Diskretna matematika

Literatura:

- Darko Žubrinić, *Diskretna matematika,* Element, Zagreb 1997.

- "kontinuirani" (neprekinuti) skupovi (npr. $\mathbb{R}, [0,1], ..$);

- "diskretni" skupovi (npr. konačni, $\mathbb{N}, \mathbb{Z}, ...$);

- Diskretna matematika

- temelj su diskretni skupovi i diskretne funkcije;

- "Kontinuirana" matematika (matematička analiza)

- temelj su kontinuirani skupovi ($\mathbb{R}$) i kontinuirane funkcije;

Diskretna matematika obuhvaća: relacije na diskretnim skupovima, rekurzivne relacije, matematičku logiku, Booleovu algebru, kombinatoriku, algoritme, teoriju grafova, diskretne algebarske strukture[1], ...

[1] Algebarskom strukturom nazivamo bilo koji skup na kojem je definirana barem jedna operacija.

1. SKUPOVI

1.1 Temeljne oznake i definicije

- *Skup* je osnovni matematički pojam (ne definira se);

- Skup je svaka množina (nekih) objekata koje nazivamo *elementima* ili *članovima* skupa;

- Oznake:

- skupove - velikim slovoma A, B, S, X, ...;

- elemente - malim slovoma a, b, s, x, ...;

- činjenicu da element x pripada skupu A bilježimo sa $x \in A$;

- činjenicu da element x ne pripada skupu A bilježimo sa $x \notin A$;

- Skupove zadajemo:

- popisivanjem njegovih elemenata (ako je to moguće);

- opisno, pomoću nekog svojstva.

1.2 Odnosi (relacije) među skupovima

Definicija Za skup A kažemo da je podskup skupa B ako je A sadržan u B, tj. ako vrijedi da ako je $x \in A$ onda je $x \in B$. Pišemo $A \subseteq B$.
Ako je $A \subseteq B$ onda kažemo da je B nadskup od A (oznaka $B \supseteq A$).

" $\subseteq$ " - inkluzija (uključivanje).

Definicija Kažemo da su skupovi A i B jednaki ako vrijedi $A \subseteq B$ i $B \subseteq A$. Pišemo $A = B$.

Definicija Kažemo da je A pravi podskup od B ako vrijedi $A \subseteq B$ i $A \neq B$. Pišemo $A \subset B$.

Vrijedi:

- $A \subseteq A$ za svaki skup A;

- $\emptyset \subseteq A$ za svaki skup A, gdje je $\emptyset$ oznaka za prazan skup, tj. skup bez elemenata;

1.3 Operacije sa skupovima

Primjer

$B = \{x : \ x$ nije prirodan broj$\}$ - neprecizno definiran skup

Da bi B bio dobro definiran uvodimo pojam univerzalnog skupa U. To je skup koji je prozivoljan, ali unaprijed zadan i svi skupovi koje promatramo su podskupovi tog skupa.

Definicija Neka je A podskup univerzalnog skupa U. Skup $\{x \in U : \ x \notin A\}$ nazivamo komplement skupa A i označavamo sa $\bar{A}$ (ili A^C).

Definicija Neka su skupovi A i B (podskupovi univerzalnog skupa U).

Skup $\{x : \ x \in A$ ili $x \in B\}$ nazivamo unija skupova A i B i označava sa $A \cup B$.

Skup $\{x : \ x \in A$ i $x \in B\}$ nazivamo presjek skupova A i B i označava sa $A \cap B$.

Skup $\{x : \ x \in A$ i $x \notin B\}$ nazivamo razlika skupova A i B i označava sa $A \setminus B$.

Definicija Neka je X skup. Skup svih podskupova od X nazivamo partitivan skup od X i označavamo sa 2^X (ili $\mathcal{P}(X)$).

Na partitivnom skupu 2^X dobro su definirane tri osnovne operacije:

- unija $\cup : (A, B) \to A \cup B$;
- presjek $\cap : (A, B) \to A \cap B$;
- komplementiranje $^- : A \to \bar{A}$.

Operacije $\cup$ i $\cap$ su binarne operacije (dvama elementima iz 2^X pridružuju treći iz 2^X), a komplementiranje je unarna (jednom elem. iz 2^X pridružuje drugi iz 2^X).

Teorem 1 Neka su A, B, $C \in 2^X$ tada vrijedi:

1. idempotentnost unije i presjeka:

$$A \cup A = A, \qquad A \cap A = A;$$

2. asocijativnost:

$$(A \cup B) \cup C = A \cup (B \cup C),$$
$$(A \cap B) \cap C = A \cap (B \cap C);$$

3. komutativnost:

$$A \cup B = B \cup A, \qquad A \cap B = B \cap A;$$

4. distributivnost:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C);$$

5. De Morganove formule:

$$\overline{A \cup B} = \bar{A} \cap \bar{B} \qquad \overline{A \cap B} = \bar{A} \cup \bar{B};$$

6. $A \cup \emptyset = A, \quad A \cap X = A;$

7. $A \cup X = X, \quad A \cap \emptyset = \emptyset;$

8. komplementarnost:

$$A \cup \bar{A} = X, \qquad A \cap \bar{A} = \emptyset;$$

9. involutivnost komplementiranja: $\overline{\overline{A}} = A.$

Napomene:

- Sva svojstva iz prethodnog teorema imaju svojstvo dualnosti, tj. zamjenom

$$\cup \leftrightarrow \cap \quad i \quad \emptyset \leftrightarrow X$$

u jednom pravilu dobivamo drugo (valjano) pravilo.

- Zbog asocijativnosti opravdano je umjesto $(A \cup B) \cup C$ pisati $A \cup B \cup C$. Slično za $\cap$.

Ako imamo (konačan ili beskonačan) niz skupova $A_1, A_2, ..., A_n, ...$, onda, zbog asocijativnosti, uniju označavamo

$A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{k=1}^{n} A_k$ (za konačan niz)

$A_1 \cup A_2 \cup ... \cup A_n \cup ... = \bigcup_{k=1}^{\infty} A_k$ (za beskonačan niz).

Slično za presjek.

