - q_i \cdot m'')x + (n' - q_i n'')y$,

Euklidov algoritam za NZD

Example

- $\gcd(91, 287) = 7$
- iz $287 = 3 \cdot 91 + 14$, je $14 = 287 - 3 \cdot 91$,
- iz $91 = 6 \cdot 14 + 7$, je $7 = 91 - 6 \cdot (287 - 3 \cdot 91) = 19 \cdot 91 - 6 \cdot 287$

Modularna aritmetika

Izračunavanje inverza elemenata iz $\mathbb{Z}_p$:

- p je prost broj i
- a je prirodan broj, takava da je $0 < a < p$
- tražimo x za koji je $0 < x < p$, tako da je $a \cdot x \equiv_p 1$, odnosno $x = a^{-1}$ u $\mathbb{Z}_p$
- p i a su uzajamno prosti, $\gcd(a, p) = 1$
- Euklidov algoritam daje u i v:

$$\gcd(a, p) = 1 = u \cdot a + v \cdot p$$

- $a \cdot u \equiv_p 1$
- ne mora biti $u < p$, inverz elementa a je $a^{-1} \equiv_p u$

Modularna aritmetika

Izračunavanje inverza elemenata iz $\mathbb{Z}_p$:

- p je prost broj i
- a je prirodan broj, takava da je $0 < a < p$
- tražimo x za koji je $0 < x < p$, tako da je $a \cdot x \equiv_p 1$, odnosno $x = a^{-1}$ u $\mathbb{Z}_p$
- p i a su uzajamno prosti, $\gcd(a, p) = 1$
- Euklidov algoritam daje u i v:

$$\gcd(a, p) = 1 = u \cdot a + v \cdot p$$

- $a \cdot u \equiv_p 1$
- ne mora biti $u < p$, inverz elementa a je $a^{-1} \equiv_p u$

Modularna aritmetika

Izračunavanje inverza elemenata iz $\mathbb{Z}_p$:

- p je prost broj i
- a je prirodan broj, takava da je $0 < a < p$
- tražimo x za koji je $0 < x < p$, tako da je $a \cdot x \equiv_p 1$, odnosno $x = a^{-1}$ u $\mathbb{Z}_p$
- p i a su uzajamno prosti, $\gcd(a, p) = 1$
- Euklidov algoritam daje u i v:

$$\gcd(a, p) = 1 = u \cdot a + v \cdot p$$

- $a \cdot u \equiv_p 1$
- ne mora biti $u < p$, inverz elementa a je $a^{-1} \equiv_p u$

Modularna aritmetika

Izračunavanje inverza elemenata iz $\mathbb{Z}_p$:

- p je prost broj i
- a je prirodan broj, takava da je $0 < a < p$
- tražimo x za koji je $0 < x < p$, tako da je $a \cdot x \equiv_p 1$, odnosno $x = a^{-1}$ u $\mathbb{Z}_p$
- p i a su uzajamno prosti, $\gcd(a, p) = 1$
- Euklidov algoritam daje u i v:

$$\gcd(a, p) = 1 = u \cdot a + v \cdot p$$

- $a \cdot u \equiv_p 1$
- ne mora biti $u < p$, inverz elementa a je $a^{-1} \equiv_p u$

Modularna aritmetika

Example

Neka je $p = 234527$, i neka je potrebno izračunati 2^{-1} u $\mathbb{Z}_p$. Tada je:

- $234527 = 117263 \cdot 2 + 1$, pa je
- $-117263 \cdot 2 + 1 \cdot 234527 = 1$ i
- $-117263 \equiv_{234527} 117264$,
- $2^{-1} \equiv_{234527} 117264$

Modularna aritmetika

Primene modularne aritmetike:

- generatori pseudoslučajnih brojeva,
- heš-funkcije i
- kriptologija.

Generatori pseudoslučajnih brojeva

- *generatori pseudoslučajnih brojeva* se koriste za simulaciju slučajnosti u programima
- generišu niz brojeva u nekom intervalu tako da postoji uniformna verovatnoća izbora bilo kog broja
- niz izgleda kao slučajan, ali se elementi izračunavaju pomoću determinističkih funkcija prethodnika

Generatori pseudoslučajnih brojeva

Metod linearne kongruencije:

- biraju se prirodni brojevi:
  - n, modul u odnosu na koga se posmatra kongruencija $\equiv_n$,
  - množilac a, takav da je $2 \leq a < n$,
  - pomeraj c, takav da $0 < c < n$ i
  - polazni element niza, x_0, koji se naziva i *seme*, takav da $0 \leq x_0 < n$.
- generiše se niz $\{x_i\}_i$ brojeva iz $\mathbb{Z}_n$ formulom

$$x_{n+1} \equiv_n (a \cdot x_n + c).$$

Generatori pseudoslučajnih brojeva

Example

Neka je $n = 9$, $a = 7$, $c = 4$ i $x_0 = 3$. Tada je:

- $7 * 3 + 4 = 25$ i $25 \equiv_9 7$, pa je $x_1 = 7$,
- $7 * 7 + 4 = 53$ i $53 \equiv_9 8$, pa je $x_2 = 8$, i slično
- $x_3 = 60 \equiv_9 6$, $x_4 = 46 \equiv_9 1$ itd.

Generatori pseudoslučajnih brojeva

- nakon ponavljanja jednog broja u nizu (a do takve situacije mora doći jer su članovi niza $0 \leq x_i < n$) ulazi se u ciklus
- za duži period preporučljivo je da n i a budu veliki, ali ne toliko da $a \cdot (n-1)$ dovede do prekoračenja
- za brzo izračunavanja ostatka pri deljenju sa n je pogodno i da je n oblika 2^m, jer se deljenje realizuje jednostavnim odbacivanjem najlakših bitova
- postupak je efikasan u smislu memorijskog zauzeća i vremena izvršavanja
- postoje i drugi, napredniji, postupci sa manjim stepenom korelacije generisanih pseudoslučajnih brojeva koji se primenjuju, na primer, u kriptografskim aplikacijama

Heš-funkcije

- U programiranju se često javlja potreba da se radi sa velikim brojem podataka koje je potrebno brzo pretraživati
- *heš-funkcije* na osnovu identifikatora podatka određuju njegovu lokaciju, recimo:
  - ako je k identifikator podatka i n prirodan broj koji odgovara broju raspoloživih memorijskih lokacija, onda je heš-funkcija h definisana sa
  - $h(k) = a$, gde je $a \equiv_n k$ ostatak pri delenju k sa n.

Heš-funkcije

- U programiranju se često javlja potreba da se radi sa velikim brojem podataka koje je potrebno brzo pretraživati
- *heš-funkcije* na osnovu identifikatora podatka određuju njegovu lokaciju, recimo:
  - ako je k identifikator podatka i n prirodan broj koji odgovara broju raspoloživih memorijskih lokacija, onda je heš-funkcija h definisana sa
  - $h(k) = a$, gde je $a \equiv_n k$ ostatak pri delenju k sa n.

Heš-funkcije

Example

Za $k_1 = 21$ i $k_2 = 35$ i $n = 9$:

- kako je $3 \equiv_9 21$, onda je $h(k_1) = 3$ i
- kako je $8 \equiv_9 35$, onda je $h(k_2) = 8$.
- problem: za $k_3 = 39$, $3 \equiv_9 39$, pa je $h(k_3) = 3 = h(k_1)$
- kreira se dinamička lista na koju pokazuje sadržaj memorijske lokacije u koju se preslikava više podataka, a sama lista sadrži te podatke, ili
- ako je memorijska lokacija u čiju adresu se preslikava neki podatak već zauzeta, podatak se smešta u prvu sledeću slobodnu lokaciju.

Heš-funkcije

Example

Za $k_1 = 21$ i $k_2 = 35$ i $n = 9$:

- kako je $3 \equiv_9 21$, onda je $h(k_1) = 3$ i
- kako je $8 \equiv_9 35$, onda je $h(k_2) = 8$.
- problem: za $k_3 = 39$, $3 \equiv_9 39$, pa je $h(k_3) = 3 = h(k_1)$
- kreira se dinamička lista na koju pokazuje sadržaj memorijske lokacije u koju se preslikava više podataka, a sama lista sadrži te podatke, ili
- ako je memorijska lokacija u čiju adresu se preslikava neki podatak već zauzeta, podatak se smešta u prvu sledeću slobodnu lokaciju.

Heš-funkcije

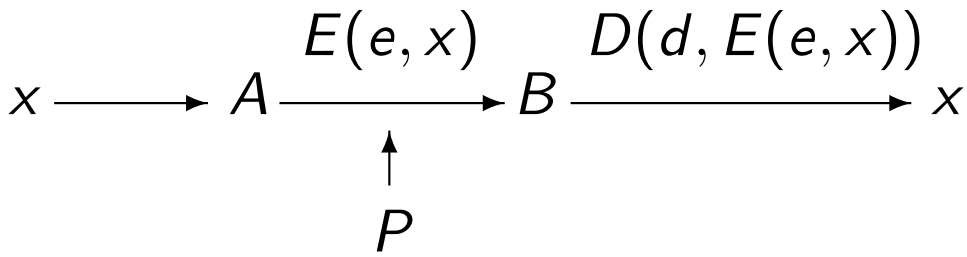
Example

Za $k_1 = 21$ i $k_2 = 35$ i $n = 9$:

- kako je $3 \equiv_9 21$, onda je $h(k_1) = 3$ i
- kako je $8 \equiv_9 35$, onda je $h(k_2) = 8$.
- problem: za $k_3 = 39$, $3 \equiv_9 39$, pa je $h(k_3) = 3 = h(k_1)$
- kreira se dinamička lista na koju pokazuje sadržaj memorijske lokacije u koju se preslikava više podataka, a sama lista sadrži te podatke, ili
- ako je memorijska lokacija u čiju adresu se preslikava neki podatak već zauzeta, podatak se smešta u prvu sledeću slobodnu lokaciju.

RSA algoritam

Komunikacija dve strane u prisustvu prisluškivača:



- A želi da pošalje poruku osobi B
- E i D - algoritmi za kodiranje, dekodiranje, $D(d, E(e, x)) = x$
- E i D terba da se efikasno izračunavaju
- sigurnost komunikacije: e i d su tajni ključevi, x se ne može efikasno izračunati iz $E(e, x)$ bez d.

RSA algoritam

Example

Kodiranje pomoću sabiranje po modulu 2 po bitovima:

10101001 - tekst poruke x,

$+$ 11000111 - ključ a

01101110 - kodirani tekst dobijen kao $x + a$.

Pošto je $D(a, E(a, x)) = (x + a) + a = x$, dekodiranjem dobijamo:

01101110 - kodirani tekst $x + a$,

$+$ 11000111 - ključ a

10101001 - tekst poruke x, dobijen kao $(x + a) + a$,

RSA algoritam

Nastavak primera

Ako prisluškivač uspe da sazna x i kodiranu poruku, otkriva i ključ:

$$\begin{array}{rl} & 10101001 \text{ - tekst poruke } x, \\ + & 01101110 \text{ - kodirani tekst } x + a, \\ & 11000111 \text{ - ključ } a, \text{ dobijen kao } x + (x + a). \end{array}$$

Odavde sledi da prisluškivač može dekodirati kodiranu poruku ako i samo ako zna a, što je primer takozvane apsolutne sigurnosti kodiranja.

RSA algoritam

Nastavak primera

Ako prisluškivač uspe da sazna x i kodiranu poruku, otkriva i ključ:

$$\begin{array}{rl} & 10101001 \text{ - tekst poruke } x, \\ + & 01101110 \text{ - kodirani tekst } x + a, \\ & 11000111 \text{ - ključ } a, \text{ dobijen kao } x + (x + a). \end{array}$$

Odavde sledi da prisluškivač može dekodirati kodiranu poruku ako i samo ako zna a, što je primer takozvane apsolutne sigurnosti kodiranja.

RSA algoritam

Problemi:

- dogovor osoba A i B koji se obavlja pre komunikacije, jer je reč o razmeni ključa koji treba da ostane tajan i koji je iste dužine kao i poruka
- ako se koristi kraći ključ, ili isti više puta:
- ako je ključ kratak, vrši se pretraga kroz prostor svih mogućih ključeva
- ako se ključ koristi više puta u kodiranju, vrše se razne analize
- kriptološki sistemi sa *javnim ključem*

RSA algoritam

Problemi:

- dogovor osoba A i B koji se obavlja pre komunikacije, jer je reč o razmeni ključa koji treba da ostane tajan i koji je iste dužine kao i poruka
- ako se koristi kraći ključ, ili isti više puta:
- ako je ključ kratak, vrši se pretraga kroz prostor svih mogućih ključeva
- ako se ključ koristi više puta u kodiranju, vrše se razne analize
- kriptološki sistemi sa *javnim ključem*

RSA algoritam

Problemi:

- dogovor osoba A i B koji se obavlja pre komunikacije, jer je reč o razmeni ključa koji treba da ostane tajan i koji je iste dužine kao i poruka
- ako se koristi kraći ključ, ili isti više puta:
- ako je ključ kratak, vrši se pretraga kroz prostor svih mogućih ključeva
- ako se ključ koristi više puta u kodiranju, vrše se razne analize
- kriptološki sistemi sa *javnim ključem*

RSA algoritam

Sistem RSA (R. Ravist, A. Shamir, L. Adleman):

- biraju se dva prosta broja p i q, recimo $p = 47$ i $q = 71$,
- razmatraju se njihov proizvod, $n = pq = 47 \cdot 71 = 3337$, i $(p-1)(q-1) = 6 \cdot 70 = 3220$,
- iz skupa $\{1, \ldots, (p-1)(q-1)\}$ se bira broj e koji je uzajamno prost sa $(p-1)(q-1)$, recimo $e = 79$,
- nalazi se broj d takav da je $ed \equiv_{(p-1)(q-1)} 1$, $d = 79^{-1} \equiv_{3220} 1019$,
- funkcija kodiranja je

$$E(e, x) \equiv_{pq} x^e$$

- funkcija dekodiranja je

$$D(d, E(a, x)) \equiv_{pq} E(a, x)^d \equiv_{pq} x^{ed} \equiv_{pq} x.$$

RSA algoritam

- javni ključ - (pq, e), tajni ključ - (pq, d)
- p i q treba da ostanu tajni, inače se d efikasno izračunava
- nalaženje inverzne funkcije od $E(e, x)$ svodi na problem faktorisanja brojeva, koji je težak ako su p i q tajni
- u realnim primenama veličine brojeva p, q, e i d su reda stotina bita
- mogućnost efikasnog izračunavanja velikih brojeva koji se pojavljuju pri RSA kodiranju ($x^e(\mod pq)$)

RSA algoritam - digitalni potpis

- $x^{ed} \equiv_{pq} x^{de}$, postupci kodiranja i dekodiranja za RSA komutiraju
- *digitalni potpis* uverava B da je A poslala poruku x
- A i B imaju javne ključeve e_A i e_B i tajne ključeve d_A i d_B,
- A šalje potpisanu poruku $S_A(x) = (x, D(d_A, x)) = (x, x^d)$ koja sadrži originalnu poruku x na koju je nadovezan potpis, tj. vrednost $D(d_A, x) \equiv_{pq} x^d$
- B proverava potpis računajući $E(e_A, D(d_A, x)) \equiv_{pq} x^{de} \equiv_{pq} x$.

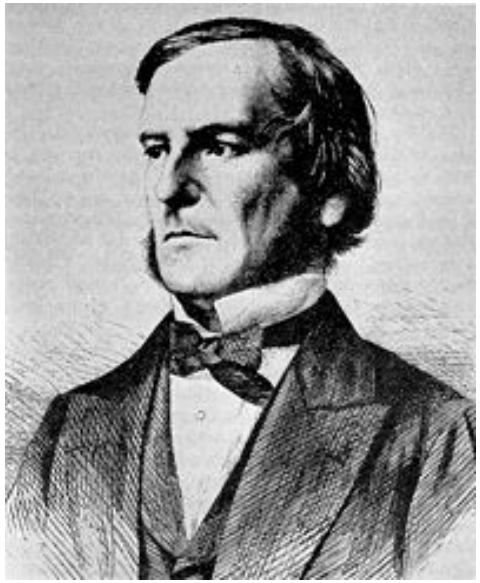
Bulove algebre

Definition

Bulova algebra je algebarska struktura $\langle B, +, \cdot, ', 1, 0\rangle$ za koju važi:

- Komutativnost: $x \cdot y = y \cdot x$ i $x + y = y + x$
- Asocijativnost: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ i $x + (y + z) = (x + y) + z$
- Distributivnost:
  $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ i
  $x + (y \cdot z) = (x + y) \cdot (x + z)$
- Svojstva elemenata 0 i 1: $x \cdot 1 = x$ i $x + 0 = x$
- Svojstva komplementa: $x \cdot x' = 0$ i $x + x' = 1$.

George Boole, 1815 –1864



Engleski matematičar. Najpoznatiji rezultati koje je dao sistematizovani su u knjizi *An Investigation of the Laws of Thought, on Which are Founded the Mathematical Theories of Logic and Probabilities* (1854) gde je uveo algebarski sistem kojim je formalizovao logičko zaključivanje. Smatrao je da je verovatnoća deo logike i precizirao postupke kojima se na osnovu verovatnoća uslova izračunavaju verovatnoće logičkih posledica.

Bulove algebre

Primeri:

- *algebra skupova* $\langle \mathbb{P}(A), \cup, \cap, \mathbb{C}, A, \emptyset \rangle$, gde su A neprazan skup, $\mathbb{P}(A)$ partitivni skup skupa A i $\mathbb{C}$ komplement u odnosu na skup A,
- *intervalna algebra* u kojoj su elementi skupa nosača konačne unije poluotvorenih intervala oblika $[a, b) \subset [0, +\infty)$, a operacije su unija, presek i komplement u odnosu na $[0, +\infty)$, $1 = [0, +\infty)$ i $0 = [0, 0)$ i
- *iskazna algebra* $BA_2 = \langle \{\top, \bot\}, \vee, \wedge, \neg, \top, \bot \rangle$,
- Lindenbaum-Tarski algebra u kojoj je skup nosač skup svih klasa ekvivalencije skupa iskaznih formula u odnosu na relaciju $\alpha \sim \beta$ definisanu sa $\vdash \alpha \leftrightarrow \beta$, a operacije su $[\alpha] \vee [\beta] = [\alpha \vee \beta]$, $[\alpha] \wedge [\beta] = [\alpha \wedge \beta]$, $\neg[\alpha] = [\neg\alpha]$, $1 = [\alpha \vee \neg\alpha]$ i $0 = [\alpha \wedge \neg\alpha]$.

Bulove algebre

Theorem (Stonova teorema o reprezentaciji)

Svaka Bulova algebra je izomorfna nekoj algebri skupova. (kod konačnih algebri kardinalnost skupa nosača mora biti stepen broja 2)

Theorem

Jednakost $t_1 = t_2$ važi u svim Bulovim algebrama ako i samo ako važi u Bulovoj algebri BA_2.

Bulove algebre

Theorem

Iskazna formula α na jeziku $\{\neg, \wedge, \vee\}$ je tautologija ako i samo ako u Bulovoj algebri BA_2 važi jednakost $\alpha = 1$, pri čemu se iskazna slova shvataju kao promenljive.

Theorem (Princip dualnosti)

Iskaz važi u svim Bulovim algebrama ako i samo ako u svim Bulovim algebrama važi i njegov dual (sistematska zamena simbola $+$ i $\cdot$, odnosno 1 i 0.).

Bulove algebre

Theorem

U svim Bulovim algebrama važi:

1. *jedinstvenost komplementa: ako* $x + y = 1$ *i* $x \cdot y = 0$, *onda* $x' = y$,
2. *idempotencija:* $x \cdot x = x$, $x + x = x$,
3. $x \cdot 0 = 0$, $x \cdot 1 = x$,
4. *apsorpcija:* $x + (x \cdot y) = x$, $x \cdot (x + y) = x$,
5. *involucija:* $(x')' = x$,
6. $0' = 1$, $1' = 0$,
7. $x \cdot (x' + y) = x \cdot y$, $x + (x' \cdot y) = x + y$,
8. *De Morganovi zakoni:* $(x + y)' = x' \cdot y'$, $(x \cdot y)' = x' + y'$,
9. $x \cdot y + x \cdot y' = x$, $(x + y) \cdot (x + y') = x$,
10. *konsenzus:* $x \cdot y + x' \cdot z + y \cdot z = x \cdot y + x' \cdot z$, $(x + y) \cdot (x' + z) \cdot (y + z) = (x + y) \cdot (x' + z)$.

Bulove algebre

Proof.

1 Jedinstvenost komplementa, $(x + y = 1) \wedge (x \cdot y = 0) \Rightarrow (x' = y)$:
$y = y \cdot 1 = y \cdot (x + x') = (y \cdot x) + (y \cdot x') = 0 + (y \cdot x') =$
$(x' \cdot x) + (x' \cdot y) = x' \cdot (x + y) = x' \cdot 1 = x'$.

8 De Morganovi zakoni, $(x + y)' = x' \cdot y'$, $(x \cdot y)' = x' + y'$:
$(x + y) + (x' \cdot y') = ((x + y) + x') \cdot ((x + y) + y') =$
$((x + x') + y) \cdot (x + (y + y')) = 1 \cdot 1 = 1$, kao i
$(x+y)\cdot(x'\cdot y') = (x'\cdot y')\cdot(x+y) = ((x'\cdot y')\cdot x)+((x'\cdot y')\cdot y) = 0+0 = 0$,
pa je na osnovu jedinstvenosti komplemeta $(x + y)' = x' \cdot y'$.

10 konsenzus, $x \cdot y + x' \cdot z + y \cdot z = x \cdot y + x' \cdot z$:
$x \cdot y + x' \cdot z + y \cdot z = x \cdot y + x' \cdot z + y \cdot z \cdot (x + x') =$
$x\cdot y+x'\cdot z+x\cdot y\cdot z+x'\cdot y\cdot z = x\cdot y\cdot(1+z)+x'\cdot z\cdot(1+y) = x\cdot y+x'\cdot z$.

Augustus De Morgan, 1806 – 1871

Engleski matematičar i logičar. Formulisao je zakone nazvane po njemu i strogo zasnovao ideju indukcije.

Bulove funkcije

Definition (Bulove funkcije)

Za Bulovu algebru $\langle B, +, \cdot, ', 1, 0\rangle$ *klasa Bulovih funkcija sa n promenljivih* sadrži osnovne funkcije:

- konstantne funkcije $f(x_1, \ldots, x_n) = b$ za svaki $b \in B$ i
- funkcije projekcije $f(x_1, \ldots, x_n) = x_i$

i sve funkcije koje se od njih dobijaju konačnom primenom pravila:

- $(f + g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)$,
- $(f \cdot g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)$ i
- $(f')(x_1, \ldots, x_n) = (f(x_1, \ldots, x_n))'$

na već definisane funkcije f i g.

Bulove funkcije

Ispitivanje jednakosti dva izraza nekada nije trivijalan zadatak, efektivan metod koji se može sprovoditi automatski je dobrodošao.

Definition

Neka je $f(x_1, x_2, \ldots, x_n)$ Bulova funkcija i

- $f_{x_1'}(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$ i
- $f_{x_1}(x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$.

Funkcije $f_{x_1'}(x_2, \ldots, x_n)$ i $f_{x_1}(x_2, \ldots, x_n)$ se nazivaju *kofaktori* funkcije $f(x_1, x_2, \ldots, x_n)$ u odnosu na x_1.
Izrazi $f(0, \ldots, 0, 0)$, $f(0, \ldots, 0, 1)$, $\ldots$, $f(1, \ldots, 1, 1)$ se nazivaju *diskriminante*.