- Skup $\emptyset$ možemo shvatiti kao najmanji, a skup X kao najveći element skupa 2^X (u smislu relacije "biti podskup"), tj. za svaki skup $A \in 2^X$ vrijedi: $\emptyset \subseteq A \subseteq X$

1.4 Kartezijev produkt

Definicija Neka su $A_1,\ A_2, ...A_n$ neprazni skupovi, onda definiramo Kartezijev produkt

$$A_1 \times A_2 \times ... \times A_n$$

kao skup svih uređenih $n-$torki $(a_1,\ a_2, ..., a_n)$ takvih da je $a_k \in A_k$ za sve $k = 1, 2, ..., n$.
Kraća oznaka $\prod_{k=1}^{n} A_k$.

Alternativna definicija

Uočimo: ako je $(a_1,\ a_2, ..., a_n) \in A_1 \times A_2 \times ... \times A_n$, onda $n-$torku $(a_1,\ a_2, ..., a_n)$ možemo promatrati kao funkciju

$$f : \{1, 2, ..., n\} \to \bigcup_{k=1}^{n} A_k$$

danu sa $f(k) = a_k \in A_k$ za sve $k = 1, 2, ..., n$, tj.

$$(a_1,\ a_2, ..., a_n) \equiv (f(1),\ f(2), ..., f(n)).$$

Vrijedi i obrnuto.

Dakle, Kartezijev produkt $\prod_{k=1}^{n} A_k$ možemo definirati i kao skup svih funkcija $f : \{1, 2, ..., n\} \to \bigcup_{k=1}^{n} A_k$ tako da je $f(k) = a_k \in A_k$ za sve $k = 1, 2, ..., n$.

1.5 Ekvipotentnost skupova. Kardinani broj.

Definicija Kažemo da je skup A *ekvipotentan (jednakobrojan)* sa skupom B ako postoji bijekcija $f : A \longrightarrow B$. Oznaka $A \sim B$.

Teorem 2 Ekvipotentnost ima ova svojstva:

- refleksivnost: $A \sim A$ za svaki skup A;
- simetričnost: ako je $A \sim B$, onda je $B \sim A$;
- tranzitivnost: ako je $A \sim B$ i $B \sim C$, onda je $A \sim C$;

Dakle, ekvipotentnost je relacija ekvivalencije među skupovima.

Definicija Za skupove A i B kažemo da imaju isti *kardinalni broj* ako su ekvipotentni. Pišemo $|A| = |B|$ (ili $card\, A = card\, B$).

Definicija Za skup kažemo da je *beskonačan* ako je ekvipotentan sa svojim pravim podskupom. Za skup kažemo da je *konačan* ako nije beskonačan.

Tvrdnja Skup prirodnih brojeva $\mathbb{N}$ je beskonačan, a skup $\{1, 2, ..., n\}$ je konačan. Skup realnih brojeva $\mathbb{R}$ je beskonačan.

Definicija Kardinalni broj skupa $\mathbb{N}$ označavamo sa $\aleph_0$ (alef nula) i pišemo $card\,\mathbb{N} = \aleph_0$.

Kardinalni broj skupa $\{1, 2, ..., n\}$ označavamo sa n i pišemo $card\ \{1, 2, ..., n\} = n.$

Svaki skup S za koji je $card\,S = \aleph_0$, tj. koji je ekvipotentan sa $\mathbb{N}$ kažemo da je prebrojivo beskonačan.

Svaki skup S za koji je $card\,S = n$, tj. koji je ekvipotentan sa $\{1, 2, ..., n\}$ kažemo da ima n elemenata.

Primjer $card\,\mathbb{Z} = card\,\mathbb{Q} = \aleph_0$, tj. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ su prebrojivo beskonačni (sve elemente možemo poredati u beskonačni niz).

Teorem 3 Svaki beskonačan podskup prebrojivog skupa je prebrojiv.

Teorem 4 Neka je A beskonačan skup i K njegov konačan podskup, onda su skupovi A i $A \setminus K$ ekvipotentni, tj. $card\, A = card\, A \setminus K$.

Teorem 5 (Cantor) Skup realnih brojeva $\mathbb{R}$ je *neprebrojiv*, tj. nije ekvipotentan sa $\mathbb{N}$**.** Dakle, vrijedi $\aleph_0 < card\, \mathbb{R} = c$ (*kontinum*).

Dokaz: Kontradikcijom. (Cantorov dijagonalni postupak).

Pitanje: Postoji li skup S, $\mathbb{N} \subset S \subset \mathbb{R}$ koji nije ekvipotentan ni sa $\mathbb{N}$ ni sa $\mathbb{R}$, tj. tako da je $\aleph_0 < cardS < c$?

Odgovor: *Neodlučiv.* Pokazano je da se ne može se odgovoriti na to pitanje pomoću aksioma teorije skupova (Choen 1964.). Uz pretpostavku da takav skup ne postoji (*Cantorova hipoteza kontinuma*) imamo jednu teoriju skupova, a uz pretpostavku da takav skup postoji, drugu.

Definicija Za realan broj a kažemo da je *algebarski broj* ako postoji polinom $P(x)$ s cjelobrojnim koeficijentima takav ada je $P(a) = 0$.

Propozicija Skup svih algebarskih brojeva brojeva je prebrojiv.

Definicija Realni brojevi koji nisu algebarski nazivaju se *transcedentni.*

Dodatak: Gödelizacija

Teorem 6 Neka je $\mathbb{N}^k = \mathbb{N} \times \mathbb{N} \times ... \times \mathbb{N}$ skup svih uređenih $k-$torki prirodnih brojeva, tada je skup $A = \bigcup_{k=1}^{\infty} \mathbb{N}^k$ prebrojiv. Drugim riječima, skup svih konačnih nizova prirodnih brojeva je prebrojiv.

Definicija Funkcija $f : \bigcup_{k=1}^{\infty} \mathbb{N}^k \to \mathbb{N}$ definirana sa

$$f(n_1, n_2, ..., n_k) = p_1^{n_1} p_2^{n_2} \cdot ... \cdot p_k^{n_k},$$

gdje je $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., niz prostih brojeva, se naziva **gödelizacija skupa** $A = \bigcup_{k=1}^{\infty} \mathbb{N}^k$.