Bulove funkcije

Ispitivanje jednakosti dva izraza nekada nije trivijalan zadatak, efektivan metod koji se može sprovoditi automatski je dobrodošao.

Definition

Neka je $f(x_1, x_2, \ldots, x_n)$ Bulova funkcija i

- $f_{x_1'}(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$ i
- $f_{x_1}(x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$.

Funkcije $f_{x_1'}(x_2, \ldots, x_n)$ i $f_{x_1}(x_2, \ldots, x_n)$ se nazivaju *kofaktori* funkcije $f(x_1, x_2, \ldots, x_n)$ u odnosu na x_1.
Izrazi $f(0, \ldots, 0, 0)$, $f(0, \ldots, 0, 1)$, $\ldots$, $f(1, \ldots, 1, 1)$ se nazivaju *diskriminante*.

Bulove funkcije

Theorem (Bul-Šenonova (Shannon) teorema ekspanzije)

Za svaku Bulovu funkciju $f : B^n \to B$ *i sve* $(x_1, \ldots, x_n) \in B$ *je*

$$f(x_1, x_2, \ldots, x_n) = x_1' \cdot f(0, x_2, \ldots, x_n) + x_1 \cdot f(1, x_2, \ldots, x_n)$$

i dualno

$$f(x_1, x_2, \ldots, x_n) = (x_1' + f(1, x_2, \ldots, x_n)) \cdot (x_1 + f(0, x_2, \ldots, x_n)).$$

Proof.

Dokaz jednakosti se sprovodi indukcijom po složenosti funkcija. Za konstantne funkcije i funkcije projekcije tvrđenje trivijalno važi. U indukcijskom koraku se pretpostavi da tvrđenje važi za funkcije f i g i proverava da važi za funkcije koje se od njih dobijaju. □

Bulove funkcije

Theorem (Bul-Šenonova (Shannon) teorema ekspanzije)

Za svaku Bulovu funkciju $f : B^n \to B$ *i sve* $(x_1, \ldots, x_n) \in B$ *je*

$$f(x_1, x_2, \ldots, x_n) = x_1' \cdot f(0, x_2, \ldots, x_n) + x_1 \cdot f(1, x_2, \ldots, x_n)$$

i dualno

$$f(x_1, x_2, \ldots, x_n) = (x_1' + f(1, x_2, \ldots, x_n)) \cdot (x_1 + f(0, x_2, \ldots, x_n)).$$

Proof.

Dokaz jednakosti se sprovodi indukcijom po složenosti funkcija. Za konstantne funkcije i funkcije projekcije tvrđenje trivijalno važi. U indukcijskom koraku se pretpostavi da tvrđenje važi za funkcije f i g i proverava da važi za funkcije koje se od njih dobijaju. □

Bulove funkcije

Example

Primena teoreme ekspanzije na $f = x_1 \cdot x_2 \cdot x_3' + x_2 \cdot (x_1' + x_3)$ daje:

$$f = x_1' \cdot x_2 + x_1 \cdot (x_2 \cdot x_3' + x_2 \cdot x_3) = (x_1' + x_1) \cdot x_2 = x_2,$$

odnosno dualnom varijantom teoreme

$$f = (x_1' + (x_2 \cdot x_3' + x_2 \cdot x_3)) \cdot (x_1 + x_2) = (x_1' + x_2) \cdot (x_1 + x_2) = x_2,$$

pri čemu je
$f(0, x_2, \ldots, x_n) = x_2 \cdot (1 + x_3) = x_2$ i
$f(1, x_2, \ldots, x_n) = (x_2 \cdot x_3' + x_2 \cdot x_3) = x_2.$

Kanonske forme Bulovih funkcija

Dalje razvijanje izraza daje *kanonske forme*:

- *kanonska disjunktivna forma* ili *kanonska minterm forma* za $f \neq 0$:

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= x_1' \cdot \ldots \cdot x_{n-1}' \cdot x_n' \cdot f(0, \ldots, 0, 0) + \\ & \quad x_1' \cdot \ldots \cdot x_{n-1}' \cdot x_n \cdot f(0, \ldots, 0, 1) + \ldots + \\ & \quad x_1 \cdot \ldots \cdot x_{n-1} \cdot x_n \cdot f(1, \ldots, 1, 1) \end{aligned}$$

  Izrazi $x_1' \cdot \ldots \cdot x_{n-1}' \cdot x_n'$, $\ldots$: *mintermi*

- *kanonska konjunktivna forma* ili *kanonska maksterm forma* za $f \neq 1$:

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= (x_1 + \ldots + x_{n-1} + x_n + f(0, \ldots, 0, 0)) \cdot \\ & \quad (x_1 + \ldots + x_{n-1} + x_n' + f(0, \ldots, 0, 1)) \cdot \ldots \cdot \\ & \quad (x_1' + \ldots + x_{n-1}' + x_n' + f(1, \ldots, 1, 1)). \end{aligned}$$

  Izrazi $x_1' + \ldots + x_{n-1}' + x_n'$, $\ldots$: *makstermi*

Kanonske forme Bulovih funkcija

Example

Posmatrajmo funkciju

$$f(x, y) = x + y.$$

Kako je $f(0,0) = 0$ i $f(1,0) = f(0,1) = f(1,1) = 1$, to je disjunktivna kanonska forma oblika

$$x' \cdot y' \cdot f(0,0) + x' \cdot y \cdot f(0,1) + x \cdot y' \cdot f(1,0) + x \cdot y \cdot f(1,1) = x' \cdot y + x \cdot y' + x \cdot y.$$

Kanonske forme Bulovih funkcija

Example

Posmatrajmo funkciju

$$f = x_1 \cdot x_2 + a \cdot x_2'$$

nad Bulovom algebrom sa skupom nosačem $B = \{0, a, b, 1\}$. Njena disjunktivna kanonska forma je

$$a \cdot x_1' \cdot x_2' + 0 \cdot x_1' \cdot x_2 + a \cdot x_1 \cdot x_2' + 1 \cdot x_1 \cdot x_2,$$

dok je

$$(a + x_1' + x_2') \cdot (0 + x_1' + x_2) \cdot (a + x_1 + x_2') \cdot (1 + x_1 + x_2)$$

njena konjunktivna kanonska forma.

Kanonske forme Bulovih funkcija

Theorem

Kanonske forme date Bulove funkcije su jedinstvene (do na redosled minterma/maxterma u zapisu).

Proof.

- $f(x_1, x_2, \ldots, x_n) \neq 0$ ima dve kanonske disjunktivne forme
- argumenti diskriminanti $f(0, \ldots, 0, 0)$, $\ldots$, su 0 ili 1, pa i vrednosti
- nakon izračunavanja vrednosti diskriminanti, forme su (M_i, N_j mintermi):
  - $f(x_1, x_2, \ldots, x_n) = M_1 + \ldots + M_m$ i
  - $f(x_1, x_2, \ldots, x_n) = N_1 + \ldots + N_n$,
- postoji minterm koji jeste u jednoj, a nije u drugoj formi: M_k

Kanonske forme Bulovih funkcija

Theorem

Kanonske forme date Bulove funkcije su jedinstvene (do na redosled minterma/maxterma u zapisu).

Proof.

- $f(x_1, x_2, \ldots, x_n) \neq 0$ ima dve kanonske disjunktivne forme
- argumenti diskriminanti $f(0, \ldots, 0, 0)$, $\ldots$, su 0 ili 1, pa i vrednosti
- nakon izračunavanja vrednosti diskriminanti, forme su (M_i, N_j mintermi):
  - $f(x_1, x_2, \ldots, x_n) = M_1 + \ldots + M_m$ i
  - $f(x_1, x_2, \ldots, x_n) = N_1 + \ldots + N_n$,
- postoji minterm koji jeste u jednoj, a nije u drugoj formi: M_k

Kanonske forme Bulovih funkcija

Theorem

Kanonske forme date Bulove funkcije su jedinstvene (do na redosled minterma/maxterma u zapisu).

Proof.

- $f(x_1, x_2, \ldots, x_n) \neq 0$ ima dve kanonske disjunktivne forme
- argumenti diskriminanti $f(0, \ldots, 0, 0)$, $\ldots$, su 0 ili 1, pa i vrednosti
- nakon izračunavanja vrednosti diskriminanti, forme su (M_i, N_j mintermi):
  - $f(x_1, x_2, \ldots, x_n) = M_1 + \ldots + M_m$ i
  - $f(x_1, x_2, \ldots, x_n) = N_1 + \ldots + N_n$,
- postoji minterm koji jeste u jednoj, a nije u drugoj formi: M_k

Kanonske forme Bulovih funkcija

Theorem

Kanonske forme date Bulove funkcije su jedinstvene (do na redosled minterma/maxterma u zapisu).

Proof.

- $f(x_1, x_2, \ldots, x_n) \neq 0$ ima dve kanonske disjunktivne forme
- argumenti diskriminanti $f(0, \ldots, 0, 0)$, $\ldots$, su 0 ili 1, pa i vrednosti
- nakon izračunavanja vrednosti diskriminanti, forme su (M_i, N_j mintermi):
  - $f(x_1, x_2, \ldots, x_n) = M_1 + \ldots + M_m$ i
  - $f(x_1, x_2, \ldots, x_n) = N_1 + \ldots + N_n$,
- postoji minterm koji jeste u jednoj, a nije u drugoj formi: M_k

Kanonske forme Bulovih funkcija

Theorem

Kanonske forme date Bulove funkcije su jedinstvene (do na redosled minterma/maxterma u zapisu).

Proof.

- $f(x_1, x_2, \ldots, x_n) \neq 0$ ima dve kanonske disjunktivne forme
- argumenti diskriminanti $f(0, \ldots, 0, 0)$, $\ldots$, su 0 ili 1, pa i vrednosti
- nakon izračunavanja vrednosti diskriminanti, forme su (M_i, N_j mintermi):
  - $f(x_1, x_2, \ldots, x_n) = M_1 + \ldots + M_m$ i
  - $f(x_1, x_2, \ldots, x_n) = N_1 + \ldots + N_n$,
- postoji minterm koji jeste u jednoj, a nije u drugoj formi: M_k

Kanonske forme Bulovih funkcija

Nastavak dokaza:

- $M_k \neq N_j$ za $(j = 1, n)$
- za svaki N_j postoji $x_{k(j)}$ takav da je $x_{k(j)}$ u M_k, a $x'_{k(j)}$ u N_j, ili obrnuto
- odatle: $M_k \cdot N_j = 0$ za $(j = 1, n)$
- sledi:
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (M_1 + \ldots + M_m) = M_k \cdot M_k = M_k$ i
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (N_1 + \ldots + N_n) = 0$,
- očigledna kontradikcija, pa je kanonska disjunktivna forma jedinstvena

Kanonske forme Bulovih funkcija

Nastavak dokaza:

- $M_k \neq N_j$ za $(j = 1, n)$
- za svaki N_j postoji $x_{k(j)}$ takav da je $x_{k(j)}$ u M_k, a $x'_{k(j)}$ u N_j, ili obrnuto
- odatle: $M_k \cdot N_j = 0$ za $(j = 1, n)$
- sledi:
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (M_1 + \ldots + M_m) = M_k \cdot M_k = M_k$ i
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (N_1 + \ldots + N_n) = 0$,
- očigledna kontradikcija, pa je kanonska disjunktivna forma jedinstvena

Kanonske forme Bulovih funkcija

Nastavak dokaza:

- $M_k \neq N_j$ za $(j = 1, n)$
- za svaki N_j postoji $x_{k(j)}$ takav da je $x_{k(j)}$ u M_k, a $x'_{k(j)}$ u N_j, ili obrnuto
- odatle: $M_k \cdot N_j = 0$ za $(j = 1, n)$
- sledi:
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (M_1 + \ldots + M_m) = M_k \cdot M_k = M_k$ i
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (N_1 + \ldots + N_n) = 0$,
- očigledna kontradikcija, pa je kanonska disjunktivna forma jedinstvena

Kanonske forme Bulovih funkcija

Nastavak dokaza:

- $M_k \neq N_j$ za $(j = 1, n)$
- za svaki N_j postoji $x_{k(j)}$ takav da je $x_{k(j)}$ u M_k, a $x'_{k(j)}$ u N_j, ili obrnuto
- odatle: $M_k \cdot N_j = 0$ za $(j = 1, n)$
- sledi:
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (M_1 + \ldots + M_m) = M_k \cdot M_k = M_k$ i
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (N_1 + \ldots + N_n) = 0$,
- očigledna kontradikcija, pa je kanonska disjunktivna forma jedinstvena

Kanonske forme Bulovih funkcija

Nastavak dokaza:

- $M_k \neq N_j$ za $(j = 1, n)$
- za svaki N_j postoji $x_{k(j)}$ takav da je $x_{k(j)}$ u M_k, a $x'_{k(j)}$ u N_j, ili obrnuto
- odatle: $M_k \cdot N_j = 0$ za $(j = 1, n)$
- sledi:
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (M_1 + \ldots + M_m) = M_k \cdot M_k = M_k$ i
  - $M_k \cdot f(x_1, x_2, \ldots, x_n) = M_k \cdot (N_1 + \ldots + N_n) = 0$,
- očigledna kontradikcija, pa je kanonska disjunktivna forma jedinstvena

Kanonske forme Bulovih funkcija

- ako dve funkcije imaju jednake kanonske forme, one su jednake
- svaka Bulova funkcija potpuno okarakterisana diskriminantama, odnosno vrednostima u ovim specijalnim tačkama, i bez obzira na skup nosač B koji ne mora biti $\{0, 1\}$

Kanonske forme Bulovih funkcija

Example

Funkcije

- $f(x, y) = x + y$ i
- $g(x, y) = x' \cdot y + x$

imaju istu kanonsku disjunktivnu formu: $x' \cdot y + x \cdot y' + x \cdot y$.
Reč je samo o različitim zapisima iste funkcije.

Kanonske forme Bulovih funkcija

Example

Ako je za funkciju $f(x, y)$ ispunjeno da je

$$f(0,0) = 0, f(1,0) = f(0,1) = f(1,1) = 1$$

njena disjunktivna kanonska forma je

$$x' \cdot y + x \cdot y' + x \cdot y$$

Bulove funkcije i logički dizajn

Example

Puni sabirač (binarni sabirač) je elektronsko kolo sa:

- ulazima x, y (bitovi koji se sabiraju) i c (prenos sa prethodnog para)
- izlazima r i s, gde je r bit rezultata, a s bit prenosa

x	y	c	r	s
1	1	1	1	1
1	1	0	0	1
1	0	1	0	1
1	0	0	1	0
0	1	1	0	1
0	1	0	1	0
0	0	1	1	0
0	0	0	0	0

Bulove funkcije i logički dizajn

Nastavak primera:

Kanonske disjunktivne normalne forme:

- za r: $(x' \cdot y' \cdot c) + (x' \cdot y \cdot c') + (x \cdot y' \cdot c') + (x \cdot y \cdot c)$
- za s: $(x' \cdot y \cdot c) + (x \cdot y' \cdot c) + (x \cdot y \cdot c') + (x \cdot y \cdot c)$

Optimizacija:

- za r: $(x' \cdot ((y' \cdot c) + (y \cdot c'))) + (x \cdot ((y' \cdot c') + (y \cdot c)))$
- za r: $x \veebar (y \veebar c)$
- za s: $(y \cdot c) + (x \cdot ((y' \cdot c) + (y \cdot c')))$
- za s: $(y \cdot c) + (x \cdot (y \veebar c))$

Bulove funkcije i logički dizajn

Nastavak primera:

Kanonske disjunktivne normalne forme:

- za r: $(x' \cdot y' \cdot c) + (x' \cdot y \cdot c') + (x \cdot y' \cdot c') + (x \cdot y \cdot c)$
- za s: $(x' \cdot y \cdot c) + (x \cdot y' \cdot c) + (x \cdot y \cdot c') + (x \cdot y \cdot c)$

Optimizacija:

- za r: $(x' \cdot ((y' \cdot c) + (y \cdot c'))) + (x \cdot ((y' \cdot c') + (y \cdot c)))$
- za r: $x \veebar (y \veebar c)$
- za s: $(y \cdot c) + (x \cdot ((y' \cdot c) + (y \cdot c')))$
- za s: $(y \cdot c) + (x \cdot (y \veebar c))$

Bulove funkcije i logički dizajn

Optimizacija broja elemenata logičkih kola, pored direktnih ušteda, smanjuje i mogućnost grešaka u razvoju.
"Biti jednostavniji izraz":

- razmatraju se ekvivalentni izrazi predstavljeni u disjunktivnoj formi (kao zbirovi proizvoda *literala* - promenljivih ili komplementiranih promenljivijih),
- jednostavniji izrazi imaju manji broj proizvoda koji se sabiraju i
- ako se dva izraza sastoje od istog broja proizvoda, jednostavniji je onaj koji ima ukupno manji broj literala (pri čemu se broje sve pojave literala, a ne samo različiti literali).

Ne mora postojati jedinstveni najjednostavniji izraz.
Jedna od metoda za optimizaciju: *Karnuovi dijagrami*.

Bulove funkcije i logički dizajn

Optimizacija broja elemenata logičkih kola, pored direktnih ušteda, smanjuje i mogućnost grešaka u razvoju.
"Biti jednostavniji izraz":

- razmatraju se ekvivalentni izrazi predstavljeni u disjunktivnoj formi (kao zbirovi proizvoda *literala* - promenljivih ili komplementiranih promenljivijih),
- jednostavniji izrazi imaju manji broj proizvoda koji se sabiraju i
- ako se dva izraza sastoje od istog broja proizvoda, jednostavniji je onaj koji ima ukupno manji broj literala (pri čemu se broje sve pojave literala, a ne samo različiti literali).

Ne mora postojati jedinstveni najjednostavniji izraz.
Jedna od metoda za optimizaciju: *Karnuovi dijagrami*.

Karnuovi dijagrami

- tabelarna metoda za optimizovanje za neki unapred fiksirani skup promenljivih
- polja tabele odgovaraju mintermima nad tim promenljivim

Karnuov dijagram za promeljive x, y i z:

	$y \cdot z$	$y' \cdot z$	$y' \cdot z'$	$y \cdot z'$
x	$x \cdot y \cdot z$	$x \cdot y' \cdot z$	$x \cdot y' \cdot z'$	$x \cdot y \cdot z'$
x'	$x' \cdot y \cdot z$	$x' \cdot y' \cdot z$	$x' \cdot y' \cdot z'$	$x' \cdot y \cdot z'$

Mintermi su poređani tako da se u susednim ćelijama razlikuju samo na jednom mestu (svi literali sem jednog su identični,a taj literal je u jednoj ćeliji promenljiva, a u drugoj njen komplement). Pod susednim ćelijama ovde se podrazumevaju i ćelije na početku i kraju jednog reda, odnosno jedne kolone, ali ne i ćelije susedne po nekoj dijagonali.

Karnuovi dijagrami

- tabelarna metoda za optimizovanje za neki unapred fiksirani skup promenljivih
- polja tabele odgovaraju mintermima nad tim promenljivim

Karnuov dijagram za promeljive x, y i z:

	$y \cdot z$	$y' \cdot z$	$y' \cdot z'$	$y \cdot z'$
x	$x \cdot y \cdot z$	$x \cdot y' \cdot z$	$x \cdot y' \cdot z'$	$x \cdot y \cdot z'$
x'	$x' \cdot y \cdot z$	$x' \cdot y' \cdot z$	$x' \cdot y' \cdot z'$	$x' \cdot y \cdot z'$

Mintermi su poređani tako da se u susednim ćelijama razlikuju samo na jednom mestu (svi literali sem jednog su identični,a taj literal je u jednoj ćeliji promenljiva, a u drugoj njen komplement). Pod susednim ćelijama ovde se podrazumevaju i ćelije na početku i kraju jednog reda, odnosno jedne kolone, ali ne i ćelije susedne po nekoj dijagonali.

Karnuovi dijagrami

- tabelarna metoda za optimizovanje za neki unapred fiksirani skup promenljivih
- polja tabele odgovaraju mintermima nad tim promenljivim

Karnuov dijagram za promeljive x, y i z:

	$y \cdot z$	$y' \cdot z$	$y' \cdot z'$	$y \cdot z'$
x	$x \cdot y \cdot z$	$x \cdot y' \cdot z$	$x \cdot y' \cdot z'$	$x \cdot y \cdot z'$
x'	$x' \cdot y \cdot z$	$x' \cdot y' \cdot z$	$x' \cdot y' \cdot z'$	$x' \cdot y \cdot z'$

Mintermi su poređani tako da se u susednim ćelijama razlikuju samo na jednom mestu (svi literali sem jednog su identični,a taj literal je u jednoj ćeliji promenljiva, a u drugoj njen komplement). Pod susednim ćelijama ovde se podrazumevaju i ćelije na početku i kraju jednog reda, odnosno jedne kolone, ali ne i ćelije susedne po nekoj dijagonali.

Karnuovi dijagrami

Za konkretan izraz u ćelijama koje odgovaraju mintermima prisutnim u disjunktivnoj normalnoj formi izraza upisuje je 1, dok su ostale ćelije prazne.

Izraz $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z'$ je predstavljen Karnuovim dijagramom:

	$y \cdot z$	$y' \cdot z$	$y' \cdot z'$	$y \cdot z'$
x		1	1	
x'	1			1

Karnuovi dijagrami

Za konkretan izraz u ćelijama koje odgovaraju mintermima prisutnim u disjunktivnoj normalnoj formi izraza upisuje je 1, dok su ostale ćelije prazne.

Izraz $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z'$ je predstavljen Karnuovim dijagramom:

	$y \cdot z$	$y' \cdot z$	$y' \cdot z'$	$y \cdot z'$
x		1	1	
x'	1			1

Karnuovi dijagrami

- prisutnost znaka 1 u susednim ćelijama nekog Karnuovog dijagrama znači da su disjunktivnoj normalnoj formi izraza prisutna dva minterma koja se razlikuju samo u jednom literalu
- u tom slučaju ta promenljiva se može eliminisati
- $x \cdot y' \cdot z + x \cdot y' \cdot z' = x \cdot y'(z + z') = x \cdot y'$
- $x' \cdot y \cdot z + x' \cdot y \cdot z' = x' \cdot y$
- pa je: $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z' = x \cdot y' + x' \cdot y$
- znak 1 u 4 (ili 8, ili 2^n) susedne ćelije omogućava eliminisanje većeg broja promenljivih

Karnuovi dijagrami

- prisutnost znaka 1 u susednim ćelijama nekog Karnuovog dijagrama znači da su disjunktivnoj normalnoj formi izraza prisutna dva minterma koja se razlikuju samo u jednom literalu
- u tom slučaju ta promenljiva se može eliminisati
- $x \cdot y' \cdot z + x \cdot y' \cdot z' = x \cdot y'(z + z') = x \cdot y'$
- $x' \cdot y \cdot z + x' \cdot y \cdot z' = x' \cdot y$
- pa je: $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z' = x \cdot y' + x' \cdot y$
- znak 1 u 4 (ili 8, ili 2^n) susedne ćelije omogućava eliminisanje većeg broja promenljivih

Karnuovi dijagrami

- prisutnost znaka 1 u susednim ćelijama nekog Karnuovog dijagrama znači da su disjunktivnoj normalnoj formi izraza prisutna dva minterma koja se razlikuju samo u jednom literalu
- u tom slučaju ta promenljiva se može eliminisati
- $x \cdot y' \cdot z + x \cdot y' \cdot z' = x \cdot y'(z + z') = x \cdot y'$
- $x' \cdot y \cdot z + x' \cdot y \cdot z' = x' \cdot y$
- pa je: $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z' = x \cdot y' + x' \cdot y$
- znak 1 u 4 (ili 8, ili 2^n) susedne ćelije omogućava eliminisanje većeg broja promenljivih

Karnuovi dijagrami

- prisutnost znaka 1 u susednim ćelijama nekog Karnuovog dijagrama znači da su disjunktivnoj normalnoj formi izraza prisutna dva minterma koja se razlikuju samo u jednom literalu
- u tom slučaju ta promenljiva se može eliminisati
- $x \cdot y' \cdot z + x \cdot y' \cdot z' = x \cdot y'(z + z') = x \cdot y'$
- $x' \cdot y \cdot z + x' \cdot y \cdot z' = x' \cdot y$
- pa je: $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z' = x \cdot y' + x' \cdot y$
- znak 1 u 4 (ili 8, ili 2^n) susedne ćelije omogućava eliminisanje većeg broja promenljivih

Karnuovi dijagrami

- prisutnost znaka 1 u susednim ćelijama nekog Karnuovog dijagrama znači da su disjunktivnoj normalnoj formi izraza prisutna dva minterma koja se razlikuju samo u jednom literalu
- u tom slučaju ta promenljiva se može eliminisati
- $x \cdot y' \cdot z + x \cdot y' \cdot z' = x \cdot y'(z + z') = x \cdot y'$
- $x' \cdot y \cdot z + x' \cdot y \cdot z' = x' \cdot y$
- pa je: $x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y \cdot z + x' \cdot y \cdot z' = x \cdot y' + x' \cdot y$
- znak 1 u 4 (ili 8, ili 2^n) susedne ćelije omogućava eliminisanje većeg broja promenljivih

Karnuovi dijagrami - postupak

- odrediti izolovana polja u kojima je znak 1, odnosno polja koja sadrže, a njihovi susedi ne sadrže 1; mintermi koji im odgovaraju ne mogu biti eliminisani, ni skraćeni
- odrediti polja u kojima je znak 1, a koja imaju tačno jedno susedno polje u kome je takođe 1; 2 odgovarajuća minterma zamenjuju se jednim proizvodom literala koji je zajednički tim poljima,
- odrediti polja u kojima je znak 1, a koja na jedinstveni način formiraju blok od 4 susedna polja; 4 odgovarajuća minterma zamenjuju se jednim proizvodom literala koji je zajednički tim poljima, (postupak ponoviti za blokove od 8, 16, . . . , polja),
- za preostala polja koja sadrže 1 formirati najveće kvadratne blokove, tako da je tih blokova što manje a da su sva takva polja u njih uključena.

Moguće: isto polje je u sklopu različitih blokova. Nije problem: isti minterm se više puta pojavljuje u polaznom izrazu.

Karnuovi dijagrami

Example

Razmotrimo izraz:

$$x \cdot y \cdot z + x \cdot y' \cdot z + x \cdot y' \cdot z' + x' \cdot y' \cdot z' + x \cdot y \cdot z'$$

i njemu odgovarajući Karnuov dijagram:

	$y \cdot z$	$y' \cdot z$	$y' \cdot z'$	$y \cdot z'$
x	1	1	1	
x'			1	1

Karnuovi dijagrami

Nastavak primera:

- u dijagramu ne postoje izolovana polja u kojima je znak 1
- polja u kojima je znak 1, a koja imaju tačno jedno susedno polje u kome je takođe 1 su: $x \cdot y \cdot z$ (susedno je polje $x \cdot y' \cdot z$) i $x' \cdot y \cdot z'$ (susedno je polje $x' \cdot y' \cdot z'$)
- dobijaju se proizvodi: $x \cdot z$ i $x' \cdot z'$
- nema blokova od 4 susedna polja u kojima je 1
- razmatramo blokove od 2 susedna polja u kojima je 1

Karnuovi dijagrami

Nastavak primera (2):

- može se uraditi na dva načina:
  - to je blok polja $x \cdot y' \cdot z'$ i njemu susednog polja $x' \cdot y' \cdot z'$ ili
  - to je blok polja $x \cdot y' \cdot z'$ i njemu susednog polja $x \cdot y' \cdot z$.
- prvim izbor daje proizvod $y' \cdot z'$
- drug izbor daje $x \cdot y'$
- dve forme minimalnog izraza:
  - $x \cdot z + x' \cdot z' + y' \cdot z'$
  - $x \cdot z + x' \cdot z' + x \cdot y'$.

Izračunljivost

- Teorija izračunljivosti (tj. teorija algoritama)
- oblast nastala između 1930. i 1940. godine, pre razvoja digitalnih računara
- rezultat pretresanja osnova matematike zbog paradoksa koji su se pojavili krajem XIX i početkom XX veka.

Izračunljivost

- postavljalo se pitanje (*Entscheidungsproblem, problem odlučivanja*) da li postoji opšti postupak utvrđivanja istinitosti matematičkih iskaza
- vodi poreklo još od Leibnitz-a koji je u XVII veku, nakon uspešne konstrukcije mehaničke računske mašine, razmišljao o konstrukciji mašine koja bi mogla manipulisati simbolima i na taj način odrediti istinitost iskaza
- problem je aktuelizovao Hilbert, u poznatom predavanju na Kongresu matematičara održanom 1900
- odgovor - treba precizirati šta se podrazumeva pod postupkom mehaničkog izvođenja
- nezavisno jedan od drugog, Čerč i Tjuring su negativno odgovorili na ovo pitanje (jednakosti λ-izraza, halting problem)

Gottfried Wilhelm Leibnitz (Lajbnić), 1646 – 1716

Matematičar i filozof, verovatno slovenskog porekla. Jedan od kreatora diferencijalnog računa, mislilac koji je išao daleko ispred svog vremena. Nakon uspešne konstrukcije mehaničke računske mašine, razmišljao je o konstrukciji mašine koja bi mogla manipulisati simbolima jednog veštačkog univerzalnog jezika i na taj način odrediti istinitost iskaza.

D. Hilbert, 1862 – 1943, W. Ackermann, 1896 – 1962

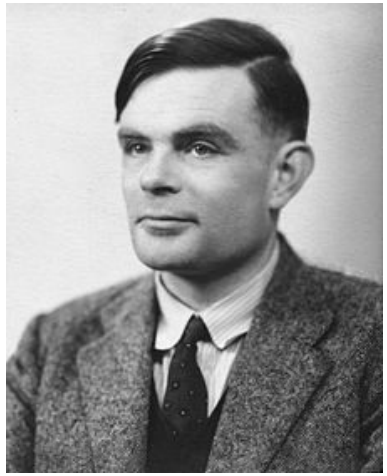
David Hilbert, nemački matematičar (levo). Smatra se da je jedan od najuticajnijih matematičara svih vremena. Wilhelm Friedrich Ackermann, nemački matematičar (desno). Sarađivao je sa Hilbertom u pisanju knjige *Grundzüge der theoretischen Logik*.

K. Gödel, 1906 – 1978, J. Herbrand, 1908 – 1931

Kurt Gödel, austrijski logičar (levo). Najpoznatiji je po rezultatima o esencijalnoj nepotpunosti aksiomatizacije Peanove aritmetike koji su imali dalekosežne posledice po razvoj ljudske misli. Uvršten je u listu 100 najznačajnijih ličnosti 20. veka koju je 1999. godine objavio magazin TIME.

Jacques Herbrand, francuski matematičar (desno). Dao je fundamentalne priloge u oblasti izračunljivih funkcija i logici. Poginuo na planinarenju.

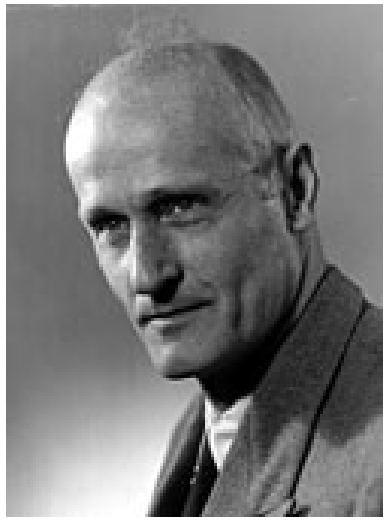
A. Church, 1903 –1995, A. Turing, 1912 – 1954



Alonzo Church, američki matematičar (levo). Najpoznatiji po doprinosima u logici i osnovama teorijskog računarstva. Uveo je λ-račun i formulisao čuvenu hipotezu nazvanu po njemu.

Alan Turing, engleski logičar (desno). Razvio ideje formalizacije koncepta izračunavanja, računara kao univeralne mašine, veštačke inteligencije. Tokom Drugog svetskog rata je rukovodio razbijanjem Enigma, razvio elektro-mehaničku mašinu Bombe 1940. godine, i dao osnovne ideje za prvi programibilni elektronski računar. Uvršten je u listu 100 najznačajnijih ličnosti 20. veka koju je 1999. godine objavio magazin TIME.

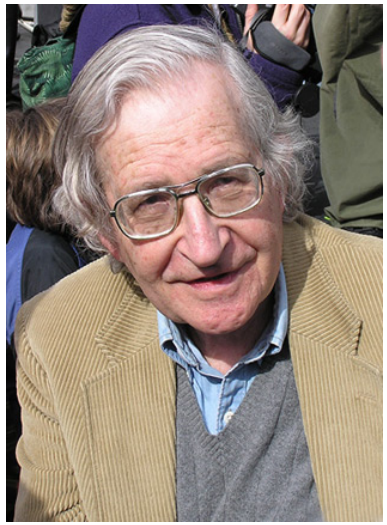
E. Post, 1897 – 1954, S. Kleene, 1909 – 1994



Emil Leon Post,matematičar poljskog porekla (levo). Najpoznatiji je po radu u oblasti teorije izračunljivost.

Stephen Kleene, američki matematičar (desno). Smatra se jednim od osnivača teorije rekurzivnih funkcija.

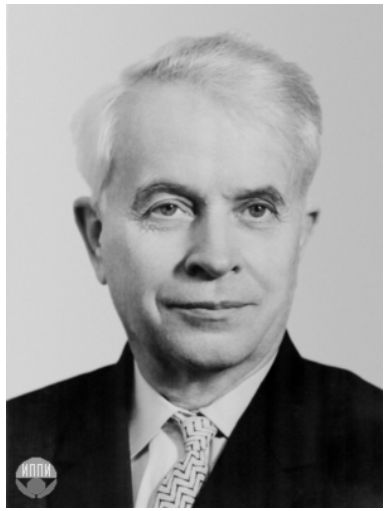
J. Nojman, 1903 – 1957, N. Čomski, 1928 –



János-a Neumann, John von Neumann, matematičar mađarskog porekla (levo). Jedan od najuticijnijih matematičara 20. veka. Radio u teoriji skupova, funkcionalnoj analizi, teoriji igara i ekonomiji, kao i u fizici, posebno u kvantnoj mehanici. Učesnik projekta Manhattan, savetnik u timu u koji je realizovao projekt EDVAC i autor izveštaja *First Draft of a Report on the EDVAC* iz 1945. godine u kome su data logička načela koje su u osnovi arhitekture i današnjih računara.

Avram Noam Chomsky (desno), čuveni liberalni mislilac i aktivista. Poznat je kao osnivač moderne lingvistike.

A. Markov, 1903 – 1979, J. Matijaševič, 1947 –



Андрей Андреевич Марков (levo), ruski matematičar. Jedan je od onivača ruske škole konstruktivne matematike.

Юрий Матиясевич (desno), ruski matematičar. Rešio deseti Hilbertov problem pokazavši da rešivost diofantskih jednačina nije odlučiva.

Algoritmi

- rešavanje problema razvojem algoritama i pisanjem programa je jedan od osnovnih zadataka u računarstvu
- matematičkim sredstvima proučavaju se i sami postupci rešavanja, algoritmi.
- formalni modeli izračunavanja, naizgled različiti, određuju jednu te istu klasu algoritama što navodi na tezu da ti modeli izračunavanja upravo određuju granice mogućnosti mehaničkog izračunavanja
- granice razdvajaju klase problema na one na za koje, u principu, postoji mogućnost programskog rešavanja i one za koje to nije slučaj

Intuitivni pojam algoritma

- postupak se opisuje konačnim nizom jednostavnih naredbi
- postoji idealna mašina (računar) koja izvršava te naredbe prema unapred utvrđenim pravilima,
- ta mašina započinje izračunavanje u nekom inicijalnom stanju; primenjena na ulazne podatke mašina izvršava naredbe u diskretnim koracima u kojima menja svoja stanja,
- izvršavanje svake naredbe se izvodi u konačnom vremenu pri čemu se koristi konačan memorijski prostor,
- izvršavanje naredbe je determinističko: iz jednog stanja izvršavanjem iste naredbe mašina uvek prelazi u isto stanje i
- prelaskom u završno stanje mašina prestaje sa izračunavanjem.

Intuitivni pojam algoritma

- determinisanost - mogućnost ponavljanja izvršavanja algoritama
- nedeterministički algoritmi
- ne zahteva se da se algoritam uvek završi, tj. da se rezultat uvek dobije u konačnom vremenu (finitnost),
- slično i sa zahtevom za ukupno memorijsko zauzeće
- algoritam predstavlja opis funkcije koja ulazne podatke preslikava u odgovor
- algoritamske (efektivne, izračunljive) funkcije

Algoritmi

- Za probleme za koje poznajemo postupke rešavanja lako utvrđujemo da jesu algoritamski rešivi.
- Šta ako nismo u stanju da damo rešenje?
- Da li je to samo posledica naše nesposobnosti, ili je reč o principijelnoj nemogućnosti?
- Potrebno je formalno precizirati pojmove algoritma.

Diofantske jednačine

- Problem postojanja efektivnog postupka za utvrđivanje da li proizvoljna diofantskih jednačina $p(x_1, \ldots, x_m) = 0$ ima nenegativna celobrojna rešenja
- $p(x_1, \ldots, x_m)$ je polinom sa celobrojnim koeficijentima i promenljivim $x_1, \ldots, x_m$
  $x_1^4 x_3 - 3x_2^5 + 6$
- nabrajanjem svih m-torki prirodnih brojeva i proverom da li predstavljaju nule polinoma bi se, pre ili posle, stiglo do rešenja jednačine, ako ono postoji
- neke jednačine ovog tipa ($x^2 - 2 = 0$), nemaju rešenja, prethodno opisani postupak se u takvim slučajevima ne bi nikada završio, zbog čega i ne predstavlja rešenje problema

Diofantske jednačine

- provera postojanja rešenja diofantskih jednačina je zapravo ekvivalentna formulacija desetog Hilbertovog problema
- svaki eventualni odgovor na ovo pitanje mora na neki način ponuditi i formalnu definiciju onoga što se podrazumeva pod efektivnim postupkom, bilo u smislu da ponuđeno rešenje potpada pod tu definiciju, bilo da ne postoji rešenje sa zahtevanim svojstvima
- formalna definicija efektivnog postupka pojavila se razvojem teorije izračunljivosti
- Jurij Matijaševič je 1970. godine sredstvima razvijenim u okviru te teorije negativno rešio sam problem

Formalni algoritamski sistemi

- Sistem izračunljivosti predstavljen u formalnom sistemu aritmetike je predložio Gödel između 1931. i 1934. godine, pri čemu se funkcija f smatra izračunljivom ako za svako m i n za koje je $f(m) = n$, u formalnom sistemu važi $\vdash f(m) = n$.
- Prikazivanje izračunljivih funkcija kao jedinstvenih rešenja sistema funkcionalnih jednačina je u istom periodu opisao takođe Gödel, a prema ideji Erbrana.
- λ-račun koji je razvio Čerč do 1936. godine je jednostavan formalni jezik za koji se definiše pojam redukcije koji predstavlja izračunavanje, a funkcija je izračunljiva ako se može opisati u jeziku.

Formalni algoritamski sistemi

Sistemi zasnovani na automatima formalizuju pojam algoritma opisujući idealne modele računara (neki sistemi su dati pre nastanka digitalnih računara):

- Tjuringova mašina (1936.)
- Postova mašina (1936.)
- Neograničena registarska mašina (URM, Shepherdson i Sturgis 1963.)

Formalni algoritamski sistemi

- Aritmetički opis zasnovao je Klini (generališe induktivne definicije)
- Sistemi produkcija (sistemi sa prezapisivanjem, Rewriting systems):
  - Postovi sistemi iz 1943. godine,
  - Markovljevi algoritmi uvedeni 1954. godine i
  - Gramatike Čomskog predložene 1956. godine,

  su jedna vrsta formalnih sistema u kojima se opisuju moguće transformacije jednih u druge reči na unapred fiskiranom alfabetu. Funkcije se opisuju kao skupovi parova reči (u, v) za koje postoji niz reči koje se dobijaju počev od u primenama pravila izvođenja i koji završava rečju v.
- *while*-programi su vrsta notacije proizašle iz ideja Goldstine-a i von Neumann-a o algoritamskim šemama kao formalizmu za prikazivanje izračunljivih funkcija. *while*-programi se sastoje samo od naredbi dodeljivanja, nizanja naredbi i *while*-naredbi.

Formalni algoritamski sistemi

- izvori inspiracije ovih sistema se međusobno značajno razlikuju
- pokazuje se da su sistemi međusobno ekvivalentni
- neuspeh pokušaja konstrukcije zadatka i postupka njegovog rešavanja koji ne potpadaju pod ove klasifikacije
- Čerčova teza: verovanje da je postignut nekakav apsolutni koncept i da se svi algoritmi mogu izraziti u svakom od ovih sistema

Formalni algoritamski sistemi

- izvori inspiracije ovih sistema se međusobno značajno razlikuju
- pokazuje se da su sistemi međusobno ekvivalentni
- neuspeh pokušaja konstrukcije zadatka i postupka njegovog rešavanja koji ne potpadaju pod ove klasifikacije
- Čerčova teza: verovanje da je postignut nekakav apsolutni koncept i da se svi algoritmi mogu izraziti u svakom od ovih sistema

Apstraktni model digitalnog računara

- celina sastavljena od procesora, memorije i ulazno-izlaznih uređaja
- procesor iz memorije pribavlja naredbe i podatke
- procesor vrši obradu u skladu sa značenjem naredbi
- dobijeni rezultati se vraćaju u memoriju
- preko ulazno-izlaznih uređaja podaci koji će biti obrađeni se unose u memoriju, odnosno iz memorije se preuzimaju rezultati obrade i prikazuju na odgovarajući način
- komunikacija delova računara se obavlja preko magistrala.

Tjuringova mašina

Tjuringova mašina je preteča ovakvog modela računara, pri čemu su neka svojstva idealizovana:

- memorija - potencijalno beskonačna
- u svakom koraku izračunavanja Tjuringove mašine zauzet je samo konačan broj memorijskih registara,
- ne postoji ograničenje koliki je taj konačan broj registara
- svakom koraku izračunavanja moguće je i zahtevati novi, do tada neiskorišteni memorijski registar i svaki takav zahtev se ispunjava

Tjuringova mašina

- Tjuringova mašina je restrikcija koncepta savremenog računara u smislu operacija koje je u stanju da izvršava, a koje su elementarne.
- Operacije su dovoljne za opisivanje proizvoljnih algoritama.
- Prednost u odnosu na bogatije programske jezike je upravo u jednostavnosti koja olakšava analizu.

Tjuringova mašina

Razmatraju se i slabije klase mašina koje su restrikcije druge vrste u odnosu na aktuelne računare:

- neki modeli nemaju memoriju (konačni automati - Finite automata)
- memorija je organizovana na poseban način (stek kod potisnih automata - Push-down automata),
- ulazno-izlazni podaci su ograničeni na reči,
- neki automati nemaju izlaz (konačni automati) itd.

Alfabet Tjuringove mašina

- svaki problem se izražava u nekom jeziku
- alfabet je skup znaka koji su nedeljive celine
- reč na nekom alfabetu je bilo koja konačna sekvenca znaka tog alfabeta
- sekvenca od nula znaka se naziva prazna reč
- reči se razdvajaju znakom blanko koji se ne smatra delom alfabeta već pomoćnim simbolom
- jezik je neki podskup skupa svih reči odgovarajućeg alfabeta
- t je podreč od q ako postoje, možda i prazne, reči u i v tako da je $q = utv$.
- obično je alfabet konačan skup znaka
- koristićemo unarni alfabet $A = \{1\}$
- blanko-znak (0)

Neformalni opis Tjuringove mašine

Tjuringova mašina se sastoji od:

- *trake* podeljene u ćelije, memorijske registre, koja se neograničeno pruža na levo i desno; broj ćelija (tj. dužina trake) je neograničen; sadržaj svake ćelije je ili znak 1 ili blanko znak (znak 0),
- *glave* koja se uvek nalazi nad tačno jednom ćelijom trake i može:
  - pročitati sadržaj ćelije nad kojom se nalazi i
  - upisati u ćeliju nad kojom se nalazi znak 1 ili 0 (blanko znak, tj. obrisati ćeliju) ili pomeriti se za jedan korak u levo ili u desno u odnosu na trenutnu poziciju,
- *indikatora stanja mašine*.

Neformalni opis Tjuringove mašine

- TM se u svakom trenutku nalazi u tačno jednom od konačno mnogo stanja koje se eventualno menja nakon svakog koraka izračunavanja.
- Skup svih stanja mašine označićemo sa $S = \{q_0, q_1, \ldots\}$.
- Izvršavanje mašine se izvodi pod dejstvom programa - konačan niz naredbi.
- Svaka naredba je četvorka oblika:
  $q_i \ s \ o \ q_j$
  gde su q_i i q_j neka stanja iz skupa S, s je znak nad kojim se nalazi glava mašine, a $o \in \{1, 0, L, R\}$ je oznaka operacije.

Neformalni opis Tjuringove mašine

- U svakom koraku rada mašina analizira stanje u kojem se nalazi i sadržaj ćelije nad kojom je glava, a zatim izvršava naredbu koja ima odgovarajuće vrednosti parametara q_i i s.
- Efekat izvršenja naredbe $q_i\ s\ o\ q_j$:
  - ako je $o = 1$, u ćeliju nad kojom se nalazi glava upisuje se znak 1,
  - ako je $o = 0$, u ćeliju nad kojom se nalazi glava upisuje se 0, tj. blanko znak,
  - ako je $o = L$, glava se pomera ulevo za jednu ćeliju i
  - ako je $o = R$, glava se pomera udesno za jednu ćeliju.
  - potom mašina menja stanje i prelazi u stanje q_j.

Neformalni opis Tjuringove mašine

Primeri determinističkih naredbi:

$q_5\ 0\ 1\ q_{17}$,

$q_1\ 0\ 0\ q_2$ i

$q_0\ 1\ L\ q_0$.

Primeri nedeterminističkih naredbi (q_i i s se poklapaju, a vrednosti parametara o i q_j se razlikuju):

$q_4\ 1\ 1\ q_5$ i

$q_4\ 1\ L\ q_2$

Neformalni opis Tjuringove mašine

Konvencije:

- Stanje $q_0 \in S$ - početno stanje
- Inicijalno, mašina se uvek nalazi u početnom stanju.
- Pri tome traka sadrži samo konačno mnogo ćelija u koje je upisan znak 1, dok sve ostale ćelije sadrže znak 0.
- Reč se na traci prikazuje kao neprekidan niz ćelija koje sadrže znak 1, a sa leve i desne strane tog niza se nalazi najmanje po jedan blanko znak (0).
- Po pravilu, na početku i na kraju izvršavanja glava mašine se nalazi iznad najlevlje ćelije koja sadrži znak 1.
- Skup stanja S proširićemo jednim novi stanjem q_z koje ne pripada do sada razmatranom skupu stanja.
- q_z - završno stanje; Kada se mašina nađe u stanju q_z ona prekida sa izvršavanjem.