2. MATEMATIČKA LOGIKA

2.1 Temeljne oznake i definicije

Definicija *Sud* je svaka smislena izjavna rečenica koja može biti samo *istinita* ili *lažna*.;

Oznake:

- sudove - (obično) velikim slovoma A, B, C, ...;

- svakom sudu A pridružujemo vrijednost $\top$ (*"istina"*) ako je istinit, a vrijednost $\bot$ (*"laž"*) ako je lažan;

- vrijednost istinitosti suda A označavamo sa $\tau(A)$ i nazivamo *semantička* ili *istinitosna vrijednost*. Dakle, $\tau(A) = \top$ znači: sud A je istinit, a $\tau(A) = \bot$ znači: sud A je lažan;

- ponekad se umjesto $\top$ i $\bot$ koristi 1 (*"istina"*) i 0 (*"laž"*);

- matematičku logiku ne zanima sadržaj suda već samo njegova istinitost, pa se ponekad se umjesto $\tau(A) = \top$ piše $A \equiv \top$, a umjesto $\tau(A) = \bot$ piše $A \equiv \bot$, tj. identificiramo sud s njegovom istinitošću.

2.2 Operacije sa sudovima

Skup svih sudova možemo identificirati sa skupom $\{\top, \bot\}$. Uz tu identifikaciju na skupu $\{\top, \bot\}$ imamo:

- 4 različite *unarne logičke operacije* (jednom sudu pridružuje drugi - samo jedna varijabla),

- 16 različitih *binarnih logičkih operacija* (dvama sudovima (uređenom paru) pridružuje treći - dvije varijable).

Sve te operacije opisane su pomoću tzv. *semantičkih (istinitnosnih) tablica*. Najvažnije operacije su:

Definicija Neka je A sud. *Negacija suda* A je sud kojeg označavamo sa $\rceil A$ ("non A", "ne A"). Sud $\rceil A$ je istinit ako je A lažan, a lažan ako je A istinit. Pripadna tablica istinitosti je

A	$\rceil A$
$\top$	$\bot$
$\bot$	$\top$

Sve unarne operacije f_i, $i = 1, 2, 3, 4$, na $\{\top, \bot\}$ su dane tablicom:

A	$f_1(A)$	$f_2(A)$	$f_3(A)$	$f_4(A)$
$\top$	$\bot$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\top$	$\top$

Vidimo da je $f_3(A) = \neg A$.

Definicija Neka su A i B sudovi.

- Sud $A \wedge B$ ("A *i* B" ili "A *et* B") nazivamo *konjunkcija* sudova A i B. Sud $A \wedge B$ je istinit samo onda ako je istinit sud A i ako je istinit sud B. Pripadna tablica istinitosti je

A	B	$A \wedge B$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

.

- Sud $A \vee B$ ("A *ili* B", "A *vel* B") nazivamo *inkluzivna (uključiva) disjunkcija* sudova A i B. Sud $A \vee B$ je lažan samo onda ako je lažan sud A i ako je lažan sud B. Pripadna tablica istinitosti je

A	B	$A \vee B$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

Napomena: Veznik "ili" ovdje se shvaća u inkluzivnom (uključivom) smislu, tj. on dopušta također "A i B".

- Sud $A \veebar B$ ("*ili* A *ili* B", "*aut* A *aut* B") nazivamo *ekskluzivna (isključiva) disjunkcija* sudova A i B. Sud $A \veebar B$ je istinit samo onda ako je jedan od sudova A i B istinit, a drugi lažan. Pripadna tablica istinitosti je

A	B	$A \veebar B$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

Napomena: Veznik "ili" ovdje se shvaća u ekskluzivnom (isključivom) smislu, tj. on ne dopušta "A i B".

- Sud $A \Longrightarrow B$ ("*iz* A *slijedi* B", "B *je posljedica od* A") nazivamo *implikacija*. Sud $A \Longrightarrow B$ je lažan ako je sud A istinit, a B lažan. Pripadna tablica istinitosti je

A	B	$A \Longrightarrow B$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

Napomena: $A \Longrightarrow B$ se još čita: "ako je A onda je B", "A je dovoljan uvjet za B", "B je nužan uvjet za A".

- Sud $A \Longleftrightarrow B$ (" A *je ekvivalentan sa* B") nazivamo *ekvivalencija (jednakovrijednost)*. Sud $A \Longleftrightarrow B$ je istinit ako su vrijednosti istinitosti sudova A i B jednake. Pripadna tablica istinitosti je

A	B	$A \Longleftrightarrow B$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

Napomena: $A \Longleftrightarrow B$ se još čita: " A je onda i smo onda ako je B", "A je nužan i dovoljan uvjet za B",

Sve binarne operacije f_i, $i = 1, 2, ..., 16$ na $\{\top, \bot\}$ su dane tablicom:

A	B	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\top$

Vidimo da je:

- $f_{12}(A, B) = A \wedge B$,
- $f_2(A, B) = A \vee B$,
- $f_8(A, B) = A \veebar B$,
- $f_4(A, B) = A \Longrightarrow B$,
- $f_9(A, B) = A \Longleftrightarrow B$

Na sličan način, mogu se definirati *$n-$arne logičke operacije*. $n-$arna logička operacija f svakoj uređenoj $n-$ torci sudova $(A_1, ..., A_n)$ pridružuje novi sud $f(A_1, ..., A_n)$. Ukupan broj različitih $n-$arnih operacija je 2^{2^n}.

$n-$arna operacija se može zadati dvojako:

- tablicom istinitosti
- *formulom algebre sudova,* tj. kao složeni sud.

Definicija Kažemo da su dvije formule P i Q algebre sudova *logički ekvivalentne* ako imaju isti broj varijabli i iste tablice istinitosti. Pišemo $P \equiv Q$.