Neformalni opis Tjuringove mašine

Definition

Pod *konfiguracijom* Tjuringove mašine podrazumevamo opis koji sadrži: opis sadržaja trake, položaj glave i stanje mašine. *Standardna konfiguracija* je konfiguracija u kojoj je:

- ili traka prazna (tj. sve ćelije sadrže blanko znak) ili sadrži najviše konačno mnogo nepraznih reči razdvojenih po jednim blanko znakom,
- glava mašine je iznad prve (gledano sa leva) ćelije trake koja sadrži znak 1 i
- ako počinje sa izvršavanjem, mašina se nalazi u početnom stanju q_0, a ako završava sa radom u završnom stanju q_z.

Programi - funkcije koje preslikavaju skup konfiguracija mašine u samog sebe.

Neformalni opis Tjuringove mašine

Na traci je jedna reč sastavljena od 1 (ostatak su 0) nad čijim krajnjim levim znakom se nalazi glava. Program dopisuje dva znaka 1 sa desne strane reči, glavu vraća na levo, na početak reči, pa staje:

$q_0\ 1\ R\ q_0$	glava se pomera udesno, na kraj reči
$q_0\ 0\ 1\ q_1$	na mestu prve 0 upisuje se 1
$q_1\ 1\ R\ q_2$	glava se pomera udesno
$q_2\ 0\ 1\ q_3$	na mestu druge 0 upisuje se 1
$q_3\ 1\ L\ q_3$	glava se pomera ulevo
$q_3\ 0\ R\ q_z$	do prve 0, ide udesno i zaustavlja se

$\ldots 01q_01000\ldots$
$\ldots 011q_0000\ldots$
$\ldots 0110q_000\ldots$
$\ldots 0111q_100\ldots$
$\ldots 01110q_20\ldots$
$\ldots 01111q_30\ldots$

$\ldots 0111q_310\ldots$
$\ldots 011q_3110\ldots$
$\ldots 01q_31110\ldots$
$\ldots 0q_311110\ldots$
$\ldots 01q_z1110\ldots$

Neformalni opis Tjuringove mašine

U opisu Tjuringove mašine ne kaže se šta se događa ako za sadržaj ćelije nad kojim se nalazi glava i tekuće stanje mašine u programu ne postoji odgovarajuća naredba.
Ovo odgovara 'zaglavljivanju' programa pisanih na standardnim programskim jezicima i može se formalizovati kompletiranjem programa naredbama koje u takvim situacijama ne menjaju ni stanje, ni poziciju glave, ni sadržaj ćelije nad kojom se glava nalazi. Ako u programu ne postoji naredba koja odgovara situaciji kada je mašina u stanju q_i, a sadržaj ćelije nad kojom se nalazi glava 0, možemo program proširiti naredbom koja predstavlja jednu beskonačnu petlju:

$q_i\ 0\ 0\ q_i$

Tjuringove mašine i funkcije

Tjuringove mašine se mogu iskoristiti kao algoritmi, tj. za izračunavanje funkcija koje preslikavaju prirodne brojeve u prirodne brojeve.

Tjuringove mašine i funkcije

Definition

Aritmetička funkcija je preslikavanje f za koje važi:

- domen preslikavanja, $Dom(f)$, je podskup skupa $\mathbb{N}^k$ $(k > 0)$ i
- kodomen preslikavanja, $Im(f)$, je podskup skupa $\mathbb{N}$.

Ako je za neki $k > 0$, $Dom(f) = \mathbb{N}^k$, f je *totalna funkcija*. Ako je $Dom(f) \subset \mathbb{N}^k$, za neki $k > 0$ i $Dom(f) \neq \mathbb{N}^k$, f je *parcijalna funkcija*.

Definition

Unarna reprezentacija prirodnog broja n u unarnom alfabetu $A = \{1\}$ je reč koja sadrži $n + 1$ znak 1.

Tjuringove mašine i funkcije

Definition

Neka je f aritmetička funkcija oblika $f : X \to \mathbb{N}$, gde je $X \subset \mathbb{N}$. Funkcija f je *Tjuring-izračunljiva* ako postoji program P za Tjuringovu mašinu tako da je za svaki $m \in X$:

- pre početka izvršavanja programa P Tjuringova mašina u standardnoj konfiguraciji, pri čemu je jedina reč zapisana na traci unarna reprezentacija broja m i
- po završetku rada programa P Tjuringova mašina u standardnoj konfiguraciji, pri čemu je jedina reč zapisana na traci unarna reprezentacija broja $f(m)$.

Program P tada *izračunava* funkciju f.

Analogno je moguće definisati k-arne aritmetičke Tjuring-izračunljive funkcije.

Tjuringove mašine i funkcije

Tjuring-izračunljive funkcije su parcijalne, odnosno ako se neki m ne nalazi u domenu Tjuring-izračunljive funkcije f, odgovarajući program P ne staje.

$q_0\ 0\ 0\ q_0$
$q_0\ 1\ 1\ q_0$

Program nikada ne staje, pa izračunava jedino funkciju čiji je domen prazan skup.

Tjuringove mašine i funkcije

- $P(x_1, x_2, \ldots, x_k) \downarrow y$ označava da program P polazeći od standardne konfiguracije u kojoj traka sadrži unarne reprezentacije prirodnih brojeva x_1, x_2, $\ldots$, x_k završava rad pri čemu se mašina nalazi u standardnoj konfiguraciji u kojoj traka sadrži unarnu reprezentaciju prirodnog broja y.
- $P(x_1, x_2, \ldots, x_k) \downarrow$ znači da je za neko y ispunjeno $P(x_1, x_2, \ldots, x_k) \downarrow y$.
- $P(x_1, x_2, \ldots, x_k) \uparrow$ znači da nije $P(x_1, x_2, \ldots, x_k) \downarrow$.

Definition

Program P *konvergira* za ulaz x_1, x_2, $\ldots$, x_k ako je ispunjeno $P(x_1, x_2, \ldots, x_k) \downarrow$. Program P *divergira* za ulaz x_1, x_2, $\ldots$, x_k ako je ispunjeno $P(x_1, x_2, \ldots, x_k) \uparrow$.

Tjuringove mašine i funkcije

Sledeći program izračunava funkciju $f(x) = 0$.

$q_0\ 1\ 0\ q_1$
$q_0\ 0\ 1\ q_z$
$q_1\ 0\ R\ q_0$

Sadržaj trake se briše, pri čemu se glava pomera na desno. Kada se naiđe na prvi znak 0, upisuje se znak 1 i završava rad. Dakle, $P(x) \downarrow 0$.

Tjuringove mašine i funkcije

Sledeći program izračunava funkciju naslednika prirodnog broja u nizu prirodnih brojeva, $f(x) = x'$.

$q_0\ 1\ L\ q_0$
$q_0\ 0\ 1\ q_z$

U programu se glava najpre pomera na levo, nakon čega se nalazi iznad ćelije koja sadrži znak 0. U tu ćeliju se upisuje znak 1 i prelazi u završno stanje. Dakle, $P(x) \downarrow x'$.

Tjuringove mašine i funkcije, $f(x_1, \ldots, x_k) = x_i$ (1)

Sledeći program za fiksirane k i i $(k \geq i \geq 1)$ izračunava funkciju koja se naziva i-ta projekcija, $f(x_1, \ldots, x_k) = x_i$.

$q_0\ 1\ 0\ q_1$	briše zapisa broja x_1
$q_0\ 0\ R\ q_2$	
$q_1\ 0\ R\ q_0$	
$\ldots$	
$q_j\ 1\ 0\ q_{j+1}$	briše zapisa broja x_{i-1}
$q_j\ 0\ R\ q_{j+2}$	
$q_{j+1}\ 0\ R\ q_j$	
$q_{j+2}\ 1\ R\ q_{j+2}$	prelazi zapis broja x_i
$q_{j+2}\ 0\ R\ q_{j+3}$	
$q_{j+3}\ 1\ 0\ q_{j+4}$	briše zapisa broja x_{i+1}
$q_{j+3}\ 0\ R\ q_{j+5}$	
$q_{j+4}\ 0\ R\ q_{j+3}$	
$\ldots$	

Tjuringove mašine i funkcije, $f(x_1, \ldots, x_k) = x_i$ (2)

$\ldots$

$q_l\ 1\ 0\ q_{l+1}$ briše zapisa broja x_k

$q_l\ 0\ L\ q_s$

$q_{l+1}\ 0\ R\ q_l$

$q_s\ 0\ L\ q_s$ vraća se na početak zapisa broja x_i

$q_s\ 1\ L\ q_{s+1}$

$q_{s+1}\ 1\ L\ q_{s+1}$

$q_{s+1}\ 0\ R\ q_z$

Tjuring-neizračunljive funkcije

Kako je svaki program konačan niz naredbi, a svaka naredba konačan niz simbola iz nekog prebrojivog skupa, to postoji samo prebrojivo mnogo programa. Kako svih aritmetičkih funkcija ima neprebrojivo mnogo, to znači da postoje funkcije koje nisu Tjuring-izračunljive.

Theorem

Tjuring-izračunljivih funkcija ima prebrojivo mnogo. Postoje funkcije koje nisu Tjuring-izračunljive.

Varijante Tjuringove mašine

- alfabet kojim se zapisuje sadržaj ćelija trake ne mora biti unarni,
- pored završnog stanja q_z uvode se i neka specijalna završna stanja, recimo q_{da} i q_{ne} koja, intuitivno, znače pozitivan, odnosno, negativan odgovor na postavljeni problem,
- dozvoljena je traka koja je beskonačna samo na jednu stranu, tj. postoji krajnja leva ćelija, dok se na desno traka pruža neograničeno,
- umesto samo jedne postoji više traka, a za svaku traku postoji posebna glava,
- nad jednom trakom postoji više glava umesto samo jedne,
- traka je dvodimenzionalna, a ne jednodimenzionalna, tj. traka podseća na beskonačnu šahovsku ploču,
- u jednoj naredbi mašine moguće je i upisati znak u ćeliju i pomerati glavu,
- ne važi zahtev za determinisanošću itd.

Varijante Tjuringove mašine

- Uglavnom, u smislu izračunljivosti gotovo sve od ovih varijanti Tjuringove mašine odgovaraju istoj klasi funkcija, tj. klasi Tjuring-izračunljivih funkcija, kao i osnovna verzija mašine.
- Izuzetak predstavljaju neki slabiji, restriktivni slučajevi: recimo, mašina čija traka je ograničena sa jedne strane i koristi unarni alfabet ili mašina koja ima samo dva stanja i koristi alfabet od dva znaka.
- Ekvivalencija varijanti Tjuringove mašine se dokazuje tako što se pokaže da za svaki program P za neku od varijanti Tjuringove mašine postoje programi za preostale varijante koji simuliraju izvršenje programa P i izračunavaju istu funkciju.

Tjuringova mašina sa bogatijim alfabetom

- reči bilo kog prebrojivog alfabeta se mogu prikazati pomoću unarnog alfabeta
- u većini slučajeva (mašine sa trakom koja nije ograničena ni sa jedne strane) alfabet može, zavisno od potrebe, slobodno određivati
- binarna, a ne kao do sada u unarnoj, reprezentacija prirodnih brojeva - ušteda (unarna reprezentacija prirodnih brojeva je eksponencijalno duža od binarne).

Tjuringova mašina sa trakom koja ima početak sa leve strane

- Alfabet sadrži još jedan specijalni znak, $\triangleright$
- služi da se prepozna početna ćelija sa leve strane
- preko $\triangleright$ se nikada ne prepisuje ni jedan drugi simbol, niti se glava sme pomeriti levo
- kada je $\triangleright$ u ćeliji ispod glave dozvoljene su jedino narede oblika $q_i \triangleright R\ q_j$

Tjuringova mašina sa više traka

- Za neki $k > 0$ Tjuringova mašina sa k traka sastoji se od traka označenih sa 1, 2, 3, . . . , k
- Sve trake imaju kraj sa leve strane, što nije ograničenje
- Nad svakom trakom nalazi se posebna glava
- U svakom koraku čita se tekuća ćelija na svakoj od traka i preduzima odgovarajuća akcija

  $q_i \ s_1 \ \ldots s_k \ o_1 \ \ldots o_k \ q_j$
- Na početku rada ulazni podaci su na prvoj traci, ostale trake su prazne
- Ako izvršavanje mašine shvatimo kao izračunavanje neke funkcije, rezultat se smešta u k-tu traku.

Tjuringova mašina sa više traka

Example

Da li je neka reč palindrom (čitanjem sa leva na desno i sa desna na levo se dobija isti niz znaka)?

- reč iz prve trake se iskopira na drugu traku
- glava prve trake se vrati na levo
- glava druge ostaje u krajnjoj desnoj poziciji
- dve glave se kreću u suprotnim smerovima i ispituju da li se nalaze nad jednakim znacima.

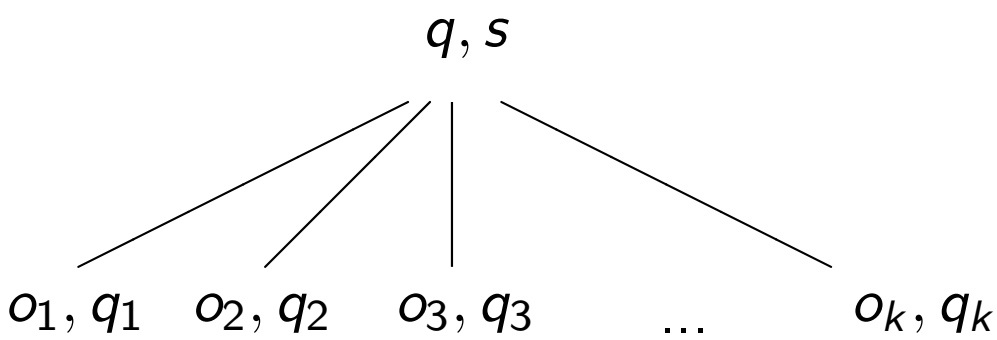
Tjuringova mašina sa više traka

Theorem

Za datu determinističu Tjuringovu mašinu M_1 sa k-traka može se konstruisati deterministička Tjuringova mašina M_2 sa jednom trakom koja simulira rad mašine M_1. Dužina rada mašine M_2 je ograničena polinomijalnom funkcijom dužine rada mašine M_1.

Nedeterministička Tjuringova mašina

- za tekuću konfiguraciju mašine može postojati više različitih konfiguracija do kojih se dolazi izvršavanjem neke od naredbi programa - mogućnost izbora
- grananje u drvetu je konačno - konačno mnogo opcija za izbor
- svaka grana - jedan mogući redosled rada



Nedeterministička Tjuringova mašina

- nedeterminističke mašine su pogodne za davanje odgovora 'da' ili 'ne' na pitanja oblika 'da li za ulazne podatke važi . . . ?'
- nova završna stanja: q_{da} i q_{ne}
- brzina nedeterminističkih je posledica asimetrične konvencije:
  - odgovor 'da' - bar jedno od mogućih izračunavanja završava u stanju q_{da},
  - odgovor 'ne' - sva izračunavanja završavaju u stanju q_{ne}
- ako ni jedno izračunavanje ne dovodi do stanja q_{da} i bar jedno izračunavanje ne dovodi ni do kog završnog stanja, nedeterministička mašina divergira.

Nedeterministička Tjuringova mašina

Model nedeterminističke mašine:

- višeprocesorski sistem
- u svakom koraku svaki od procesora kreira onoliko novih procesora koliko ima različitih konfiguracija u koje taj procesor može preći izvršavanjem tekuće naredbe
- ako mu bilo koji od potomaka vrati potvrdni odgovor, procesor tu informaciju šalje neposrednom pretku
- negativan odgovor se prosleđuje samo ako je dobijen od svih neposrednih potomaka
- svaki procesor izračunava disjunkciju odgovora svojih potomaka

Nedeterministička Tjuringova mašina

Example

Pretpostavimo da želimo ispitati da li je neki prirodan broj n složen ili prost. Običnom Tjuringovom mašinom problem bi se mogao rešiti na sledeći način: delili bismo broj svim prirodnim brojevima između 2 i $\frac{n}{2}$ i na osnovu toga dali odgovor. U slučaju nedeterminističke Tjuringove mašine na jednom mestu bismo imali mogućnost izbora broja kojim delimo broj n, pa ako je n složen, a izabrani broj delilac, mogli bismo dati odgovor u jednom koraku, što bi bio značajan dobitak u odnosu na deterministički postupak.

Nedeterministička Tjuringova mašina

Lako je uočiti da ovaj postupak nije realan, u smislu da izbor delioca podrazumeva da mi već znamo da je n složen, tj. da nam je poznat bar jedan njegov činilac. Međutim, i pored toga, nedeterministička Tjuringova mašina se može simulirati determinističkom mašinom, tako da se izražajnost u smislu onoga šta mašina može odgovoriti ne menja.

Nedeterministička Tjuringova mašina

M_1 nedeterministička TM, M_2 deterministička TM:

- M_2 sistematski prelazi sve moguće redoslede izvršavanja M_1
- najpre dužine 1, pa dužine 2 itd
- ni jedno moguće konačno izvršavanje neće biti preskočeno
- ako bi se M_1 u nekom trenutku našla u stanju q_{da}, to isto će pre ili posle biti slučaj i sa M_2
- ako sva izvršavanja M_1 dovode do stanja q_{ne}, i M_2 će se naći u tom stanju kada iscrpi sve mogućnosti
- ako M_1 divergira za date ulazne podatke ni M_2 se neće zaustaviti.

Nedeterministička Tjuringova mašina

- M_2 u najgorem slučaju bar jednom posećuje svaki čvor drveta koje prikazuje izvršavanje M_1
- čvorova drveta za M_1 može biti eksponencijalno više nego što je dužina najkraćeg mogućeg izračunavanja mašine M_1 koje dovodi do stanja q_{da}
- izvršavanje determinističke mašine M_2 u najgorem slučaju eksponencijalno duže nego izvršavanje nedeterminističke mašine M_1
- za sada nije poznato da li je simulaciju moguće izvesti uz samo polinomijalni gubitak vremena
- problem da li je $P = NP$

Nedeterministička Tjuringova mašina

Theorem

Za datu nedeterminističku Tjuringovu mašinu M_1 sa k-traka može se konstruisati deterministička Tjuringova mašina M_2 sa jednom trakom koja simulira rad mašine M_1. Dužina rada mašine M_2 je ograničena eksponencijalnom funkcijom dužine rada mašine M_1.

Za sada nije poznato da li je determinističku simulaciju rada nedeterminističkih mašina moguće izvesti u polinomijalnom vremenu.

Nedeterministička Tjuringova mašina

Theorem

Za datu nedeterminističku Tjuringovu mašinu M_1 sa k-traka može se konstruisati deterministička Tjuringova mašina M_2 sa jednom trakom koja simulira rad mašine M_1. Dužina rada mašine M_2 je ograničena eksponencijalnom funkcijom dužine rada mašine M_1.

Za sada nije poznato da li je determinističku simulaciju rada nedeterminističkih mašina moguće izvesti u polinomijalnom vremenu.

Univerzalna Tjuringova mašina *UTM*

- *UTM* primer programibilnog digitalnog računara opšte namene sa programom i podacima smeštenim u memoriju
- simulira izvršavanje ostalih Tjuringovih mašina
- ulazni podaci za *UTM* su opis - program neke posebne mašine i ulazni podaci te mašine,
- rezultat izvršavanja *UTM* je rezultat rada simulirane posebne mašine
- zamisao o postojanju ovakve mašine Tjuring je konkretizovao: napisao je njen program.

Univerzalna Tjuringova mašina *UTM*

Univerzalna logička povezanost pojmova programa, podataka i automata koji izvršava dati program nad odgovarajućim podacima, potpuno revolucionarna u to vreme, predstavlja temelj savremenog računarstva:

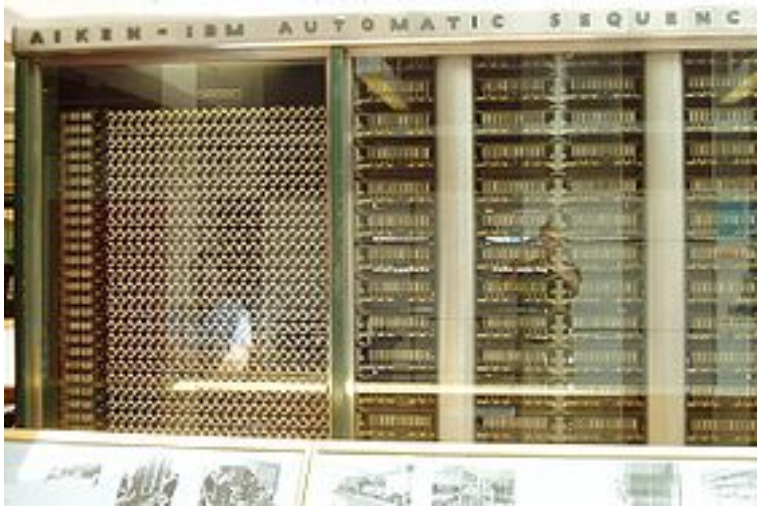
- "*. . . Smatrao bih kao najčudniju koincidenciju na koju sam ikada naišao ako bi se ispostavilo da se osnovna logika mašine dizajnirane za numeričko rešavanje diferencijalnih jednačina polkapa sa logikom mašine koja proizvodi račune u nekoj robnoj kući . . .*",
izjavio je 1956. godine Howard Aiken.

Univerzalna Tjuringova mašina *UTM*

Univerzalna logička povezanost pojmova programa, podataka i automata koji izvršava dati program nad odgovarajućim podacima, potpuno revolucionarna u to vreme, predstavlja temelj savremenog računarstva:

- "*. . . Smatrao bih kao najčudniju koincidenciju na koju sam ikada naišao ako bi se ispostavilo da se osnovna logika mašine dizajnirane za numeričko rešavanje diferencijalnih jednačina polkapa sa logikom mašine koja proizvodi račune u nekoj robnoj kući . . .*",
  izjavio je 1956. godine Howard Aiken.

Howard Aiken, 1900 – 1973



Howard Aiken, američki fizičar, jedan od pionira u konstrukciji računara, osnivač računarske laboratorije Univerziteta Harvard, konceptualni dizajner elektro-mehaničkog računara Automatic Sequence Controlled Calculator (kasnije nazvanog Harvard Mark I) 1944. godine.

Univerzalna Tjuringova mašina *UTM*

- "*. . . Vratimo se sada na analogiju sa teorijskim mašinama za izračunavanje . . . Može se pokazati da jedna specijalna mašina tog tipa može obavljati posao svih njih. U stvari, ona može raditi kao model bilo koje druge mašine. Ta specijalna mašina se može nazvati univerzalnom mašinom . . .*",
izjavio je 1947. godine Alan Turing na predavanju u Londonskom Matematičkom društvu.