Poredak logičkih operacija po padajućoj snazi vezivanja dogovorno je:

$$\neg\ ,\ \wedge\ ,\ \vee\ ,\ \Longrightarrow\ ,\ \Longleftrightarrow$$

Teorem 1 Neka su A, B, C sudovi tada vrijedi:

1. idempotentnost disjunkcije i konjunkcije:

$$A \vee A \equiv A, \qquad A \wedge A \equiv A;$$

2. asocijativnost:

$$(A \vee B) \vee C \equiv A \vee (B \vee C),$$
$$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C);$$

3. komutativnost:

$$A \vee B \equiv B \vee A, \qquad A \wedge B \equiv B \wedge A;$$

4. distributivnost:

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C),$$
$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C);$$

5. De Morganove formule:

$$\rceil (A \vee B) \equiv \rceil A \wedge \rceil B \qquad \rceil (A \wedge B) \equiv \rceil A \vee \rceil \bar{B};$$

6. $A \vee \bot \equiv A, \quad A \wedge \top \equiv A;$

7. $A \vee \top \equiv \top, \quad A \wedge \bot \equiv \bot;$

8. komplementarnost:

$$A \vee \rceil A \equiv \top, \qquad A \wedge \rceil A \equiv \bot;$$

9. pravilo dvostruke negacije: $\rceil\rceil\, A \equiv A$.

Napomene:

- Sva svojstva iz prethodnog teorema imaju svojstvo dualnosti, tj. zamjenom

$$\vee \leftrightarrow \wedge \quad i \quad \bot \leftrightarrow \top$$

u jednom pravilu dobivamo drugo (valjano) pravilo.

- Zbog asocijativnosti opravdano je umjesto $(A \vee B) \vee C$ pisati $A \vee B \vee C$. Slično za $\wedge$.

Ako imamo (konačan ili beskonačan) niz sudova A_1, A_2, ..., A_n, ..., onda, zbog asocijativnosti, pišemo

$A_1 \vee A_2 \vee \ldots \vee A_n = \vee_{i=1}^{n} A_k$ (za konačan niz)

$A_1 \vee A_2 \vee \ldots \vee A_n \vee \ldots = \vee_{i=1}^{n} A_k$ (za besk. niz).

Slično za $\wedge$.

2.3 Tautologije, pravila zaključivanja

Definicija Za neku formulu P algebre sudova kažemo da je *tautologija* ako je identički istinita, tj. $P \equiv \top$.
Pišemo $\models P$ (čitamo: P je tautologija).
Formulu F algebre sudova koja identički lažna, tj. $F \equiv \bot$, nazivamo *kontradikcija (protuslovlje)* .

Dakle, formula F je kontradikcija onda i samo onda ako je $\neg F$ tautologija.

Primijedba Za dvije formule algebre sudova P i Q vrijedi $P \equiv Q$ onda i samo onda ako je $P \iff Q$ tautologija.

Neke važne tautologije:

- $\models A \vee \neg A$ (**zakon isključenja trećeg,** tj. svaka tvrdnja je ili istinita ili lažna (nema trećeg));

- $\models (A \Longrightarrow B) \wedge (B \Longrightarrow C) \Longrightarrow (A \Longrightarrow C)$ (**pravilo silogizma** ili **tranzivnost implikacije**);

- $\models \neg (A \wedge \neg A)$ (**zakon neproturječnosti);**

- $\models \neg\neg A \equiv A$ **(zakon dvostruke negacije);**

- $\models (A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)$ **(pravilo kontrapozicije);**

- $\models A \vee (A \wedge B) \Longleftrightarrow A$ i $\models A \wedge (A \vee B) \Longleftrightarrow A$ **(zakon apsorpcije ili upijanja).**

Definicija Kažemo da je sud Q *logička posljedica (zaključak)* sudova $P_1, P_2, ..., P_n$ ako iz pretpostavke da su svi sudovi istiniti slijedi da je i sud Q istinit. Pišemo:

$$P_1, P_2, ..., P_n \models Q.$$

Sudovi $P_1, P_2, ..., P_n$ se nazivaju *premise (pretpostavke)*, a sud Q *kozekvenca (posljedica, zaključak)*.

Teorem 2 Ako vrijedi $P_1, P_2, ..., P_n \models Q$ onda je $\models P_1 \wedge P_2 \wedge ... \wedge P_n \Longrightarrow Q$ i obrnuto.

Teorem 3 Za sudove A i B vrijedi

$$A,\ A \Longrightarrow B \models B.$$

Ovo pravilo zaključivanja nazivamo **modus ponens ili pravilo otkidanja.**

Teorem 4 Za sud A vrijedi

$$\rceil A \Longrightarrow \bot \ \models A$$

Ovo pravilo zaključivanja nazivamo **pravilo kontradikcije ili protuslovlja.**

Po pravilu kontrapozicije iz modus poensa dobivamo pravilo zaključivanja koje nazivamo **modus tollens** (utvrđuje nešto što nije): Za sudove A i B vrijedi

$$A \Longrightarrow B, \ \rceil B \ \models \ \rceil A.$$

Primjer:

P_1: Ako se Ana kandidira na izborima (A), ona će biti izabrana (B).

P_2 : Ako Ana dođe na sastanak (C), ona će se kandidirati na izborima (A).

P_3 : Ana će doći na sastanak (C) ili će ići u Italiju (D).

P_4 : Ana neće ići u Italiju ($\rceil D$).

Q : (Dakle,) Ana će biti izabrana (B).

2.4 Dokazi u matematici

Početkom 20 st. uvidjelo se da treba dati stroge kriterije kada će se dokaz neke tvrdnje prihvatiti ili ne prihvatiti kao valjan. Ti kriteriji koriste pravila matematičke logike.

Mnoge tvrdnje u matematici imaju jedan od oblika:

- $\models P \Longrightarrow Q$, tj. $\models P_1 \wedge P_2 \wedge ... \wedge P_n \Longrightarrow Q$

- $\models Q \Longleftrightarrow P$.

Neke vrste dokaza:

Direktni dokaz

Krenemo od pretpostavki teorema, pa koristeći pravila zaključivanja (te definicije i poznate (već dokazane) tvrdnje) dolazimo do zaključka teorema. Kod ovakvih dokaza najčešće koristimo pravilo silogizma (tranzitivnost implikacije).