Čerčova teza

svaki algoritam definiše funkciju koja
pripada jednoj dobro definisanoj klasi funkcija

(klasa Tjuring-izračunljivih funkcija, klasa parcijalno rekurzivnih funkcija, klasa λ-definabilnih funkcija ili neka druga ekvivalentna klasa), tj.klasa intuitivno izračunljivih funkcija se poklapa sa svakom od tih klasa

Čerčova teza

- intuitivni pojam algoritma je zasnovan na iskustvenom znanju o ljudskim umnim sposobnostima
- klase izračunljivih funkcija precizno definisane odgovarajućim formalnim modelima izračunavanja
- Čerčova teza izjednačava neformalni i formalni pristup pojmu efektivne izračunljivosti
- u strogom smislu nije matematičko tvrđenje (sličnija je formulacijama raznih fizičkih zakona)
- ne može se dokazati u okviru neke formalne teorije
- može biti opovrgnuta ako bi bila pronađena funkcija koja jeste intuitivno izračunljiva, a nije Tjuring-izračunljiva

Čerčova teza

- Argumenti u prilog tezi:
  - nema kontraprimera
  - međusobna ekvivalentnost raznorodnih formalnih modela izračunavanja do koje teško da bi došlo da neka od intuitivnih karakteristika algoritama nije njima obuhvaćena
- Čerčova teza se može prihvatiti i kao definicija izračunljivosti

Čerčova teza

Primene

- da bi se u raznim dokazima istakle suštinske ideje i izbegli tehnički detalji često se pribegava formulaciji oblika: 'funkcija je intuitivno izračunljiva, pa je prema Čerčovoj tezi formalno izračunljiva'
- argument pri objašnjavanju zašto neki problem nije rešiv: postupak za rešavanje problema se ne nalazi u nekoj od formalizovanih klasa izračunljivih funkcija, na osnovu Čerčove teze ne postoji efektivni postupak za rešavanje tog problema

Čerčova teza i praktična izračunljivost

- formalna izračunljivost = izračunljivost u principu
- praktična izračunljivost: ono što se stvarno može izračunati
- postoje formalno izračunljive funkcije za čije izračunavanje je potrebno vreme duže od vremena proteklog od nastanka kosmosa, i/ili se zahteva veći broj memorijskih registara nego što je broj atoma na Zemlji
- da li su takve funkcije zaista izračunljive
- Čerčova teza predstavlja korisnu granicu klase funkcija izvan koje sigurno nema praktično izračunljivih funkcija

Odlučivost

- razlog uvođenja formalnih modela izračunavanja: utvrđivanje da li za neki problem postoji algoritam koji ga rešava
- Čerčova teza i definicije Tjuring-izračunljivih (parcijalno rekurzivnih funkcija, ...) određuju jasnu granicu dosega algoritama
- problemi se obično formulišu sa 'da li je ...' ili 'da li važi ...'
- ako smo u stanju da na takvo pitanje uvek odgovorimo problem je rešiv (odlučiv)
- probleme možemo shvatiti kao predikate (skupove)

Odlučivost

- predikat (relacija, skup, problem) je podskup od $\mathbb{N}^n$ za neko $n > 0$
- karakteristična funkcija predikata za k-torku argumenata ima vrednost 1 ako za tu k-torku predikat važi, inače je vrednost funkcije 0

Definition

Predikat (skup) R je *rekurzivan (odlučiv)* ako je njegova karakteristična funkcija $C_R(x_1, \ldots, x_n)$:

$$C_R(x_1, \ldots, x_n) = \begin{cases} 1 & \text{ako važi } R(x_1, \ldots, x_n) \\ 0 & \text{ako ne važi } R(x_1, \ldots, x_n) \end{cases}$$

totalna Tjuring izračunljiva funkcija, inače je *neodlučiv*.

Odlučivost

- predikat (relacija, skup, problem) je podskup od $\mathbb{N}^n$ za neko $n > 0$
- karakteristična funkcija predikata za k-torku argumenata ima vrednost 1 ako za tu k-torku predikat važi, inače je vrednost funkcije 0

Definition

Predikat (skup) R je *rekurzivan (odlučiv)* ako je njegova karakteristična funkcija $C_R(x_1, \ldots, x_n)$:

$$C_R(x_1, \ldots, x_n) = \begin{cases} 1 & \text{ako važi } R(x_1, \ldots, x_n) \\ 0 & \text{ako ne važi } R(x_1, \ldots, x_n) \end{cases}$$

totalna Tjuring izračunljiva funkcija, inače je *neodlučiv*.

Odlučivost

Primeri odlučivih skupova:

- skup $\mathbb{N}$
- svaki konačan podskup od $\mathbb{N}$
  - za konačan skup $\{a_1, \ldots, a_n\}$ prirodnih brojeva karakteristična funkcija $x = a_1 \vee \ldots \vee x = a_n$ je rekurzivna
- skup parnih brojeva
- skup neparnih brojeva
- klasa odlučivih skupova (predikata) je zatvorena za osnovne operacije komplementiranja (u odnosu na skup $\mathbb{N}^k$), $\cup$, $\cap$, $\setminus$ (iz razmatranja karakterističnih funkcija za skupove dobijene tim operacijama)
- odlučivost je izuzetak, neodlučivi problemi su mnogo prisutniji

Odlučivost

Primeri odlučivih skupova:

- skup $\mathbb{N}$
- svaki konačan podskup od $\mathbb{N}$
  - za konačan skup $\{a_1, \ldots, a_n\}$ prirodnih brojeva karakteristična funkcija $x = a_1 \vee \ldots \vee x = a_n$ je rekurzivna
- skup parnih brojeva
- skup neparnih brojeva
- klasa odlučivih skupova (predikata) je zatvorena za osnovne operacije komplementiranja (u odnosu na skup $\mathbb{N}^k$), $\cup$, $\cap$, $\setminus$ (iz razmatranja karakterističnih funkcija za skupove dobijene tim operacijama)
- odlučivost je izuzetak, neodlučivi problemi su mnogo prisutniji

Neodlučivi predikati

- problem zaustavljanja - da li proizvoljna Tjuringova mašina za proizvoljan ulaz završava rad u konačno mnogo koraka,
- da li je proizvoljna Tjuring-izračunljiva funkcija totalna,
- da li su dve proizvoljne Tjuring-izračunljive funkcije jednake,
- problem reči za grupe, tj. ako je grupa G sa jediničnim elementom e generisana skupom elemenata $Gen_G = \{g_1, g_2, \ldots\}$, da li za proizvoljan izraz t_1 sastavljan od elemenata iz Gen_G (recimo $t_1 = g_2^3 g_1^{-1} g_5$) važi $t_1 = e$,

Neodlučivi predikati

- rešivost diofantskih jednačina,
- problemi zadovoljivosti i valjanosti formula predikatskog računa prvog reda,
- problem pokrivanja (tiling problem) ravni u kome je dat konačan broj proizvoljnih oblika poligona, a postavlja se pitanje da li je moguće u potpunosti, bez preklapanja, pokriti ravan poligonima samo tih oblika itd.
- Peanova aritmetika, teorija grupa, teorija prstena, teorija polja, ZF teorija skupova itd.

Neodlučivi predikati

Svi netrivijalni skupovi Tjuring-izračunljivih funkcija su neodlučivi:

Theorem (Rajsova teorema)

Neka je $\mathbb{B}$ neprazna prava potklasa klase svih Tjuring-izračunljivih funkcija. Problem da li proizvoljna Tjuring-izračunljiva funkcija pripada $\mathbb{B}$ nije odlučiv.

Neodlučivi predikati

Na osnovu Rajsove teoreme neodlučivi problemi su:

- domen funkcije je konačan,
- domen funkcije je beskonačan,
- kodomen funkcije je konačan i
- kodomen funkcije je beskonačan.

Parcijalno odlučivi predikati

Definition

Predikat (odnosno skup ili problem) R je *parcijalno odlučiv* (*rekurzivno nabrojiv*) ako je njegova karakteristična funkcija oblika

$$C_R(x_1, \ldots, x_n) = \begin{cases} 1 & \text{ako važi } R(x_1, \ldots, x_n) \\ \text{nedefinisano} & \text{inače.} \end{cases}$$

parcijalna Tjuring-izračunljiva[a] funkcija.

[a] Ova definicija se može oslabiti tako što se dozvoli da za neke, ali ne nužno sve, $x_1, \ldots, x_n$ za koje $R(x_1, \ldots, x_n)$ ne važi, bude $C_R(x_1, \ldots, x_n) = 0$.

Parcijalno odlučivi predikati

Dokazuje se:

- Predikat P je parcijalno odlučiv ako i samo ako postoji parcijalna Tjuring-izračunljiva funkcija f čiji je domen P.
- Predikat $P(x_1, \ldots, x_n)$ je parcijalno odlučiv ako i samo ako postoji odlučiv predikat $R(x_1, \ldots, x_n, y)$ tako da važi $P(x_1, \ldots, x_n)$ ako i samo ako važi $(\exists y)R(x_1, \ldots, x_n, y)$.

Parcijalno odlučivi predikati

- Predikat P je odlučiv ako i samo ako su predikati P i $\mathbb{C}P$ parcijalno odlučivi
- predikat $P(x)$ je parcijalno odlučiv ako postoji program koji odgovara potvrdno u slučaju da predikat važi za argumente programa, inače program ne mora da se zaustavi
- ako bi postojali takvi programi $Prog_P$ za predikat P i $Prog_{\mathbb{C}P}$ za njegov komplement $\mathbb{C}P$, mogli bismo na dva računara da ih pokrenemo paralelno; pošto za svaki x važi ili $P(x)$ ili $\mathbb{C}P(x)$ jedan od programa će se posle izvesnog vremena zaustaviti. Ako se zaustavi program $Prog_P$ odgovor bi bio 'važi $P(x)$', a ako se zaustavi program $Prog_{\mathbb{C}P}$ odgovor bi bio 'ne važi $P(x)$', pa bi predikat P bio odlučiv.

Parcijalno odlučivi predikati

- Predikat P je odlučiv ako i samo ako su predikati P i $\mathbb{C}P$ parcijalno odlučivi
- predikat $P(x)$ je parcijalno odlučiv ako postoji program koji odgovara potvrdno u slučaju da predikat važi za argumente programa, inače program ne mora da se zaustavi
- ako bi postojali takvi programi $Prog_P$ za predikat P i $Prog_{\mathbb{C}P}$ za njegov komplement $\mathbb{C}P$, mogli bismo na dva računara da ih pokrenemo paralelno; pošto za svaki x važi ili $P(x)$ ili $\mathbb{C}P(x)$ jedan od programa će se posle izvesnog vremena zaustaviti. Ako se zaustavi program $Prog_P$ odgovor bi bio 'važi $P(x)$', a ako se zaustavi program $Prog_{\mathbb{C}P}$ odgovor bi bio 'ne važi $P(x)$', pa bi predikat P bio odlučiv.

Parcijalno odlučivi predikati

- Predikat P je odlučiv ako i samo ako su predikati P i $\mathbb{C}P$ parcijalno odlučivi
- predikat $P(x)$ je parcijalno odlučiv ako postoji program koji odgovara potvrdno u slučaju da predikat važi za argumente programa, inače program ne mora da se zaustavi
- ako bi postojali takvi programi $Prog_P$ za predikat P i $Prog_{\mathbb{C}P}$ za njegov komplement $\mathbb{C}P$, mogli bismo na dva računara da ih pokrenemo paralelno; pošto za svaki x važi ili $P(x)$ ili $\mathbb{C}P(x)$ jedan od programa će se posle izvesnog vremena zaustaviti. Ako se zaustavi program $Prog_P$ odgovor bi bio 'važi $P(x)$', a ako se zaustavi program $Prog_{\mathbb{C}P}$ odgovor bi bio 'ne važi $P(x)$', pa bi predikat P bio odlučiv.

Parcijalno odlučivi predikati

Primeri:

- problem zaustavljanja proizvoljne Tjuringova mašina za proizvoljan ulaz
- rešivost diofantskih jednačina (Matijaševič je pokazao da su svi parcijalno odlučivi predikati ekvivalentni problemima rešavanja nekih diofantskih jednačina, pa taj problem nije odlučiv)
- komplementi ovih problema nisu ni odlučivi, ni parcijalno odlučivi jer bi u suprotnom svi problemi bili odlučivi
- problem da li je proizvoljna Tjuring-izračunljiva funkcija totalna nije parcijalno odlučiv
- postoji hijerarhija skupova prirodnih brojeva koja se naziva *aritmetička hijerarhija* tako da su skupovi na višim nivoima u nekom smislu više neodlučivi od skupova sa nižih nivoa

Parcijalno odlučivi predikati

Primeri:

- problem zaustavljanja proizvoljne Tjuringova mašina za proizvoljan ulaz
- rešivost diofantskih jednačina (Matijaševič je pokazao da su svi parcijalno odlučivi predikati ekvivalentni problemima rešavanja nekih diofantskih jednačina, pa taj problem nije odlučiv)
- komplementi ovih problema nisu ni odlučivi, ni parcijalno odlučivi jer bi u suprotnom svi problemi bili odlučivi
- problem da li je proizvoljna Tjuring-izračunljiva funkcija totalna nije parcijalno odlučiv
- postoji hijerarhija skupova prirodnih brojeva koja se naziva *aritmetička hijerarhija* tako da su skupovi na višim nivoima u nekom smislu više neodlučivi od skupova sa nižih nivoa

Parcijalno odlučivi predikati

Primeri:

- problem zaustavljanja proizvoljne Tjuringova mašina za proizvoljan ulaz
- rešivost diofantskih jednačina (Matijaševič je pokazao da su svi parcijalno odlučivi predikati ekvivalentni problemima rešavanja nekih diofantskih jednačina, pa taj problem nije odlučiv)
- komplementi ovih problema nisu ni odlučivi, ni parcijalno odlučivi jer bi u suprotnom svi problemi bili odlučivi
- problem da li je proizvoljna Tjuring-izračunljiva funkcija totalna nije parcijalno odlučiv
- postoji hijerarhija skupova prirodnih brojeva koja se naziva *aritmetička hijerarhija* tako da su skupovi na višim nivoima u nekom smislu više neodlučivi od skupova sa nižih nivoa

Parcijalno odlučivi predikati

Primeri:

- problem zaustavljanja proizvoljne Tjuringova mašina za proizvoljan ulaz
- rešivost diofantskih jednačina (Matijaševič je pokazao da su svi parcijalno odlučivi predikati ekvivalentni problemima rešavanja nekih diofantskih jednačina, pa taj problem nije odlučiv)
- komplementi ovih problema nisu ni odlučivi, ni parcijalno odlučivi jer bi u suprotnom svi problemi bili odlučivi
- problem da li je proizvoljna Tjuring-izračunljiva funkcija totalna nije parcijalno odlučiv
- postoji hijerarhija skupova prirodnih brojeva koja se naziva *aritmetička hijerarhija* tako da su skupovi na višim nivoima u nekom smislu više neodlučivi od skupova sa nižih nivoa

Složenost izračunavanja

- razmatramo samo odlučive probleme
- postoji razlika između praktično izračunljivih funkcija i funkcija koje se mogu izračunati u principu
- praktična izračunljivost - dužina rada odgovarajućih programa limitirana nekim stepenom dužine ulaznih podataka
- problemi koji nisu praktično izračunljivi se rešavaju heuristički
- generisanje teških problema za potrebe informacione bezbednosti

Složenost izračunavanja

- predstavljen je jedan od pristupa klasifikaciji složenosti
- meri se računarskim resursima - vreme i memorijsko zauzeće
- daje se elegentna hijerarhije problema koja pruža argumente da se sa velikom pravom veruje da su neki problemi jako teški za izračunavanje, mada to, možda nismo u stanju da precizno dokažemo
- nije u potpunosti odgovoreno na pitanja koliko su i zašto neki zadaci teški
- granica između praktično izračunljivih i praktično neizračunljivih problema nije precizno određena

Složenost izračunavanja

- problem zadovoljivosti iskaznih formula u izvesnom smislu reprezent klase praktično neizračunljivih problema
- veruje se da ovaj problem ne pripada klasi praktično izračunljivih problema (problem $P = NP$?)
- ako bi se dokazalo da problem zadovoljivosti ipak praktično izračunljiv, onda bi granica koja razdvaja praktično izračunljive od praktično neizračunljivih problema morala biti znatno podignuta

Formalni model i opis problema

- Tjuringove mašine sa više traka ograničenih sa leve strane (determinističke ili nedeterminističke)
- (najčešće) binarni alfabet
- posebna završna stanja: q_{da}, q_{ne} pozitivan, negativan odgovor na pitanje
- mašina sa jednom trakom može simulirati ove tipove - ne povećava se izražajnost u odnosu na osnovni model
- Tjuringove mašine sa ulazom i izlazom ((ne)determinističke)
  - prva traka se može samo čitati,
  - u poslednju traku se može samo upisivati (glava poslednje trake ne sme ići ulevo)
  - meri se memorijsko zauzeće preostalih (radnih) traka

Formalni model i opis problema

- Tjuringove mašine sa više traka ograničenih sa leve strane (determinističke ili nedeterminističke)
- (najčešće) binarni alfabet
- posebna završna stanja: q_{da}, q_{ne} pozitivan, negativan odgovor na pitanje
- mašina sa jednom trakom može simulirati ove tipove - ne povećava se izražajnost u odnosu na osnovni model
- Tjuringove mašine sa ulazom i izlazom ((ne)determinističke)
  - prva traka se može samo čitati,
  - u poslednju traku se može samo upisivati (glava poslednje trake ne sme ići ulevo)
  - meri se memorijsko zauzeće preostalih (radnih) traka

Formalni model i opis problema

- koncept nedeterminističke mašine je nerealističan u smislu realizacije na nekom od stvarnih računara
- koristan u određivanju granica složenosti izračunavanja
- postoje problemi koji se elegantno rešavaju nedeterminističkim a veoma teško determinističkim mašinama

Formalni model i opis problema

- problemi koji se analiziraju u teoriji složenosti izračunavanja karakterišu se pitanjima na koja se obično odgovara sa "da" ili "ne"
- predstavljanje problema se vrši u nekom formalnom jeziku

Definition

Problem L za koji se ispituje složenost je podskup skupa svih reči nekog alfabeta (jezik na nekom alfabetu).
Komplement problema L, u oznaci $\overline{L}$ na nekom alfabetu je skup svih reči na tom alfabetu koje nisu u L.

Formalni model i opis problema

- problemi koji se analiziraju u teoriji složenosti izračunavanja karakterišu se pitanjima na koja se obično odgovara sa "da" ili "ne"
- predstavljanje problema se vrši u nekom formalnom jeziku

Definition

Problem L za koji se ispituje složenost je podskup skupa svih reči nekog alfabeta (jezik na nekom alfabetu).
Komplement problema L, u oznaci $\overline{L}$ na nekom alfabetu je skup svih reči na tom alfabetu koje nisu u L.

Formalni model i opis problema

- Tjuringova mašina prihvata ulazni podatak (reč x) ako postoji izračunavanje u kome se, polazeći od reči x na ulaznoj traci u početnom stanju q_0, dolazi do završnog stanja q_{da}
- Tjuringova mašina odbacuje x ako uvek dolazi do završnog stanja q_{ne}
- Ako Tjuringova mašina M prihvata sve reči x jezika L koji opisuje problemu, a odbacuje svaku reč koja nije u L, kaže se da M odlučuje problem (jezik) L
- Ako je $\overline{L}$ komplement problema L, onda je za svaki primerak x problema odgovor na pitanje da li je $\overline{L}(x)$ pozitivan, odnosno negativan, ako i samo ako je odgovor na pitanje $L(x)$ negativan, odnosno pozitivan

Formalni model i opis problema

- Tjuringova mašina prihvata ulazni podatak (reč x) ako postoji izračunavanje u kome se, polazeći od reči x na ulaznoj traci u početnom stanju q_0, dolazi do završnog stanja q_{da}
- Tjuringova mašina odbacuje x ako uvek dolazi do završnog stanja q_{ne}
- Ako Tjuringova mašina M prihvata sve reči x jezika L koji opisuje problemu, a odbacuje svaku reč koja nije u L, kaže se da M odlučuje problem (jezik) L
- Ako je $\overline{L}$ komplement problema L, onda je za svaki primerak x problema odgovor na pitanje da li je $\overline{L}(x)$ pozitivan, odnosno negativan, ako i samo ako je odgovor na pitanje $L(x)$ negativan, odnosno pozitivan

Formalni model i opis problema

Example

Neka je L problem ispitivanja povezanosti dva čvora grafa i x opis nekog grafa i njegova dva izabrana čvora.
Graf (bez izolovanih čvorova) se može prikazati kao niz ivica, odnosno niz uređenih parova čvorova, elementi konačnog skupa se prikazuju kao prirodni brojevi koji se opet prikazuju u binarnom obliku itd.
Tada je $L(x)$ primerak problema L u kome se ispituje da li su u grafu opisanom sa x povezani izabrani čvorovi.

Example

Komplement problema ispitivanja zadovoljivosti formule je ispitivanje nezadovoljivosti formule.

Formalni model i opis problema

Example

Neka je L problem ispitivanja povezanosti dva čvora grafa i x opis nekog grafa i njegova dva izabrana čvora.
Graf (bez izolovanih čvorova) se može prikazati kao niz ivica, odnosno niz uređenih parova čvorova, elementi konačnog skupa se prikazuju kao prirodni brojevi koji se opet prikazuju u binarnom obliku itd.
Tada je $L(x)$ primerak problema L u kome se ispituje da li su u grafu opisanom sa x povezani izabrani čvorovi.

Example

Komplement problema ispitivanja zadovoljivosti formule je ispitivanje nezadovoljivosti formule.

O-notacija

- u teoriji složenosti izračunavanja se razmatra brzina rasta nekih funkcija
- brzina rasta se analizira asimptotski, pri čemu se često koriste različite aproksimacije

O-notacija

Definition

Neka su f i g aritmetičke funkcije. Tada je *funkcija f u velikom O od g*[a], u oznaci $f(x) = O(g(x))$, ako:

- postoje brojevi c i n takvi da za svaki $x > n$ važi $f(x) \leq c \cdot g(x)$

Ako takvi brojevi ne postoje, onda je $f(x) \neq O(g(x))$, f *raste brže* od funkcije g.

Funkcije f i g *rastu istom brzinom*, $f(x) = \Theta(g(x))$, ako važi $f(x) = O(g(x))$ i $g(x) = O(f(x))$.

[a] f je reda funkcije g, g je asimptotska gornja granica za f.

O-notacija

Definition

Neka su f i g aritmetičke funkcije. Tada je *funkcija f u velikom O od g*[a], u oznaci $f(x) = O(g(x))$, ako:

- postoje brojevi c i n takvi da za svaki $x > n$ važi $f(x) \leq c \cdot g(x)$

Ako takvi brojevi ne postoje, onda je $f(x) \neq O(g(x))$, f *raste brže* od funkcije g.
Funkcije f i g *rastu istom brzinom*, $f(x) = \Theta(g(x))$, ako važi $f(x) = O(g(x))$ i $g(x) = O(f(x))$.

[a] f je reda funkcije g, g je asimptotska gornja granica za f.

O-notacija

Example

- funkcije n^4 i $1345 \cdot n^4 + 2007 \cdot n^3 - 7n + 5$ rastu istom brzinom
- funkcija $0.0001 \cdot n^5$ raste brže od funkcije $1345 \cdot n^4 + 2007 \cdot n^3 - 7n + 5$

O-notacija

Theorem

Neka su f i g aritmetičke funkcije i neka je

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \beta.$$

Ako je β:

- *pozitivan realan broj, onda funkcije f i g rastu istom brzinom*
- *∞, onda važi $g(x) = O(f(x))$ i $f(x) \neq O(g(x))$, tj. funkcija f raste brže od g*

O-notacija

Theorem

Neka je $P(n) = a_0 + a_1 \cdot n + \ldots + a_r \cdot n^r$, $a_r \neq 0$, *polinom stepena* r *sa celobrojim koeficijentima. Tada za* $P(n)$ *i* n^m *važi:*

1. *ako je* $m = r$, $P(n)$ *i* n^m *rastu istom brzinom,*
2. *ako je* $m < r$, $P(n)$ *raste brže od* n^m *i*
3. *ako je* $m > r$, n^m *raste brže od* $P(n)$.

O-notacija

Theorem

Neka je $k > 1$. Funkcije k^n raste brže od bilo kog polinoma sa celobrojnim koeficijentima. Svaki polinom sa celobrojnim koeficijentima raste brže od bilo koje logaritamske funkcije.

O-notacija

Theorem

Za svake dve realne konstante $c, d > 1$ *važi* $\log_c(x) = \Theta(\log_d(x))$, *tj. funkcije* $\log_c(x)$ *i* $\log_d(x)$ *rastu istom brzinom.*

O-notacija

- Funkcije koje se obično javljaju u O-notaciji prilikom analize složenosti su: $\log_2 n$, linearna funkcija $k \cdot n$, njihov proizvod $n \log_2 n$, stepena funkcija n^k, eksponencijalna funkcija k^n
- $\lim_{n\to\infty} f(n) = \infty$ (za problem većih dimenzija složenost izračunavanja je veća),
- funkcije su neopadajuće i
- postoje Tjuringove mašine koje ih izračunavaju u prostoru i vremenu koji su proporcionalni vrednostima funkcija.
- *prave funkcije složenosti*

O-notacija

- Funkcije koje se obično javljaju u O-notaciji prilikom analize složenosti su: $\log_2 n$, linearna funkcija $k \cdot n$, njihov proizvod $n \log_2 n$, stepena funkcija n^k, eksponencijalna funkcija k^n
- $\lim_{n\to\infty} f(n) = \infty$ (za problem većih dimenzija složenost izračunavanja je veća),
- funkcije su neopadajuće i
- postoje Tjuringove mašine koje ih izračunavaju u prostoru i vremenu koji su proporcionalni vrednostima funkcija.
- *prave funkcije složenosti*

Klase složenosti

- mere složenosti:
  - vreme, tj. broj koraka izvršavanja programa,
  - količinu memorije koju koristi program
- složenost se izražava kao funkcija veličine $|x|$ ulaznog podatka x
  - ulazni podatak opis grafa, pogodno je da $|x|$ bude broj čvorova grafa
  - ako je ulazni podatak reč, $|x|$ označava dužinu, tj. broj znakova reči

Klase složenosti

Definition

- *Vreme izvršavanja* izračunavanja Tjuringove mašine M koja kao ulaz dobija podatak x jednako je dužini niza konfiguracija koje predstavljaju to izračunavanje.
- Neka je f prava funkcija složenosti. Tjuringova mašina M radi *u vremenu* $f(n)$, ako je za bilo koji ulazni podatak x vreme izvršavanja bilo kog izračunavanja mašine najviše $f(|x|)$.
- Funkcija f je *vremenska granica složenosti* za M.
- $TIME(f(n))$ je skup problema za koje postoje determinističke Tjuringove mašine koje ih odlučuju, a za koje je vremenska granica složenosti $f(n)$. $NTIME(f(n))$ se definiše analogno, u odnosu na nedeterminističke Tjuringove mašine.

Klase složenosti

Definition

- *Prostor izvršavanja* izračunavanja Tjuringove mašine M sa ulazom i izlazom koja kao ulaz dobija podatak x jednak je broju različitih ćelija traka, sem prve - ulazne i poslednje - izlazne trake, nad kojima se tokom izračunavanje nađu glave traka.
- Neka je f unarna aritmetička funkcija koja zadovoljava uslove za pravu funkciju složenosti. Tjuringova mašina M radi *u prostoru* $f(n)$, ako je za bilo koji ulazni podatak x prostor izvršavanja bilo kog izračunavanja mašine najviše $f(|x|)$. Funkcija f je *prostorna granica složenosti* za M.
- $SPACE(f(n))$ je skup problema za koje postoje determinističke Tjuringove mašine koje ih odlučuju, a za koje je prostorna granica složenosti $f(n)$. Skup problema $NSPACE(f(n))$ se definiše analogno, u odnosu na nedeterminističke Tjuringove mašine.

Klase složenosti

- izbegava se uključivanje prostora u koji je upisan ulazni podatak, odnosno u koji se smešta rezultat, u razmatranje prostorne složenosti
- razmatranje mašina koje koriste manje od $|x|$, recimo $\log_2 |x|$, ćelija, gde se pod korištenjem podrazumeva da su te ćelije radni prostor, odnosno da se u njih privremeno smeštaju podaci koji se upotrebljavaju tokom izračunavanja

Klase složenosti

Example

Neka je M mašina sa ulazom i izlazom koja sadrži četiri trake i ispituje da li je ulazna reč palindrom:

- prva traka sadrži ulaznu reč
- druga traka sadrži binarni zapis indeksa i koji označava redni broj ciklusa rada, treća binarni zapis indeksa j, dok se četvrta traka ne koristi

Klase složenosti

Nastavak primera:

- na početku rada indeks i se postavlja na 1, a zatim se rad obavlja u ciklusima:
  - $j = 1$, postavlja se glava prve trake nad najlevlju ćeliju ulazne reči
  - ako je $j < i$, uvećava se j za 1 i pomera glava prve trake nadesno
  - ako je $j = i$ pamti se simbol prve trake koji se trenutno čita, $j = 1$
  - pronalazi se i-ti znak ulazne reči brojano sa desne strane i upoređuje sa zapamćenim simbolom
- postupak se prekida kada su upoređeni znaci različiti, prelazi se u stanje q_{ne}, odnosno kada je i-ti znak ulazne reči blanko znak, prelazi se u stanje q_{da}
- prostor izvršavanja je u $O(\log_2 n)$ koliko je potrebno za binarno predstavljanje indeksa i i j

Klase složenosti

Definition

Klasa složenosti je skup problema sa zajedničkom vremenskom ili prostornom granicom.

Example

Skupovi problema $TIME(f(n))$, $NTIME(f(n))$, $SPACE(f(n))$ i $NSPACE(f(n))$ su neke klase složenosti.

Nedeterminističke klase složenosti

- nedeterminističke klase složenosti sadrže probleme kod kojih je broj kandidata za rešenje veliki, ali kada se kandidat izabere, onda je provera u okviru odgovarajuće determinističke klase problema
- za svaki x koji je primerak problema postoji izračunavanje koje dovodi do prihvatanja, a problem predstavlja izbor izračunavanja kojim se x prihvata
- ni za jedan x koji nije primerak problema ne postoji takvo izračunavanje
- problem koji se nalazi u nedeterminističkoj klasi je testiranje zadovoljivosti iskaznih formula
- za proizvoljnu formulu postoji relativno veliki broj interpretacija koje treba ispitati, ali ako se izabere pogodna interpretacija pri kojoj je formula zadovoljena, sama provera nije komplikovana

Nedeterminističke klase složenosti

- nedeterminističke klase složenosti sadrže probleme kod kojih je broj kandidata za rešenje veliki, ali kada se kandidat izabere, onda je provera u okviru odgovarajuće determinističke klase problema
- za svaki x koji je primerak problema postoji izračunavanje koje dovodi do prihvatanja, a problem predstavlja izbor izračunavanja kojim se x prihvata
- ni za jedan x koji nije primerak problema ne postoji takvo izračunavanje
- problem koji se nalazi u nedeterminističkoj klasi je testiranje zadovoljivosti iskaznih formula
- za proizvoljnu formulu postoji relativno veliki broj interpretacija koje treba ispitati, ali ako se izabere pogodna interpretacija pri kojoj je formula zadovoljena, sama provera nije komplikovana

Klase složenosti

Definition

Neka je $\mathcal{C}$ neka klasa složenosti, njen komplement, u oznaci *co*-$\mathcal{C}$ je skup problema oblika $\{\overline{L} : L \in \mathcal{C}\}$.

- za sve determinističke klase složenosti važi $\mathcal{C} = co\text{-}\mathcal{C}$ jer se komplement svakog problema iz klase $\mathcal{C}$ rešava istom Tjuringovom mašinom koja dodatno menja završno stanje q_{da} u q_{ne} i obrnuto
- deterističke klase složenosti su zatvorene za komplement
- nije poznato da li u opštem slučaju isto važi i za nedeterminističke klase složenosti

Klase složenosti

Definition

Neka je $\mathcal{C}$ neka klasa složenosti, njen komplement, u oznaci *co*-$\mathcal{C}$ je skup problema oblika $\{\overline{L} : L \in \mathcal{C}\}$.

- za sve determinističke klase složenosti važi $\mathcal{C} = co\text{-}\mathcal{C}$ jer se komplement svakog problema iz klase $\mathcal{C}$ rešava istom Tjuringovom mašinom koja dodatno menja završno stanje q_{da} u q_{ne} i obrnuto
- determinističke klase složenosti su zatvorene za komplement
- nije poznato da li u opštem slučaju isto važi i za nedeterminističke klase složenosti

Odnosi između klasa složenosti

Jedno od osnovnih pitanja kojima se bavi teorija složenosti izračunavanja.

Theorem

Neka je problem $L \in TIME(f(n))$. *Tada je za proizvoljno* $\epsilon > 0$, $L \in TIME(\epsilon f(n) + n + 2)$.
Neka je problem $L \in SPACE(f(n))$. *Tada je za proizvoljno* $\epsilon > 0$, $L \in SPACE(\epsilon f(n) + 2)$.

Iz granice složenosti $f(n)$ može se eliminisati konstantni faktor kojim se množi najsloženiji deo funkcije, tj. u granici složenosti $f(n)$ bitan je red brzine rasta $O(f(n))$

Odnosi između klasa složenosti

Dovoljnim povećanjem granice složenosti klase složenosti se šire.

Theorem

Neka je $f(n)$ prava funkcija složenosti. Tada važi:

1. *ako je $f(n) \geq n$, onda je $TIME(f(n)) \subsetneq TIME((f(2n+1))^3)$ i*
2. *$SPACE(f(n)) \subsetneq SPACE(f(n) \cdot \log_2 f(n))$.*

Važnije klase složenosti

- $L = SPACE(O(\log_2 n))$
- $NL = NSPACE(O(\log_2 n))$
- $P = \cup_i TIME(n^i)$
- $NP = \cup_i NTIME(n^i)$
- $PSPACE = \cup_i SPACE(n^i)$ $(PSPACE = NPSPACE = \cup_i NSPACE(n^i))$
- $EXP = \cup_i TIME(2^{n^i})$, $NEXP = \cup_i NTIME(2^{n^i})$,
- $EXPSPACE = \cup_i SPACE(2^{n^i}), \ldots$

Hijerarhiji klasa složenosti

- $L \subset NL \subset P \subset NP \subset PSPACE \subset EXP \subset NEXP$
- $NL \neq PSPACE$ i $P \neq EXP$, pa na bar nekim mestima u hijerarhiji relacija podskup mora biti striktna
- otvorena pitanja:
  - Da li je $P = NP$? Dokaz da je $P \neq NP$ bio bi potvrda da su praktično izračunljivi problemi u P, dok bi suprotan rezultat, mada malo verovatan, doveo do prave revolucije u razvoju algoritama.
  - Da li je $P = PSPACE$?
  - Da li je $L = NL$?
  - Da li je $EXP = NEXP$?

Hijerarhiji klasa složenosti

- $L \subset NL \subset P \subset NP \subset PSPACE \subset EXP \subset NEXP$
- $NL \neq PSPACE$ i $P \neq EXP$, pa na bar nekim mestima u hijerarhiji relacija podskup mora biti striktna
- otvorena pitanja:
  - Da li je $P = NP$? Dokaz da je $P \neq NP$ bio bi potvrda da su praktično izračunljivi problemi u P, dok bi suprotan rezultat, mada malo verovatan, doveo do prave revolucije u razvoju algoritama.
  - Da li je $P = PSPACE$?
  - Da li je $L = NL$?
  - Da li je $EXP = NEXP$?

Hijerarhiji klasa složenosti

- $L \subset NL \subset P \subset NP \subset PSPACE \subset EXP \subset NEXP$
- $NL \neq PSPACE$ i $P \neq EXP$, pa na bar nekim mestima u hijerarhiji relacija podskup mora biti striktna
- otvorena pitanja:
  - Da li je $P = NP$? Dokaz da je $P \neq NP$ bio bi potvrda da su praktično izračunljivi problemi u P, dok bi suprotan rezultat, mada malo verovatan, doveo do prave revolucije u razvoju algoritama.
  - Da li je $P = PSPACE$?
  - Da li je $L = NL$?
  - Da li je $EXP = NEXP$?

Hijerarhiji klasa složenosti

- $L \subset NL \subset P \subset NP \subset PSPACE \subset EXP \subset NEXP$
- $NL \neq PSPACE$ i $P \neq EXP$, pa na bar nekim mestima u hijerarhiji relacija podskup mora biti striktna
- otvorena pitanja:
  - Da li je $P = NP$? Dokaz da je $P \neq NP$ bio bi potvrda da su praktično izračunljivi problemi u P, dok bi suprotan rezultat, mada malo verovatan, doveo do prave revolucije u razvoju algoritama.
  - Da li je $P = PSPACE$?
  - Da li je $L = NL$?
  - Da li je $EXP = NEXP$?

Pozicioniranje složenosti problema

- jedno od osnovnih pitranja: određivanje kojoj klasi složenosti pripada neki problem
- određuju se gornja i donja granica složenosti tako da budu što bliže jedna drugoj
- nekada su međusobno dosta udaljene, te se složenost ne može precizno odrediti
- gornja granica složenosti se određuje konstrukcijom algoritma za njegovo rešavanje i analizom koliko vremena i/ili memorije taj algoritam koristi
- različiti algoritmi za rešavanje nekog problema mogu dati i različite gornje granice složenosti

Pozicioniranje složenosti problema

Euklidov algoritam za nalaženje najvećeg zajedničkog delioca dva

function Euklid(m,l)
begin
    while $m > 0$ **do**
        $t := l \mod m$
        $l := m$
        $m := t$
    return l
end

Pozicioniranje složenosti problema

- Ako je $l \geq m$, uvek je $(l \mod m) < \frac{l}{2}$
- k ukupan broj prolazaka funkcije kroz petlju
- $i \leq k$, m_i i l_i vrednosti od m i l na kraju i-te petlje
- uslov za izlazak iz petlje u koraku k je da je $m_k = 0$ i $m_i \geq 1$, za $i < k$
- $l_i = m_{i-1}$ i $m_i \equiv_{m_{i-1}} l_{i-1}$, za $1 \leq i \leq k$
- za svaki $i \geq 1$, $l_i > m_i$

Pozicioniranje složenosti problema

- $m_i (\equiv_{m_{i-1}} l_{i-1}) < \frac{l_{i-1}}{2} = \frac{m_{i-2}}{2}$, $i \geq 2$
- za $k = 2d + 1$ je $m_{k-1} < \frac{m_{k-3}}{2} < \frac{m_{k-5}}{4} < \ldots < \frac{m_0}{2^d}$
- iz $m_{k-1} \geq 1$, sledi:
  - $m_0 \geq 2^d$
  - $k = 2d + 1 \leq 1 + 2 \log_2 m_0$
- slično za $k = 2d$ $(m_1 \equiv_{m_0} l_0 < m_0)$
- broj prolazaka kroz petlju je reda $\log_2 m$, binarni zapis od m, tj. $|m|$
- operacija deljenja se vrši u $O(\log_2^2 m)$
- gornja granica složenost je celog postupka u $O(n^3)$

Pozicioniranje složenosti problema

- Donja granica složenosti se određuje tako što se pokaže da su izvesno vreme i/ili memorijski prostor neophodni za rešavanje tog problema bilo kojim algoritmom
- često teško i nije poznat neki univerzalni postupak za to
- metoda brojanja: definiše se neka karakteristika ponašanja mašine, pa se analizira koliko puta se ta karakteristika mora ispuniti prilikom prihvatanja ulaza veličine n
- nekada donja granica nije valjana za sve ili za skoro sve ulazne podatke, već samo neograničeno mnogo puta, što dalje komplikuje problem

Pozicioniranje složenosti problema

- Donja granica složenosti se određuje tako što se pokaže da su izvesno vreme i/ili memorijski prostor neophodni za rešavanje tog problema bilo kojim algoritmom
- često teško i nije poznat neki univerzalni postupak za to
- metoda brojanja: definiše se neka karakteristika ponašanja mašine, pa se analizira koliko puta se ta karakteristika mora ispuniti prilikom prihvatanja ulaza veličine n
- nekada donja granica nije valjana za sve ili za skoro sve ulazne podatke, već samo neograničeno mnogo puta, što dalje komplikuje problem

Kompletni problemi - relativno pozicioniranje

Definition

Problem A se *redukuje* na problem B, u oznaci $A \leq B$, ako postoji izračunljiva funkcija f takva da je $A(x)$ tačno ako i samo ako je tačno i $B(f(x))$. Funkcija f se tada naziva *funkcija redukcije*.

Redukovanje ima smisla samo ako je složenost izračunavanja funkcije redukcije zanemarljiva u odnosu na složenost problema B (L, P)

Definition

Funkcija redukcije f problema A na problem B je *efikasna*, a problem A je *efikasno reducibalan* na problem B, u oznaci $A \leq_{ef} B$, ako je složenost funkcije f u klasi L.

Kompletni problemi - relativno pozicioniranje

Definition

Problem A se *redukuje* na problem B, u oznaci $A \leq B$, ako postoji izračunljiva funkcija f takva da je $A(x)$ tačno ako i samo ako je tačno i $B(f(x))$. Funkcija f se tada naziva *funkcija redukcije*.

Redukovanje ima smisla samo ako je složenost izračunavanja funkcije redukcije zanemarljiva u odnosu na složenost problema B (L, P)

Definition

Funkcija redukcije f problema A na problem B je *efikasna*, a problem A je *efikasno reducibalan* na problem B, u oznaci $A \leq_{ef} B$, ako je složenost funkcije f u klasi L.

Kompletni problemi - relativno pozicioniranje

Example

- da li postoji Hamiltonov put u grafu, tj. put koji kroz svaki čvor grafa prolazi tačno jednom
- efikasno se redukuje na problem SAT
- G sadrži n čvorova
- iskazna formula $R(G)$ sadrži n^2 iskaznih slova $x_{i,j}$, $1 \leq i, j \leq n$
- $x_{i,j}$: 'čvor j je i-ti čvor u Hamiltonovom putu'

Kompletni problemi - relativno pozicioniranje

Natavak primera:

- $R(G)$ je u konjunktivnoj formi, konjunkti su oblika
- $x_{1,j} \vee \ldots \vee x_{n,j}$, za svako j, što znači da se svaki čvor mora pojaviti u putu,
- $\neg x_{i,j} \vee \neg x_{k,j}$, za svako j i $i \neq k$, što znači da se svaki čvor pojavljuje tačno jednom u putu,
- $x_{i,1} \vee \ldots \vee x_{i,n}$, za svako i, što znači da jedan čvor mora biti i-ti u putu,
- $\neg x_{i,j} \vee \neg x_{i,k}$, za svako i i $j \neq k$, što znači da se samo jedan čvor može biti i-ti u putu i
- $\neg x_{k,i} \vee \neg x_{k+1,j}$, za sve čvorove i i j koji nisu susedni u grafu G i $1 \leq k \leq n-1$.

Kompletni problemi - relativno pozicioniranje

Natavak primera (2):

- interpretacija koja zadovoljava formulu $R(G)$ opisuje jedan Hamiltonov put u grafu
- svaki Hamiltonov put u grafu definiše jednu interpretaciju koja zadovoljava $R(G)$
- Tjuringova mašina sa ulazom koji opisuje graf G i koja generiše na izlaznoj traci $R(G)$ pripada klasi L
- na radnoj traci najpre predstavi u binarnoj formi broj n
- sa tri indeksa i, j i k se izgenerišu svi konjunkti formule $R(G)$ koji ne zavise od grafa G
- pomoću istih indeksa se generišu formule $\neg x_{k,i} \vee \neg x_{k+1,j}$, za sve čvorove i i j i $1 \leq k \leq n-1$, i ako odgovarajući čvorovi nisu povezani u grafu G, formula se prepiše na izlaznu traku

Kompletni problemi - relativno pozicioniranje

Definition

Klasa problema $\mathcal{C}$ je *zatvorena za* $\leq_{ef}$ ako za svaki problem $B \in \mathcal{C}$ i svaki problem A važi da ako je $A \leq_{ef} B$, onda je i $A \in \mathcal{C}$.

Može se pokazati da su klase složenosti L, NL, P, NP, $co\text{-}NP$, $PSPACE$ i EXP zatvorene za redukciju.

Kompletni problemi - relativno pozicioniranje

Definition

Klasa problema $\mathcal{C}$ je *zatvorena za* $\leq_{ef}$ ako za svaki problem $B \in \mathcal{C}$ i svaki problem A važi da ako je $A \leq_{ef} B$, onda je i $A \in \mathcal{C}$.

Može se pokazati da su klase složenosti L, NL, P, NP, $co\text{-}NP$, $PSPACE$ i EXP zatvorene za redukciju.

Kompletni problemi - relativno pozicioniranje

- ako $A \leq_{ef} B$ (upotrebom funkcije f), složenost problema A je odozgo ograničena zbirom složenosti problema B i funkcije redukcije f
- za ispitivnje da li važi $A(x)$ najpre se x preslika u $f(x)$, a zatim se primeni program za utvrđivanje da li je $B(f(x))$
- ako su poznate složenosti problema B i funkcije f moguće je odrediti jednu gornju granicu složenosti problema A
- Ako je poznato da je složenost problema A veća od nekog zadatog nivoa, onda se može odrediti i jedna donja granica složenosti problema B

Kompletni problemi - relativno pozicioniranje

Definition

Neka je B problem i $\mathcal{C}$ klasa složenosti. Tada kažemo:

- problem B je $\mathcal{C}$-*težak*, u oznaci $\mathcal{C} \leq_{ef} B$, ako je za svaki problem $A \in \mathcal{C}$ ispunjeno $A \leq_{ef} B$ i
- problem B je $\mathcal{C}$-*kompletan* ako je $\mathcal{C} \leq_{ef} B$ i $B \in \mathcal{C}$.

- problem predstavlja klasu u onosu na koju je kompletan
- NP-kompletan problem pripada klasi P ako i samo ako $P = NP$

Kompletni problemi - relativno pozicioniranje

Definition

Neka je B problem i $\mathcal{C}$ klasa složenosti. Tada kažemo:

- problem B je $\mathcal{C}$-*težak*, u oznaci $\mathcal{C} \leq_{ef} B$, ako je za svaki problem $A \in \mathcal{C}$ ispunjeno $A \leq_{ef} B$ i
- problem B je $\mathcal{C}$-*kompletan* ako je $\mathcal{C} \leq_{ef} B$ i $B \in \mathcal{C}$.