Teorem P1 Ako je x paran broj onda je i x^2 paran broj.

Dokaz po kontrapoziciji

Ako je tvrdnja oblika $\models P \Longrightarrow Q$ onda je često lakše pokazati tvrdnju koja je ekvivalentna (po pravilu kontrapozicije) a to je $\models \rceil Q \Longrightarrow \rceil P$.

Teorem P2 Neka je x prirodan broj. Ako je x^2 paran broj, onda je x paran broj.

Napomena: Neke složenije tvrdnje oblika $\models P \Longrightarrow Q$ se dokazuju u konačno *međukoraka*. Npr. ako je $P \equiv P_1 \wedge P_2 \wedge ... \wedge P_n$, onda se najprije dokaže

$$\models P_1 \wedge P_2 \wedge ... \wedge P_n \Longrightarrow Q_1$$

iz toga

$$\models P_1 \wedge P_2 \wedge ... \wedge P_n \wedge Q_1 \Longrightarrow Q_2$$

i nakon konačno koraka

$$\models P_1 \wedge P_2 \wedge ... \wedge P_n \wedge Q_1 \wedge ... \wedge Q_k \Longrightarrow Q$$

Dokaz kontradikcijom

Neku tvrdnju Q možemo dokazati kontradikcijom, tj. tako da pretpostavimo da je tvrdnja $\neg Q$ točna. Koristeći pravila zaključivanja (te definicije i poznate (već dokazane) tvrdnje) dolazimo do zaključka da je tvrdnja Q točna. Sada je $Q \wedge \neg Q \equiv \top$ u suprotnosti (kontradikciji) s činjenicom $Q \wedge \neg Q \equiv \bot$.
Zaključijemo pretpostavka $\neg Q$ nije točna, dakle Q je točna. ($\neg Q \Longrightarrow \bot \models Q$.)

Teorem P3 Ne postoji racionalan broj x čiji je kvadrat jednak 2.

Dokaz ekvivalencije

Ako je tvrdnja oblika $\models P \iff Q$ onda tvrdnju dokazujemo tako da dokažemo $\models P \Longrightarrow Q$ i $\models Q \Longrightarrow P$.

Teorem P4 Neka je x prirodan broj. Tada je x paran broj ako i samo ako je x^2 paran broj.

Dokaz kontraprimjerom

Tvrdnje oblika: Za svaki x vrijedi..., pokazujemo da nisu točne kontraprimjerom, tj. nađemo x_0 za koji tvrdnja ne vrijedi.

Tvrdnja P5 Svi višekratnici od 3 su neparni.

Kontraprimjer: 6 je višekratnik od $3,$ a nije neparan.

Tvrdnja P6 Produkt svaka dva iracionalna broja je iracionalan.

Kontraprimjer: $x = \sqrt{12}$ i $y = \sqrt{3}$ su iracionalni, ali produkt $x \cdot y = \sqrt{36} = 6$ nije iracionalan.

Dokaz indukcijom

Matmatičkom indukcijom se dokazuju tvrdnje oblika: Za sve prirodne brojeve $n \geq n_0$ vrijedi da je (tvrdnja) $P(n)$ istina.

Dokaz ima tri koraka:

- *Baza indukcije* (dokazujemo da je $P(n_0)$ istina)
- *Pretpostavka indukcije* (pretpostavljamo da $P(k)$ istina za neki $k \geq n_0$)
- *Korak indukcije* (dokazujemo da je $P(k+1)$ istina koristeći pretpostavku indukcije)

Primjer: Treba pokazati da formula

$$\sum_{i=1}^{n} i = 1+2+3+...+(n-1)+n = \frac{n\,(n+1)}{2} \quad (F(n))$$

vrijedi za svaki prirodan broj $n \in \mathbb{N}$, tj. za $n \geq 1$.

Dokaz:

Baza indukcije. (Dokazujemo da je $F\,(n)$ istina za $n = 1$)

$$\sum_{i=1}^{1} i = 1 = \frac{1 \cdot (1+1)}{2}$$

Pretpostavka indukcije. (Pretpostavimo da je $F\,(n)$ istina za $n = k$)

$$\sum_{i=1}^{k} i = 1 + 2 + ... + (k-1) + k = \frac{k\,(k+1)}{2}.$$

Korak indukcije. (Pokazujemo da je $F\,(n)$ istina za $n = k+1$)

$$\begin{aligned}
\sum_{i=1}^{k+1} i \;&=\; 1 + 2 + ... + k + (k+1) \overset{P.I.}{=} \\
&= \frac{k\,(k+1)}{2} + (k+1) = \frac{k^2 + 3k + 2}{2} \\
&= \frac{(k+1)\,(k+2)}{2} = \frac{(k+1)\,((k+1)+1)}{2}
\end{aligned}$$

Dokaz postojanja (egzistencije)

Tvrdnja je oblika: Postoji x tako da je.....
Ove tvrdnje dokazujemo tako da konstruiramo objekt x koji zadovoljava traženo svojstvo.

Tvrdnja P6 Neka je matrica $A \in \mathcal{M}_n$. Ako je $\det A \neq 0$ onda je A regularna (postoji A^{-1}).

Dokaz: (skica) Definiramo (konstruiramo) matricu

$$B = \frac{1}{\det(A)} \tilde{A}^T \quad \text{(dobro def. jer je } \det A \neq 0)$$

i pokažemo da vrijedi $AB = BA = I$, pa je $B = A^{-1}$.

Dokaz jedinstvenosti

Tvrdnja je oblika: Ako objekt x sa svojstvom $P(x)$ postoji onda je jedinstven.
Ove tvrdnje dokazujemo tako da pretpostavimo da postoje dva objekta sa svojstvom $P(x)$ i onda pokažemo da su oni nužno jednaki.

Tvrdnja P7 Neka je matrica $A \in \mathcal{M}_n$. Ako postoji matrica $B \in \mathcal{M}_n$ za koju vrijedi $AB = BA = I$ onda je ona jedinstvena.