- problem predstavlja klasu u onosu na koju je kompletan
- NP-kompletan problem pripada klasi P ako i samo ako $P = NP$

Kompletni problemi - relativno pozicioniranje

Theorem

Neka su $\mathcal{C}$ i $\mathcal{D}$ klase složenosti, takve da je $\mathcal{D} \subset \mathcal{C}$ i $\mathcal{D}$ zatvorena za $\leq_{ef}$ i neka je B jedan $\mathcal{C}$-kompletan problem. Tada važi $B \in \mathcal{D}$ ako i samo ako $\mathcal{C} = \mathcal{D}$.

- postojanje prirodnih problema koji su kompletni za neku klasu složenosti daje klasi odgovarajući značaj

Kompletni problemi - relativno pozicioniranje

Theorem

Neka su $\mathcal{C}$ i $\mathcal{D}$ klase složenosti, takve da je $\mathcal{D} \subset \mathcal{C}$ i $\mathcal{D}$ zatvorena za $\leq_{ef}$ i neka je B jedan $\mathcal{C}$-kompletan problem. Tada važi $B \in \mathcal{D}$ ako i samo ako $\mathcal{C} = \mathcal{D}$.

- postojanje prirodnih problema koji su kompletni za neku klasu složenosti daje klasi odgovarajući značaj

Kompletni problemi - relativno pozicioniranje

Primeri kompletnih problema za najznačajnije klase složenosti

- u klasi L problem kompletnosti nije značajan zbog složenosti funkcije redukcije. L je najmanja prirodna klasa složenosti jer je veličina binarne reprezentacije pokazivača na ulazni podatak x reda $\log_2 |x|$, sadrži probleme ispitivanja palindromi, probleme za grafove koji se mogu formulisati u klasičnom jeziku prvog reda (simetričnost grafa: $(\forall x)(\forall y)(G(x, y) \rightarrow G(y, x))$),
- problem *GAP* koji se odnosi na utvrđivanje da li postoji put između dva zadata čvora grafa je *NL*-kompletan,

Kompletni problemi - relativno pozicioniranje

Primeri kompletnih problema za najznačajnije klase složenosti, nastavak:

- problem *CV* koji se odnosi na izračunavanje vrednosti izlaza logičkog kola u kome ulazne promenljive imaju fiksirane vrednosti je *P*-kompletan,
- problem *SAT* koji se definiše kao skup svih zadovoljivih klasičnih iskaznih formula je *NP*-kompletan,
- *PSPACE*-kompletan je problem *RD* u kome se ispituje da li je za dati sistem procesa koji komuniciraju i neko inicijalno stanje moguće stići u stanje u kome su svi procesi zaglavljeni čekajući međusobno jedan drugog.

Komentar o pristupu analizi složenosti

Primedbe:

- hijerarhija je bazirana na analizi asimptotskog ponašanja granica složenosti
- analiziraju se slučajevi u kojima se algoritmi najgore ponašaju

Komentar o pristupu analizi složenosti

Vremenska granica	Vreme izvršavanja	Vremenska granica	Vreme izvršavanja
n^2	$3.6 \cdot 10^{-6} sec$	2^n	36.3 godine
n^{10}	19.4 godine	$2^{\sqrt[4]{n}}$	$8 \cdot 10^{-9} sec$

- dužina rada računara koji u sekundi obavlja 10^9 koraka izračunavanja za po dva polinomijalna, odnosno eksponencijalna, algoritma ($n = 60$)
- razlika je posledica izraza u stepenima polinoma, eksponetima
- algoritam eksponencijalne vremenske složenosti, kada je eksponent mali, u praktičnim slučajevima sa manjim ulazom, mogu biti pogodniji od polinomijalnih algoritma
- razdvajanje problema na praktično izračunljive i izračunljive u principu, zavisno od toga jesu li, ili ne, u klasi P nije uvek opravdano

Komentar o pristupu analizi složenosti

- primer: javlja se kod linearnog programiranja i simpleks algoritma koji je eksponencijalan, ali dobrih performansi u praksi, odnosno nekih polinomijalnih algoritama za ovaj problem koji su u praksi veoma spori
- broj slučajeva u kojima bi neki eksponencijalni algoritam mogao biti bolji od polinomijalnog je obavezano konačan
- sa stanovišta praktičnog programiranja, primerci problema koji su interesantni mogu biti upravo u tom skupu
- polinomijalnih algoritama sa ogromnim stepenima nema puno, kao ni eksponencijalnih algoritama sa jako malim eksponentom, pa spomenute sitacije nisu pravilo.

Komentar o pristupu analizi složenosti

- druga primedba: analiziraju se slučajevi u kojima se algoritmi najgore ponašaju
- *quick-sort* algoritam sortiranja za slučajan niz ima složenost $O(n \log_2 n)$, dok je složenost za najgori slučaj $O(n^2)$
- analiza očekivanog, a ne najgoreg, slučaja je u takvim situacijama mnogo informativnija
- teško za sprovođenje: potrebno je poznavanje distibucije ulaznih problema, što je često nije ostvarljivo
- pristup prihvatanja statusa praktične izračunljivosti za probleme koji su u najgorem slučaju polinomijalni je nužno pojednostavljenje koje dovodi do primenljive i elegantne teorije koja govori o stvarnim izračunavanjima.

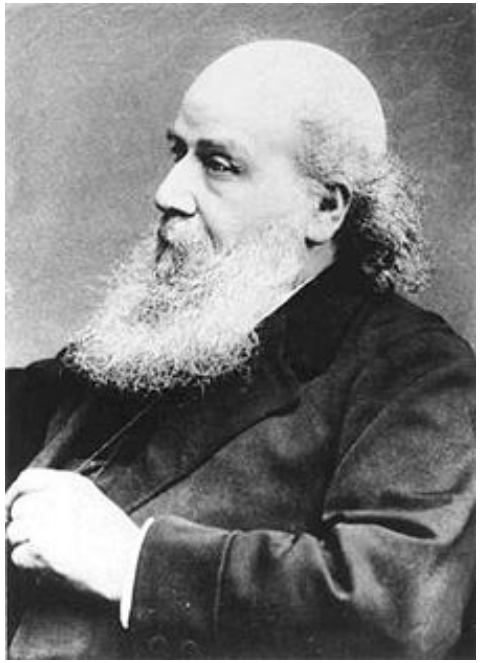
Komentar o pristupu analizi složenosti

- druga primedba: analiziraju se slučajevi u kojima se algoritmi najgore ponašaju
- *quick-sort* algoritam sortiranja za slučajan niz ima složenost $O(n \log_2 n)$, dok je složenost za najgori slučaj $O(n^2)$
- analiza očekivanog, a ne najgoreg, slučaja je u takvim situacijama mnogo informativnija
- teško za sprovođenje: potrebno je poznavanje distibucije ulaznih problema, što je često nije ostvarljivo
- pristup prihvatanja statusa praktične izračunljivosti za probleme koji su u najgorem slučaju polinomijalni je nužno pojednostavljenje koje dovodi do primenljive i elegantne teorije koja govori o stvarnim izračunavanjima.

Osnovni pojmovi u teoriji grafova

- teorija grafova danas izaziva veliko interesovanje - teorijski problemi, primenljivost rezultata
- prvi rad napisao je L. Ojler 1736. (problem mostova u Königsberg-u)
- naziv *graf* je uveo Silvester 1878. godine
- primene: računarstvo, hemija, fizika, za modeliranje saobraćajnih, električnih ili računarskih mreža, ...

James Joseph Sylvester, 1814 – 1897



Dž. Silvester, engleski matematičar, dao je veliki doprinos u teoriji matrica, teoriji invarijanti, teoriji brojeva, kombinatorici. Osnivač je časopisa American Journal of Mathematics (danas Annals of Mathematics, jedan od vodećih matematičkih časopisa).

Osnovni pojmovi u teoriji grafova

Definition

Graf je uređeni par $G = \langle V_G, E_G \rangle$, gde su:

- V_G skup *čvorova* i
- E_G skup *ivica* (*grana, rebara*) oblika $\{u, v\}$, $u, v \in V_G$.

Ivica $\{u, v\}$ povezuje čvorove u i v, pri čemu su oni *susedni*.
Graf je *regularan* ako svi njegovi čvorovi imaju isti stepen.

Osnovni pojmovi u teoriji grafova

Definition

Graf H je *podgraf* grafa G ako je dobijen brisanjem iz G nekih čvorova i ivica, pri čemu se obavezno brišu sve ivice u kojima se nalaze obrisani čvorovi.

Komplement grafa G, u oznaci $\mathbb{C}G = \langle V_G, E_{\mathbb{C}G} \rangle$, ima isti skup čvorova kao i G, ali $\{u, v\} \in E_{\mathbb{C}G}$ ako i samo ako $\{u, v\} \notin E_G$ (pretpostavljamo da je $u \neq v$).

Težinski graf je uređena trojka $G = \langle V_G, E_G, w \rangle$, gde su

- $G = \langle V_G, E_G \rangle$, graf i
- $w : E_G \mapsto [0, \infty)$ funkcija koja ivicama pridružuje težinu.

Osnovni pojmovi u teoriji grafova

- Graf je *konačan*, ili *beskonačan*, u zavisnosti od kardinalnosti njegovog skupa čvorova

Obični grafovi:

- u skladu sa definicijom ne postoje višestruke ivice koje povezuju 2 čvora
- ako između dva čvora postoji više ivica - *multigrafovi*
- ne sadrže ivice oblika $\{u, u\}$, takozvanu *petlju*.

Osnovni pojmovi u teoriji grafova

- Graf je *konačan*, ili *beskonačan*, u zavisnosti od kardinalnosti njegovog skupa čvorova

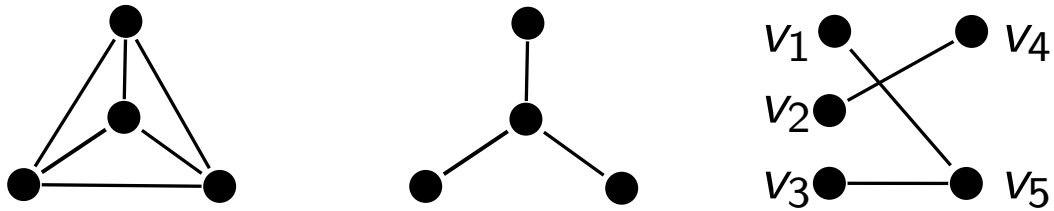
Obični grafovi:

- u skladu sa definicijom ne postoje višestruke ivice koje povezuju 2 čvora
- ako između dva čvora postoji više ivica - *multigrafovi*
- ne sadrže ivice oblika $\{u, u\}$, takozvanu *petlju*.

Osnovni pojmovi u teoriji grafova

- graf $G = \langle V_G, E_G \rangle$ predstavlja izvesnu binarne relacije na skupu V_G
- prema definiciji ivica kao skupova - relacija koju graf predstavlja je simetrična

Osnovni pojmovi u teoriji grafova



Example

Najjednostavniji primer grafa je $\langle V_G, \emptyset \rangle$ u kome ne postoji ni jedna ivica. Njegov komplement je *kompletni graf* u oznaci $K_{|V_G|}$ (K_4 slika a).
Zvezda je graf $\langle V_G, \{\{u, v\} : v \in V_G\} \rangle$ u kome sve ivice povezuju jedan čvor u sa ostalim čvorovima grafa (slika b).
Kod *bipartitnog grafa* skup čvorova ima particiju $\{V_G^1, V_G^2\}$ pri čemu svaka ivica povezuje čvor iz V_G^1 sa čvorom iz V_G^2 (slika c). *Kompletni* bipartitni graf - svaki čvor iz V_G^1 povezan sa svakim čvorom iz V_G^2.

Osnovni pojmovi u teoriji grafova

Definition

Matrica susedstva grafa $G = \langle V_G, E_G \rangle$ je kvadratna matrica $S(G)_{|V_G| \times |V_G|}$ u kojoj je $S(G)_{i,j}$ broj ivica koje povezuju čvorove v_i i v_j.

Example

Matrica

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

predstavlja matricu susedstva za bipartitni graf iz primera sa slike c. Očigledno je da je matrica simetrična.

Osnovni pojmovi u teoriji grafova

Definition

Matrica susedstva grafa $G = \langle V_G, E_G \rangle$ je kvadratna matrica $S(G)_{|V_G| \times |V_G|}$ u kojoj je $S(G)_{i,j}$ broj ivica koje povezuju čvorove v_i i v_j.

Example

Matrica

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

predstavlja matricu susedstva za bipartitni graf iz primera sa slike c. Očigledno je da je matrica simetrična.

Osnovni pojmovi u teoriji grafova

- niz ivica $e_1 = \{v_0, v_1\}$, $e_2 = \{v_1, v_2\}$, $\ldots$, $e_n = \{v_{n-1}, v_n\}$
- *susedne* ivice e_i i e_{i+1} imaju zajednički čvor ($e_i \cap e_{i+1} = \{v_i\}$, $i = 1, n-1$)
- nizu e_1, $\ldots$, e_n odgovara niz čvorova v_0, v_1, $\ldots$, v_n

Definition

Put u grafu je niz međusobno različitih susednih ivica $e_1 = \{v_0, v_1\}$, $e_2 = \{v_1, v_2\}$, $\ldots$, $e_n = \{v_{n-1}, v_n\}$ takvih da u nizu čvorova nema jednakih, sem eventualno čvorova v_0 i v_n.
Šetnja je svaki niz međusobno različitih susednih ivica kod kojih u nizu čvorova može biti i jednakih.
Dužina puta je broj ivica koje ga čine.
Ciklus (*kružni, zatvoreni put*) je put za koji važi $v_0 = v_n$.

Osnovni pojmovi u teoriji grafova

- niz ivica $e_1 = \{v_0, v_1\}$, $e_2 = \{v_1, v_2\}$, $\ldots$, $e_n = \{v_{n-1}, v_n\}$
- *susedne* ivice e_i i e_{i+1} imaju zajednički čvor ($e_i \cap e_{i+1} = \{v_i\}$, $i = 1, n-1$)
- nizu e_1, $\ldots$, e_n odgovara niz čvorova v_0, v_1, $\ldots$, v_n

Definition

Put u grafu je niz međusobno različitih susednih ivica $e_1 = \{v_0, v_1\}$, $e_2 = \{v_1, v_2\}$, $\ldots$, $e_n = \{v_{n-1}, v_n\}$ takvih da u nizu čvorova nema jednakih, sem eventualno čvorova v_0 i v_n.
Šetnja je svaki niz međusobno različitih susednih ivica kod kojih u nizu čvorova može biti i jednakih.
Dužina puta je broj ivica koje ga čine.
Ciklus (*kružni, zatvoreni put*) je put za koji važi $v_0 = v_n$.

Osnovni pojmovi u teoriji grafova

- uslov da među ivicama u putu nema istih znači da put ne sadrži kao potput ni jedan ciklus
- uslov da među odgovarajućim čvorovima u nizu nema jednakih (sem eventualno v_0 i v_n) znači da put ne seče samog sebe.
- na putu se prolazi samo kroz različite čvorove, sem možda na početku i kraju puta, kod šetnje to ne mora biti slučaj.

Osnovni pojmovi u teoriji grafova

Definition

Čvorovi u i v u grafu G su povezani putem $e_1, e_2, \ldots, e_n$ ako je $e_1 = \{u, x\}$ i $e_n = \{y, v\}$.
Graf je *povezan* ako za svaka dva čvora postoji put koji ih povezuje.
H je *povezana komponenta* grafa G ako je to maksimalan podgraf grafa G koji je povezan.

- svaki čvor grafa pripada tačno jednoj povezanoj komponenti
- svake dve povezane komponente su disjunktne, jer ako bi imale zajednički čvor i njihova unija bi bila povezana komponenta.

Osnovni pojmovi u teoriji grafova

Definition

Čvorovi u i v u grafu G su povezani putem $e_1, e_2, \ldots, e_n$ ako je $e_1 = \{u, x\}$ i $e_n = \{y, v\}$.
Graf je *povezan* ako za svaka dva čvora postoji put koji ih povezuje.
H je *povezana komponenta* grafa G ako je to maksimalan podgraf grafa G koji je povezan.

- svaki čvor grafa pripada tačno jednoj povezanoj komponenti
- svake dve povezane komponente su disjunktne, jer ako bi imale zajednički čvor i njihova unija bi bila povezana komponenta.

Osnovni pojmovi u teoriji grafova

Definition

Dva grafa $G = \langle V_G, E_G \rangle$ i $H = \langle V_H, E_S \rangle$ su *izomorfna* ako postoji bijektivna funkcija $f : G \mapsto H$ takva da $\{u, v\} \in E_G$ ako i samo ako je $\{f(u), f(v)\} \in E_H$.
Dva grafa $G = \langle V_G, E_G \rangle$ i $H = \langle V_H, E_S \rangle$ su *homeomorfna* ako se izomorfna slika jednog može dobiti iz izomorfne slike drugog grafa dodavanjem na neke ivice, ili brisanjem sa nekih ivica, čvorova stepena 2.

Problem složenosti ispitivanja (ne)izomorfnosti grafova otvoren, tj. nije poznato da li pripada klasi P ili je NP-kompletan.

Osnovni pojmovi u teoriji grafova

Definition

Dva grafa $G = \langle V_G, E_G \rangle$ i $H = \langle V_H, E_S \rangle$ su *izomorfna* ako postoji bijektivna funkcija $f : G \mapsto H$ takva da $\{u, v\} \in E_G$ ako i samo ako je $\{f(u), f(v)\} \in E_H$.
Dva grafa $G = \langle V_G, E_G \rangle$ i $H = \langle V_H, E_S \rangle$ su *homeomorfna* ako se izomorfna slika jednog može dobiti iz izomorfne slike drugog grafa dodavanjem na neke ivice, ili brisanjem sa nekih ivica, čvorova stepena 2.

Problem složenosti ispitivanja (ne)izomorfnosti grafova otvoren, tj. nije poznato da li pripada klasi P ili je NP-kompletan.

Planarnost grafova

- Neki grafovi imaju osobinu da su *predstavljivi u prostoru dimenzije k*, E^k
- nacrtani su u E^k (čvorovi prikazani kao tačke, a ivice kao linije koje ih povezuju)
- ivice se ne seku (sem što se dodiruju u temenima)

Definition

Graf je *planarni* (*predstavljivi u ravni*, E^2) ako je izomorfan nekom grafu predstavljivom u ravni.

Planarnost grafova

- Neki grafovi imaju osobinu da su *predstavljivi u prostoru dimenzije k*, E^k
- nacrtani su u E^k (čvorovi prikazani kao tačke, a ivice kao linije koje ih povezuju)
- ivice se ne seku (sem što se dodiruju u temenima)

Definition

Graf je *planarni* (*predstavljivi u ravni*, E^2) ako je izomorfan nekom grafu predstavljivom u ravni.

Planarnost grafova

Theorem

Svaki graf se može predstaviti u prostoru dimenzije 3 *(u* E^3*).*

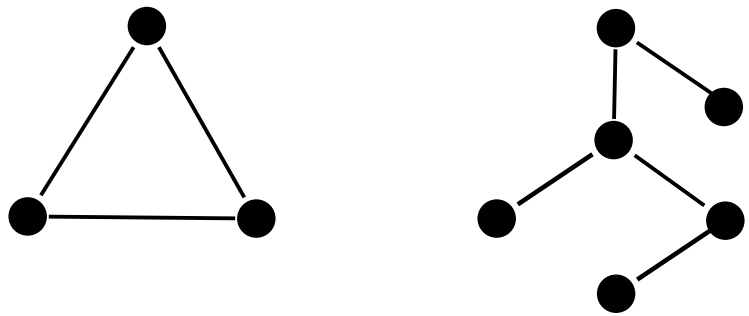
Proof.

Neka je dat graf $G = \langle V_G, E_G \rangle$ u kome je broj čvorova $|V_G| = m$, i broj ivica $|E_G| = k$. Posmatraćemo proizvoljnu pravu l i k različitih ravni α_1, α_2, ..., α_k iz pramena ravni koje se seku po pravoj l. Na pravoj l zatim biramo m tačaka A_1, A_2, ..., A_m koje će predstavljati čvorove grafa, dok svakoj od k ivica pridružimo tačno jednu od izabranih ravni. Ako je ivica oblika $e_n = \{v_i, v_j\}$, onda ćemo u ravni α_n tačke A_i i A_j povezati lukom. Time se dobija predstavljanje grafa u E^3. □

Planarnost grafova

- Da li se dimenzija prostora u kome su predstavljivi svi grafovi može spustiti na 2?
- Ako to nije slučaj - da li se za proizvoljan graf može proveriti da li je planaran?
- Primena: da li neko elektronsko kolo prikazano grafom može biti odštampano na jednom nivou štampane ploče, ili se (ako graf nije planaran) mora premostiti nekoliko nivoa štampe da bi se izbeglo da se veze elemenata seku.

Planarnost grafova



a) b)

Example

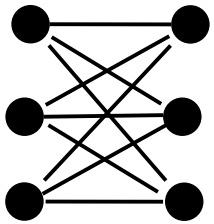
Planarni graf deli ravan na *oblasti* od kojih je nula ili više njih konačnih zatvorenih, i tačno jedna neograničena.
K_3, u obliku trougla, (slika a) deli ravan na jednu konačnu zatvorenu i jednu neograničenu oblast. Za graf u obliku stabla (slika b) postoji samo jedna neograničena oblast.