Dokaz: Sami

2.5 Skupovni prikaz algebre sudova

Definicija *Algebra sudova* je skup svih sudova S zajedno sa tri operacije na S: dvije binarne $\wedge$ i $\vee$ i jednom unarnom $\rceil$. Svojstva te algebre navedena su u Teoremu 1 (poglavlje 2.2).

Neka je X univerzalni skup. Operacije na podskupovima od X mogu se opisati pomoću logičkih operacija.
Neka su skupovi A i B (podskupovi univerzalnog skupa X), tada je:

- $A \cap B = \{x \in X : \ x \in A \wedge x \in B\}$;
- $A \cup B = \{x \in X : \ x \in A \vee x \in B\}$;
- $\bar{A} = \{x \in X : \ \rceil (x \in A)\}$;
- $A \subseteq B \equiv$ za sve $x \in X$ vrijedi $x \in A \Longrightarrow x \in B$;
- $A = B \equiv$ za sve $x \in X$ vrijedi $x \in A \Longleftrightarrow x \in B$;
- $A \triangle B = (A \cup B) \backslash (A \cap B) = \{x \in X : \ x \in A \veebar x \in B\}$ *simetrična razlika*.

Dakle, imamo analogiju (usporedba Teorema 1 (poglavlje 1.3) i Teorema 1 (poglavlje 2.2):

Sudovi	$A \wedge B$	$A \vee B$	$\neg A$	$A \Longrightarrow B$	$A \Longleftrightarrow B$	$A \veebar B$	$\bot$	$\top$
Skupovi	$A \cap B$	$A \cup B$	$\bar{A}$	$A \subseteq B$	$A = B$	$A \triangle B$	$\emptyset$	X

Ovo motivira sljedeću apstraktnu definiciju:

2.6 Booleove algebre

Definicija Neka je B skup u kojem su istaknuta dva različita elementa 0 (nula) i 1 (jedan), te neka su zadane tri operacije na B: dvije binarne $+$ (zbrajanje) i $\cdot$ (množenje) i jedna unarna $\bar{\ }$ (komplementiranje). Skup B s ove tri operacije naziva se *Booleova algebra* ako su zadovoljena svojstva:

1. idempotentnost zbrajanja i množenja:

$$a + a = a, \qquad a \cdot a = a;$$

2. asocijativnost:

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

3. komutativnost: $a + b = b + a, \qquad a \cdot b = b \cdot a;$

4. distributivnost:

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

5. De Morganove formule:

$$\overline{a + b} = \bar{a} \cdot \bar{b} \qquad \overline{a \cdot b} = \bar{a} + \bar{b};$$

6. $a + 0 = a, \quad a \cdot 1 = a;$

7. $a + 1 = 1, \quad a \cdot 0 = 0;$

8. komplementarnost: $a + \bar{a} = 1, \quad a \cdot \bar{a} = 0;$

9. involutivnost komplementarnosti: $\overline{\bar{a}} = a.$

Napomene:

- Sva svojstva iz prethodnog teorema imaju svojstvo dualnosti, tj. zamjenom

$$+ \leftrightarrow \cdot \quad i \quad 0 \leftrightarrow 1$$

  u jednom pravilu dobivamo drugo (valjano) pravilo.

- Booleovu algebru obično definiramo kao uređenu šestorku $\left(B, +, \cdot, \overline{\ .\ }, 0, 1\right)$ koja zadovoljava svojstva $1. - 9.$. Može se pokazati da je dovoljno zahtjevati da su zadovoljena svojstva $3., 4., 6., 8.$, jer sva ostala slijede iz njih.

Propozicija

a) Elementi 0 i 1 u Booleovoj algebri B određeni su jednoznačno.

b) U svakoj Booleovoj algebri vrijede *pravila apsorpcije*:

$$a + ab = a, \qquad a\,(a + b) = a$$

koja su jedno drugom dualna.

U svakoj Booleovoj algebri vrijedi:

- $1 + 1 = 1, \quad 1 + 0 = 0 + 1 = 1, \quad 0 + 0 = 0$ i dualno $0 \cdot 0 = 0, \quad 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1;$
- $\bar{0} = 1$ i $\bar{1} = 0$

Primjeri Boolovih algebri

- Ako je $B = \{\top, \bot\}$ onda je $(B, \vee, \wedge, \neg, \bot, \top)$ Boolova algebra;
- Ako je $S = \{x\}$ i $B = 2^A = \{\emptyset, S\}$ onda je $\left(B, \cup, \cap, \overline{\ .\ }, \emptyset, S\right)$ Boolova algebra;
- Ako je S bilo koji skup i $B = 2^S$ onda je

$\left(B, \cup, \cap, \overline{\cdot}, \emptyset, S\right)$ Boolova algebra;

Definicija Neka su zadane dvije Booleove algebre $\left(B_1, +, \cdot, \overline{\ .\ }, 0_1, 1_1\right)$ i $\left(B_2, +, \cdot, \overline{\ .\ }, 0_2, 1_2\right)$. Za funkciju $f : B_1 \to B_2$ kažemo da je izomorfizam Booleovih algebri B_1 i B_2 ako je bijekcija i ako za sve $a, b \in B_1$ vrijedi

$$f(a \cdot b) = f(a) \cdot f(b) \qquad \text{(i1)}$$

$$f(\bar{a}) = \overline{f(a)} \qquad \text{(i2)}$$

Propozicija Neka je $f : B_1 \to B_2$ izomorfizam Booleovih algebri, onda vrijedi

$$f(a + b) = f(a) + f(b)$$

$$f(0_1) = 0_2 \qquad \text{i} \qquad f(1_1) = 1_2.$$

Za dvije Booleove algebre B_1 i B_2 kažemo da su izomorfne ako postoji izomorfizam $f : B_1 \to B_2$. U tom slučaju kažemo da su B_1 i B_2 jednake do na izomorfizam (identificiramo ih - $a \equiv f(a)$).

Primjer Svake dvije dvočlane Booleove algebre su izomorfne, pa kažemo da, gledano do na izomorfizam, postoji samo jedna dvočlana Booleova algebra. Ta je $\left(\{0, 1\}, +, \cdot, \overline{\ .\ }\right)$, i sve ostale dvočlane identificiramo s ovom.

Primjer Neka je $B_1 = D_{30}$ skup svih djelitelja broja 30, tj. $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Definirajmo za $a, b \in D_{30}$

$a \cdot b = M(a, b)$ - najveća zajednička mjera od a i b,

$a + b = v(a, b)$ - najveći zajednički višekratnik od a i b,

$$\bar{a} = \frac{30}{a},$$

tada je $\left(D_{30}, +, \cdot, \overline{\ .\ }, 1, 30\right)$ Booleova algebra.
Neka je $S = \{x, y, z\}$ tada je $\left(2^S, \cup, \cap, \rceil, \emptyset, S\right)$ Booleova algebra. Uočimo $2^S = B_2$ ima 8 elemenata

$$2^S = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$$

Definiramo $f : D_{30} \to 2^S$ tako da je

$$f(1) = \emptyset, \quad f(30) = \{x, y, z\} = S,$$

$$f(2) = \{x\}, \ f(3) = \{y\}, \ f(5) = \{z\},$$

$f(6) = \{x, y\}$, $(f(6) = f(2 + 3) = f(2) \cup f(3) = \{x, y\})$,

$f(10) = \{x, z\}$, $(f(10) = f(2 + 5) = f(2) \cup f(5) = \{x, z\})$,

$f(15) = \{y, z\}$, $(f(15) = f(3 + 5) = f(3) \cup f(5) = \{y, z\})$.

Lako se provjeri da je $f : D_{30} \to 2^S$ izomorfizam Booleovih algebri (nije jedini- ukupno ih ima 6).

Može se pokazati da je svaka konačna Booleova algebra izomorfna nekoj algebri skupova $\left(2^S, \cup, \cap, ^\complement, \emptyset, S\right)$.

Definicija Kažemo da je B_1 podalgebra Booleove algebre $\left(B, +, \cdot, \overline{\ .\ }, 0, 1\right)$, ako je $B_1 \subseteq B$ i ako je B_1 Booleova algebra s obzirom na operacije nasljeđene iz B.

Da bi $B_1 \subseteq B$ bila podalgebra dovoljno je provjeriti da za sve $a, b \in B_1$ vrijedi

$$a \cdot b \in B_1, \qquad \bar{a} \in B_1.$$

Primjer Svaka Booleova algebra $\left(B, +, \cdot, \overline{\ .\ }, 0, 1\right)$ ima za trivijalnu podalgebru $B_1 = \{0, 1\}$.

Primjer Podalgebra Booleove algebre $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ je npr. $B_1 = \{1, 2, 15, 30\}$ (ima ih ukupno 5 različitih).

2.7 Booleove funkcije

Neka je $\left(B, +, \cdot, \overline{\cdot}, 0, 1\right)$ dvočlana Booleova algebra, tj. $B = \{0, 1\}$. Zbog lakšeg računanja (pamćenja) definirajmo: $0 < 1$. Sada operacije na B možemo definirati

$$a \cdot b = \min\{a, b\} \qquad \text{i} \qquad a + b = \max\{a, b\}.$$

Definicija Booleova funkcija (ili $n-$arna logička operacija) je bilo koja funkcija $F : B^n \to B$, gdje je $B = \{0, 1\}$.

Dakle,

$$(x_1, x_2, ..., x_n) \in B^n \xrightarrow{F} F(x_1, x_2, ..., x_n) \in B.$$

$x_1, x_2, ..., x_n$ su varijable Booleove funkcije.

Teorem 1 Broj svih Booleovih funkcija od n varijabli iznosi 2^{2^n}.

Svih Booleovih funkcija jedne varijable ima $2^{2^1} = 4$ a dane su tablicom:

x	F_1	F_2	F_3	F_4
1	0	1	0	1
0	0	0	1	1

Vidimo da je $F_3(x) = \bar{x}$.

Svih Booleovih funkcija dvije varijable ima $2^{2^2} = 16$ a dane su tablicom:

x_1	x_2	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_1
1	1	1	1	1	1	0	1	1	0	1	0	0	1	0	0
1	0	1	1	1	0	1	1	0	1	0	1	0	0	1	0
0	1	1	1	0	1	1	0	1	1	0	0	1	0	0	1
0	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0

Vidimo da je:

- $F_{12}(x_1, x_2) = x_1 \cdot x_2 \ (= x_1 \wedge x_2)$,
- $F_2(x_1, x_2) = x_1 + x_2 \ (= x_1 \vee x_2)$,
- $F_8(x_1, x_2) \ (= x_1 \veebar x_2)$,
- $F_4(x_1, x_2) \ (= x_1 \Longrightarrow x_2)$,
- $F_9(x_1, x_2) \ (= x_1 \Longleftrightarrow x_2)$
- $F_1(x_1, x_2) = 1$ (tautologija)

Primjer Skup svih Booleovih funkcija od n varijabli

$$B' = \{F \mid F : B^n \to B,\ F \text{ Booleova fja}\}$$

je Booleova algebra uz operacije $F + G$, $F \cdot G$ i $\bar{F}$ dane sa

$$\begin{aligned}
(F+G)(x_1,...,x_n) &= F(x_1,...,x_n) + G(x_1,...,x_n) \\
(F \cdot G)(x_1,...,x_n) &= F(x_1,...,x_n) \cdot G(x_1,...,x_n) \\
\bar{F}(x_1,...,x_n) &= \overline{F(x_1,...,x_n)}
\end{aligned}$$

B' ima 2^{2^n} elemenata (Teorem 1).

2.8 Disjunktivna i konjuktivna normalna forma

Svaku Booleovih funkcija možemo zadati tablicom. Pokažimo, na primjeru, da se Booleova funkcija može opisati i pomoću operacija $+, \cdot, \overline{A}$.