Planarnost grafova

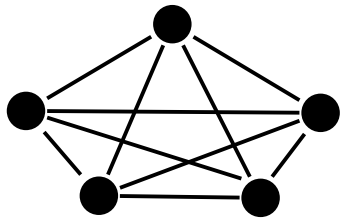
Theorem (Ojlerova teorema)

Povezani planarni graf $G = \langle V_G, E_G \rangle$ *deli ravan u* $f = |E_G| - |V_G| + 2$ *oblasti.*

Planarnost grafova



a)



b)

Primenom Ojlerove teoreme se pokazuje da nisu planarni kompletan bipartitni graf $K_{3,3}$ i kompletan graf K_5

Planarnost grafova

Example

- u $K_{3,3}$ je $|E_G| = 9$ i $|V_G| = 6$
- ako $K_{3,3}$ jeste planaran, onda su granice oblasti neki ciklusi u grafu, ivica pripada granici tačno dve oblasti
- broj ivica koje pripadaju granicama oblasti jednak je $2|E_G|$
- u $K_{3,3}$ najkraći ciklus ima 4 ivice, pa i svaka oblast mora imati granicu sa najmanje toliko ivica
- svaka ivica pripada nekom ciklusu, pa broj ivica koje pripadaju granicama oblasti nije manji od $4 \cdot f$,
- odnosno: $2|E_G| \geq 4 \cdot f$
- iz Ojlerove formule dobija se kontradikcija:

$$2|E_G| = 18 \geq 4 \cdot (|E_G| - |V_G| + 2) = 4 \cdot (9 - 6 + 2) = 20$$

Planarnost grafova

Example

- u $K_{3,3}$ je $|E_G| = 9$ i $|V_G| = 6$
- ako $K_{3,3}$ jeste planaran, onda su granice oblasti neki ciklusi u grafu, ivica pripada granici tačno dve oblasti
- broj ivica koje pripadaju granicama oblasti jednak je $2|E_G|$
- u $K_{3,3}$ najkraći ciklus ima 4 ivice, pa i svaka oblast mora imati granicu sa najmanje toliko ivica
- svaka ivica pripada nekom ciklusu, pa broj ivica koje pripadaju granicama oblasti nije manji od $4 \cdot f$,
- odnosno: $2|E_G| \geq 4 \cdot f$
- iz Ojlerove formule dobija se kontradikcija:

$$2|E_G| = 18 \geq 4 \cdot (|E_G| - |V_G| + 2) = 4 \cdot (9 - 6 + 2) = 20$$

Planarnost grafova

Example

- u $K_{3,3}$ je $|E_G| = 9$ i $|V_G| = 6$
- ako $K_{3,3}$ jeste planaran, onda su granice oblasti neki ciklusi u grafu, ivica pripada granici tačno dve oblasti
- broj ivica koje pripadaju granicama oblasti jednak je $2|E_G|$
- u $K_{3,3}$ najkraći ciklus ima 4 ivice, pa i svaka oblast mora imati granicu sa najmanje toliko ivica
- svaka ivica pripada nekom ciklusu, pa broj ivica koje pripadaju granicama oblasti nije manji od $4 \cdot f$,
- odnosno: $2|E_G| \geq 4 \cdot f$
- iz Ojlerove formule dobija se kontradikcija:

$$2|E_G| = 18 \geq 4 \cdot (|E_G| - |V_G| + 2) = 4 \cdot (9 - 6 + 2) = 20$$

Planarnost grafova

Example

- u $K_{3,3}$ je $|E_G| = 9$ i $|V_G| = 6$
- ako $K_{3,3}$ jeste planaran, onda su granice oblasti neki ciklusi u grafu, ivica pripada granici tačno dve oblasti
- broj ivica koje pripadaju granicama oblasti jednak je $2|E_G|$
- u $K_{3,3}$ najkraći ciklus ima 4 ivice, pa i svaka oblast mora imati granicu sa najmanje toliko ivica
- svaka ivica pripada nekom ciklusu, pa broj ivica koje pripadaju granicama oblasti nije manji od $4 \cdot f$,
- odnosno: $2|E_G| \geq 4 \cdot f$
- iz Ojlerove formule dobija se kontradikcija:

$$2|E_G| = 18 \geq 4 \cdot (|E_G| - |V_G| + 2) = 4 \cdot (9 - 6 + 2) = 20$$

Planarnost grafova

Example

- u $K_{3,3}$ je $|E_G| = 9$ i $|V_G| = 6$
- ako $K_{3,3}$ jeste planaran, onda su granice oblasti neki ciklusi u grafu, ivica pripada granici tačno dve oblasti
- broj ivica koje pripadaju granicama oblasti jednak je $2|E_G|$
- u $K_{3,3}$ najkraći ciklus ima 4 ivice, pa i svaka oblast mora imati granicu sa najmanje toliko ivica
- svaka ivica pripada nekom ciklusu, pa broj ivica koje pripadaju granicama oblasti nije manji od $4 \cdot f$,
- odnosno: $2|E_G| \geq 4 \cdot f$
- iz Ojlerove formule dobija se kontradikcija:

$$2|E_G| = 18 \geq 4 \cdot (|E_G| - |V_G| + 2) = 4 \cdot (9 - 6 + 2) = 20$$

Planarnost grafova

Example

- u $K_{3,3}$ je $|E_G| = 9$ i $|V_G| = 6$
- ako $K_{3,3}$ jeste planaran, onda su granice oblasti neki ciklusi u grafu, ivica pripada granici tačno dve oblasti
- broj ivica koje pripadaju granicama oblasti jednak je $2|E_G|$
- u $K_{3,3}$ najkraći ciklus ima 4 ivice, pa i svaka oblast mora imati granicu sa najmanje toliko ivica
- svaka ivica pripada nekom ciklusu, pa broj ivica koje pripadaju granicama oblasti nije manji od $4 \cdot f$,
- odnosno: $2|E_G| \geq 4 \cdot f$
- iz Ojlerove formule dobija se kontradikcija:

$$2|E_G| = 18 \geq 4 \cdot (|E_G| - |V_G| + 2) = 4 \cdot (9 - 6 + 2) = 20$$

Planarnost grafova

- graf koji ima podgraf izomorfan bilo sa $K_{3,3}$, bilo sa K_5, nije planaran
- obrnuto važi nešto slabije - homeomorfizam grafova
- posmatrajmo graf dobijen od K_5 tako što je na ivici $\{v_1, v_2\}$ dodat čvor v_6, tako da umesto $\{v_1, v_2\}$, postoje ivice $\{v_1, v_6\}$ i $\{v_6, v_2\}$. Taj novi graf i dalje nije planaran, ali nije ni izomorfan (već samo homeomorfan) sa K_5

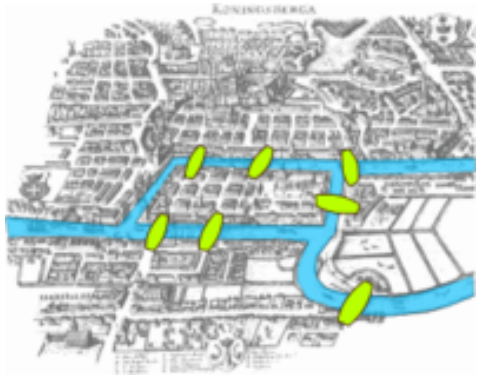
Theorem (Kuratosvki)

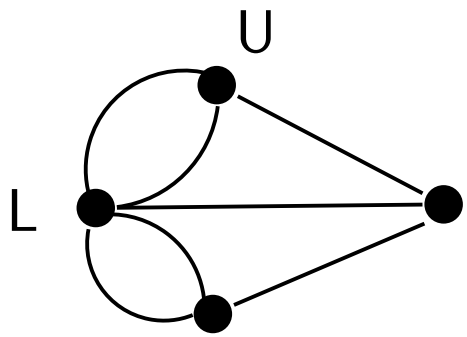
Graf je planaran ako i samo ako ni jedan njegov podgraf nije homeomorfan grafovima $K_{3,3}$, ili K_5.

Kazimierz Kuratowski, 1896 – 1980

K. Kuratovski, jedan od vodećih predstavnika poljske škole matematike (Sierpinski, Sikorski, Lindenbaum, Tarski, Łukasiewicz, Mostowski, Banach). Najvažniji rezultati su mu u topologiji i teoriji mere.

Mostovi Königsberg-a





Grafovska reprezentacija mape Königsberg-a

Mostovi Königsberg-a

- prvi poznati rad u oblasti teorije grafova (Ejler, 1736.)
- čvorovi su kvartovi razdvojeni rekom, a ivice označavaju mostove koji ih povezuju
- gornji čvor (kvart, U) 3 mosta povezuju sa ostalim kvartovima, dok je za najlevlji čvor (L) to slučaj sa 5 mostova
- radi se o multigrafu
- Problem: ispitati da li je moguće izvesti *Ojlerovu šetnju*, u kojoj se svaki most prelazi tačno jednom
- šetnja - dozvoljeno da se isti čvor poseti više puta

Mostovi Königsberg-a

- prvi poznati rad u oblasti teorije grafova (Ejler, 1736.)
- čvorovi su kvartovi razdvojeni rekom, a ivice označavaju mostove koji ih povezuju
- gornji čvor (kvart, U) 3 mosta povezuju sa ostalim kvartovima, dok je za najlevlji čvor (L) to slučaj sa 5 mostova
- radi se o multigrafu
- Problem: ispitati da li je moguće izvesti *Ojlerovu šetnju*, u kojoj se svaki most prelazi tačno jednom
- šetnja - dozvoljeno da se isti čvor poseti više puta

Mostovi Königsberg-a

- Ojler je na problem odgovorio negativno - tražena šetnja ne postoji
- šetnja ne počinje u čvoru L
- prelazeći neku od ivica stići ćemo u L, pa ga napustiti drugom ivicom, zatim se na njega vratiti trećom, pa ga ponovu napustiti četvrtom i konačno pomoću pete ivice vraćamo se u L
- zaustavljanje - iskorišteno svih 5 ivica
- ako šetnja nije započela u L, tu mora da se završi
- isto važi i za sve druge čvorove, (manji broj mostova, 3, pa je manji i broj poseta
- za svaki čvor - šetnja ili polazi iz njega, ili se u njemu završava
- graf sadrži 4 čvora, ispuniti takav zahtev nije moguće

Mostovi Königsberg-a

- Ojler je na problem odgovorio negativno - tražena šetnja ne postoji
- šetnja ne počinje u čvoru L
- prelazeći neku od ivica stići ćemo u L, pa ga napustiti drugom ivicom, zatim se na njega vratiti trećom, pa ga ponovu napustiti četvrtom i konačno pomoću pete ivice vraćamo se u L
- zaustavljanje - iskorišteno svih 5 ivica
- ako šetnja nije započela u L, tu mora da se završi
- isto važi i za sve druge čvorove, (manji broj mostova, 3, pa je manji i broj poseta
- za svaki čvor - šetnja ili polazi iz njega, ili se u njemu završava
- graf sadrži 4 čvora, ispuniti takav zahtev nije moguće

Mostovi Königsberg-a

Theorem

Ako povezani graf ima više od dva čvora neparnog stepena, u njemu nije moguće izvesti Ojlerovu šetnju. Ako povezani graf ima tačno dva čvora neparnog stepena, u njemu je moguće izvesti Ojlerovu šetnju, a svaka od tih šetnji mora početi u jednom od tih čvorova i završiti u drugom. Povezani graf ima zatvorenu Ojlerovu šetnju ako i samo ako su mu svi čvorovi parnog stepena.

Hamiltonov ciklus

- Problem postojanja *Hamiltonovog ciklus*je u izvesnom smislu dualan upravo opisanom problemu Ojlerove šetnje
- ispituje se postojanje ciklusa koji sadrži sve čvorove grafa, a ne šetnje koja sadrži sve ivice
- do sada nisu poznati potrebni i dovoljni uslovi za postojanje Hamiltonovog ciklusa u proizvoljnom grafu

Jedan od dovoljnih uslova za postojanje Hamiltonovog ciklusa:

Theorem

Povezani graf sa $n \geq 3$ čvorova u kome je stepen svakog čvora barem $\frac{n}{2}$ sadrži Hamiltonov ciklus.

Hamiltonov ciklus

- Problem postojanja *Hamiltonovog ciklus*je u izvesnom smislu dualan upravo opisanom problemu Ojlerove šetnje
- ispituje se postojanje ciklusa koji sadrži sve čvorove grafa, a ne šetnje koja sadrži sve ivice
- do sada nisu poznati potrebni i dovoljni uslovi za postojanje Hamiltonovog ciklusa u proizvoljnom grafu

Jedan od dovoljnih uslova za postojanje Hamiltonovog ciklusa:

Theorem

Povezani graf sa $n \geq 3$ čvorova u kome je stepen svakog čvora barem $\frac{n}{2}$ sadrži Hamiltonov ciklus.

William Rowan Hamilton, 1805 – 1865

W. Hamilton, irski matematičar, fizičar i astronom. Uveo je kvaternione, jednu vrstu generalizacije kompleksnih brojeva.

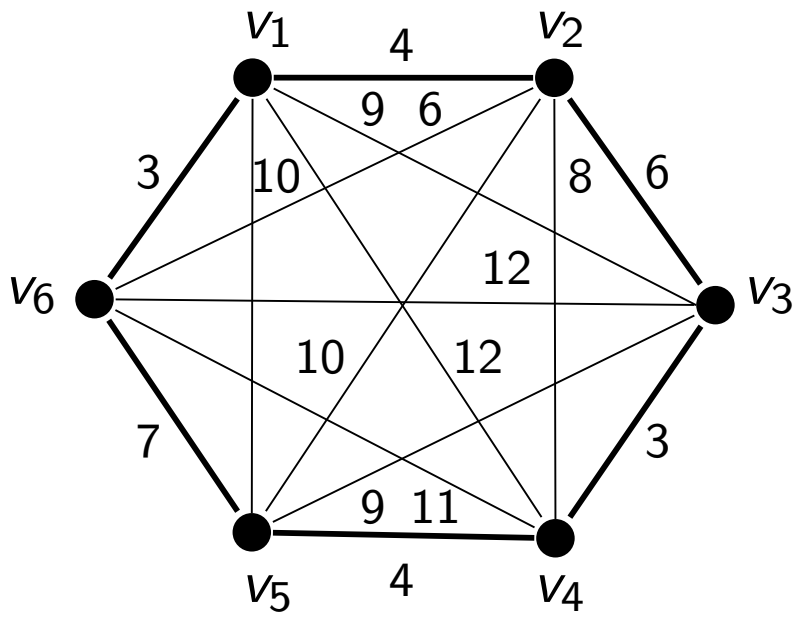
Problem trgovačkog putnika

- problem Hamiltonovih ciklusa je u vezi sa žnijm problemom kombinatorijalne optimizacije - *problem trgovačkog putnika*
- u kompletnim težinskim grafovima se traže Hamiltonovi ciklusi sa minimalnim zbirom težina ivica
- značaj problema u mnogim oblastima u kojima služi za modeliranje različitih realnih situacija
- težine ivica mogu biti rastojanja koja treba preći na putu, vremena ili količine goriva koje treba potrošiti na obavljanja nekih operacija itd.
- postoji samo konačno mnogo Hamiltonovih ciklusa u konačnom grafu, uvek postoji i bar jedan minimalan, pa je problem odlučiv
- problem: efikasan algoritam za njegovo rešavanje
- pokazano je da je ovaj problem NP-kompletan
- razvijaju se heuristički algoritmi za rešavanje

Problem trgovačkog putnika

- problem Hamiltonovih ciklusa je u vezi sa žnijm problemom kombinatorijalne optimizacije - *problem trgovačkog putnika*
- u kompletnim težinskim grafovima se traže Hamiltonovi ciklusi sa minimalnim zbirom težina ivica
- značaj problema u mnogim oblastima u kojima služi za modeliranje različitih realnih situacija
- težine ivica mogu biti rastojanja koja treba preći na putu, vremena ili količine goriva koje treba potrošiti na obavljanja nekih operacija itd.
- postoji samo konačno mnogo Hamiltonovih ciklusa u konačnom grafu, uvek postoji i bar jedan minimalan, pa je problem odlučiv
- problem: efikasan algoritam za njegovo rešavanje
- pokazano je da je ovaj problem NP-kompletan
- razvijaju se heuristički algoritmi za rešavanje

Problem trgovačkog putnika



Rešenje problema trgovačkog putnika u ovom grafu je ciklus $\langle v_1, v_2\rangle$, $\langle v_2, v_3\rangle$, $\langle v_3, v_4\rangle$, $\langle v_4, v_5\rangle$, $\langle v_5, v_5\rangle$, $\langle v_6, v_1\rangle$, ukupne težine 29.

Uparivanje u bipartitnim grafovima

- izvestan broj različitih fotokopir-uređaja i nekoliko tipova jediničnih punjenja tonera
- neke vrste tonera se sipaju u neke vrste fotokopira
- svi fotokopiri treba da budu napunjeni i
- sav toner potrošen.
- ako je tako nešto izvodljivo, ostvareno je *savršeno uparivanje*

Uparivanje u bipartitnim grafovima

- izvestan broj različitih fotokopir-uređaja i nekoliko tipova jediničnih punjenja tonera
- neke vrste tonera se sipaju u neke vrste fotokopira
- svi fotokopiri treba da budu napunjeni i
- sav toner potrošen.
- ako je tako nešto izvodljivo, ostvareno je *savršeno uparivanje*

Uparivanje u bipartitnim grafovima

- predstavljanje pomoću bipartitnih grafova
- fotokopiri i toneri su čvorovi, ivice koje ih povezuju ukazuju na kompatibilnost
- da li se može pronaći skup ivica u bipartitnom grafu tako da je svaki čvor jedne particiji povezan sa tačno jednim čvorom druge particije
- za utvrđivanje postojanja savršenog uparivanja u bipartitinom grafu postoje algoritmi sa polinomijalnom vremenskom složenošću

Uparivanje u bipartitnim grafovima

Theorem

Neka je $G = \langle V_G^1 \cup V_G^2, E_G \rangle$ *bipartitini graf. Tada:*

- *ako svaki čvor ima isti pozitivni stepen, u grafu* G *postoji savršeno uparivanje,*
- *u grafu* G *postoji savršeno uparivanje ako i samo ako* $|V_G^1| = |V_G^2|$ *i za svako* k *i svaki podskup* $A \subset V_G^1$*, takav da* $|A| = k$*, postoji* $B \subset V_G^2$*, takav da* $|B| = k$*, pri čemu su čvorovi iz* B *povezani sa barem jednim čvorom iz* A*.*

Hromatski broj grafa

- prilikom bojenja graf svakom čvoru se pridružuje jedna boja, tako da susedni čvorovi nisu iste boje
- *Hromatski broj grafa* G je k, ako je to najmanji broj boja kojima se G može obojiti
- engleski matematičar Kejli je 1879. godine postavio problem *četiri boje*: da li je moguće obojiti svaku kartu upotrebom četiri boje, pri čemu je svaka država obojena tačno jednom bojom i ni koje dve susedne države (koje imaju zajedničku graničnu liniju) nisu obojene istom bojom
- 1976. godine problem je pozitivno rešen - po prvi put u matematici ozbiljno su iskorišteni računari pomoću kojih je testiran veliki broj relevantnih slučajeva

Stabla

Definition

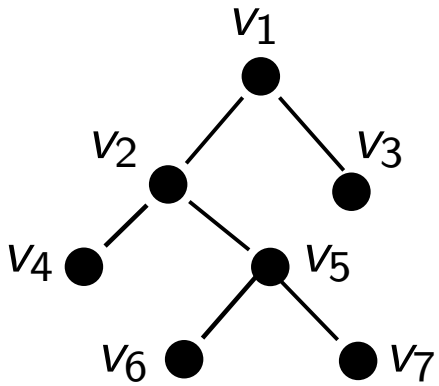
Stablo je povezan graf bez ciklusa.
Razapinjuće stablo za povezani graf $G = \langle V_G, E_G \rangle$ je stablo koje je podgraf grafa G i sadrži sve čvorove iz V_G.
Stablo sa korenom je uređena trojka $T = \langle V_T, E_T, v \rangle$, gde je $T = \langle V_T, E_T \rangle$ stablo, a $v \in V_T$ izabrani čvor koji se naziva *koren*. Čvorovi stepena 1 iz V_T, različiti od korena, se nazivaju *listovi*. Svi ostali čvorovi iz V_T se nazivaju *unutrašnji*.

Stabla

Definition

U stablu sa korenom $T = \langle V_T, E_T, v \rangle$ *nivo* čvora w je dužina jedinstvenog puta, tj. broj ivica, od korena v do w. *Visina* je maksimalni nivo čvorova u stablu. *Roditelj* čvora w nivoa k je jedinstveni susedni čvor v nivoa $k-1$. Ako je v roditelj čvora w, onda je w *potomak* čvora v.
Stablo sa korenom u kome svaki čvor ima najviše m potomaka, a bar jedan čvor ima tačno m potomaka je m-arno stablo. Ako je $m = 2$, reč je o *binarnom stablu*, a ako je $m = 3$ o *ternarnom*. m-arno stablo u kome svaki roditelj ima tačno m potomaka se naziva *puno*.

Stabla



Example

Slika prikazuje jedno puno binarno stablo. Čvor v_1 je koren, a listovi su čvorovi v_3, v_4, v_6 i v_7. Čvor v_5 je roditelj čvorova v_6 i v_7. Nivo čvora v_4 iznosi 2, dok je nivo čvorova v_6 i v_7 jednak 3, što je istovremeno i visina stabla.

Stabla

Theorem

Za svako stablo $T = \langle V_T, E_T \rangle$ važi:

- *svaki par različitih čvorova je povezan tačno jednim putem,*
- *brisanje bilo koje ivice iz E_T proizvodi dva grafa koja su oba stabla i*
- $|E_T| = |V_T| - 1$.

Stabla

Primene u razvoju algorita zasnovanih na stablima:

- sortiranje podataka pomoću binarnih stabala čiji čvorovi sadrže vrednosti tako da za svaki čvor važi da su sve vrednosti u čvorovima u levom podstablu manje do jednake od vrednosti u samom čvoru, koja je manja do jednaka od vrednosyi u čvorovima desnog podstabla,
- pretraživanje podataka po širini[1] ili po dubini[2] razapinjućeg stabla grafa koji sadrži neke podatke,
- konstrukcija minimalnog razapinjućeg stabla težinskog grafa (koji može modelirati, na primer, telefonsku ili mrežu puteva) ili najkraćeg puta između njegovih čvorova itd.

[1] Engleski: breadth-first search.
[2] Engleski: depth-first search.

Direktni grafovi

- do sada: ivice grafova su bile neusmerene, tj. uvedene su kao skupovi
- ponekad je pogodno ivicama dodati usmerenje i time razlikovati čvorove iz kojih ivice polaze, od onih u koje ivice dolaze
- interpretacija: tokom obilaska grafa nije dozvoljeno kretanje ivicama suprotno njihovim smerovima
- ivice treba definisati kao uređene parove

Direktni grafovi

Definition

Direktan graf (*digraf*) je uređeni par $G = \langle V_G, E_G \rangle$, gde je V_G skup *čvorova* i $E_G \subset V_G^2$ skup *ivica*.
Svaka ivica $e = \langle u, v \rangle \in E_G$ je uređeni par čvorova $u, v \in V_G$, gde je u *čvor repa* (*početni čvor*), a v *čvor glave* (*ulazni, završni čvor*) ivice e.
Direktan acikličan graf (DAG) je direktan graf u kojem nema ciklusa.

- većina pojmova, poput puta, ciklusa, povezanosti itd., se definišu analogno
- susedne ivice u putu u digrafu moraju biti oblika $e_i = \langle v_{i-1}, v_i \rangle$ i $e_{i+1} = \langle v_i, v_{i+1} \rangle$, tj. čvor glave ivice e_i mora biti čvor repa ivice e_{i+1}
- relacije koje predstavljaju digrafovi ne moraju biti simetrične

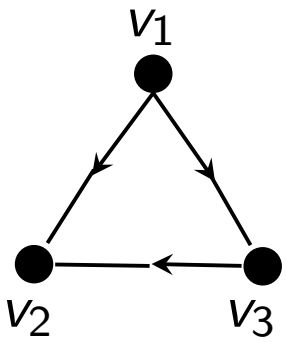
Direktni grafovi

Definition

Direktan graf (*digraf*) je uređeni par $G = \langle V_G, E_G \rangle$, gde je V_G skup *čvorova* i $E_G \subset V_G^2$ skup *ivica*.
Svaka ivica $e = \langle u, v \rangle \in E_G$ je uređeni par čvorova $u, v \in V_G$, gde je u *čvor repa* (*početni čvor*), a v *čvor glave* (*ulazni, završni čvor*) ivice e.
Direktan acikličan graf (DAG) je direktan graf u kojem nema ciklusa.

- većina pojmova, poput puta, ciklusa, povezanosti itd., se definišu analogno
- susedne ivice u putu u digrafu moraju biti oblika $e_i = \langle v_{i-1}, v_i \rangle$ i $e_{i+1} = \langle v_i, v_{i+1} \rangle$, tj. čvor glave ivice e_i mora biti čvor repa ivice e_{i+1}
- relacije koje predstavljaju digrafovi ne moraju biti simetrične

Direktni grafovi



Example

Slika prikazuje digraf $\langle \{v_1, v_2, v_3\}, \{\langle v_1, v_2\rangle, \langle v_1, v_3\rangle, \langle v_3, v_2\rangle\}\rangle$.

Direktni grafovi

Primene digrafova:

- binarni diagrami odlučivanja (BDD) koji se koriste u efikasnom predstavljanju
- maksimizacija protoka kroz transportne mreže modelirne težinskim digrafovima (gde transportna mreža može biti mreža optičkih ili električnih kablova, cevovod, . . .) itd.