Primjer Neka je $F : B^3 \to B$ dana tablicom:

x_1	x_2	x_3	F
1	1	1	0
1	1	0	1
1	0	1	0
0	1	1	0
1	0	0	1
0	1	0	1
0	0	1	0
0	0	0	1

- Pogledajmo retke kojima odgovara vrijednost 1;

- U svakom takvom retku 0 pridružimo odgovarajući $\bar{x}_i$, a 1 pridružimo x_i;

- Sada uređenoj trojci, npr. $(x_1, x_2, x_3) = (1, 1, 0)$, pridružimo $x_1 \cdot x_2 \cdot \bar{x}_3$;

Vrijedi: $x_1 \cdot x_2 \cdot \bar{x}_3 = 1$ ako i samo ako je $(x_1, x_2, x_3) = (1, 1, 0)$;

- Zbrojimo sve te izraze

$$(x_1 \cdot x_2 \cdot \bar{x}_3) + (x_1 \cdot \bar{x}_2 \cdot \bar{x}_3) + (x_1 \cdot \bar{x}_2 \cdot x_3) + (\bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3)$$

Vrijednost ovog izraza je 1 ako je barem jedan od "pribrojnika" 1. Isto tako ako je jedan "pribrojnika" 1, svi ostali su 0. Dakle, imamo samo 4 mogućnosti (od 8). Prema tome ovaj izraz ima istu tablicu kao F, tj.

$$F(x_1, x_2, x_3) = x_1 x_2 \bar{x}_3 + x_1 \bar{x}_2 \bar{x}_3 + x_1 \bar{x}_2 x_3 + \bar{x}_1 \bar{x}_2 \bar{x}_3$$

Produkt varijabli poput $x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$ koji odgovara uređenoj trojci (x_1, x_2, x_3) (općenito $n-$torci) za koju je $F = 1$ nazivamo *minterm* funkcije F. Dakle, *svaka Booleova funkcija F jednaka je zbroju svojih minterma.*

Neka je $x \in B = \{0, 1\}$, onda definiramo: $x^0 = \bar{x}$, $x^1 = x$. Dakle, $1^0 = 0$, $0^0 = 1$, $1^1 = 1$, $0^1 = 0$.

Koristeći ovaj zapis imamo:

Teorem 2 Neka je $F : B^n \to B$ Booleovih funkcija i J skup svih elemenata $(e_1, e_2, ..., e_n) \in B^n$ za koje je $F(e_1, e_2, ..., e_n) = 1$. Onda je

$$F(x_1, x_2, ..., x_n) = \sum_{(e_1,e_2,...,e_n)\in J} (x_1^{e_1} \cdot x_2^{e_2} ... \cdot x_n^{e_n}). \quad (*)$$

Izraz (*) se naziva *disjunktivna normalna forma* Booleove funkcije F.

Slično, ako gledamo retke za koje je $F = 0$, onda prvom retku pridružimo $\bar{x}_1 + \bar{x}_2 + \bar{x}_3$, itd.
Vrijedi: $\bar{x}_1 + \bar{x}_2 + \bar{x}_3 = 0$ ako i samo ako je $(x_1, x_2, x_3) = (1, 1, 1)$;
Pomnožimo sve te izraze

$$(\bar{x}_1 + \bar{x}_2 + \bar{x}_3) \cdot (\bar{x}_1 + x_2 + \bar{x}_3) \cdot (x_1 + \bar{x}_2 + \bar{x}_3) \cdot (x_1 + x_2 + \bar{x}_3)$$

Vrijednost ovog izraza je 0 ako je barem jedna od zagrada 0. Isto tako ako je jedna zagrada 0, sve ostale su 1. Dakle, imamo samo 4 mogućnosti (od 8). Prema tome ovaj izraz ima istu tablicu kao F, tj.

$$F(x_1, x_2, x_3) =$$

$$= (\bar{x}_1 + \bar{x}_2 + \bar{x}_3)(\bar{x}_1 + x_2 + \bar{x}_3)(x_1 + \bar{x}_2 + \bar{x}_3)(x_1 + x_2 + \bar{x}_3)$$

Zbroj varijabli poput $\bar{x}_1 + \bar{x}_2 + \bar{x}_3$ koji odgovara uređenoj trojci (x_1, x_2, x_3) (općenito $n-$torci) za koju je $F = 0$ nazivamo *maksterm* funkcije F.

Dakle, *svaka Booleova funkcija F jednaka je umnošku svojih maksterma.*

Teorem 2 Neka je $F : B^n \to B$ Booleovih funkcija i K skup svih elemenata $(k_1, k_2, ..., k_n) \in B^n$ za koje je $F(k_1, k_2, ..., k_n) = 0$. Onda je

$$F(x_1, x_2, ..., x_n) = \prod_{(k_1,k_2,...,k_n)\in K} \left(x_1^{\bar{k}_1} + x_2^{\bar{k}_2} ... + x_n^{\bar{k}_n} \right). \qquad (**)$$

Izraz (**) se naziva *konjunktivna normalna forma* Booleove funkcije F.

Definicija Neka je $F : B^n \to B$ Booleovih funkcija. *Dualna Booleovih funkcija* od F je funkcija $F^* : B^n \to B$ definirana sa

$$F^*(x_1, x_2, ..., x_n) = \overline{F(\bar{x}_1, \bar{x}_2, ..., \bar{x}_n)}.$$

Propozicija Operacija dualnosti je involutivna, tj. $(F^*)^* = F$.

Propozicija
a) Operacije zbrajanja $+$ i množenja $\cdot$ u Booleovoj algebri su dualne.

b) Operacija komplementiranja $\bar{A}$ je involutivna.

Problem ispunjivosti

Postoji li barem jedna $n-$ torka $(x_1, x_2, ..., x_n) \in B^n$ za koju je Booleova funkcija $F : B^n \to B$ jednaka 1?

Primjer Kaže žena nakon vjenčanja svom mužu: "Bit će mir za vrijeme ručka ako ispuniš tri uvjeta:

1. Ako ne staviš kruh (A) na stol, moraš staviti i sladoled (B).
2. Ako staviš kruh (A) i sladoled (B), ne smiješ staviti krastavce (C).
3. Ako staviš krastavce (C) ili (inkl.) ne staviš kruha (A), onda ne smiješ staviti sladoled (B)."

2.8 Logički sklopovi Knjiga str. 31.

2.8 Predikatni račun

Rečenice kao:

- $P_1(x)$: " x je bio trener "Hajduka" 1971.";
- $P_2(x, y)$: "$x + y = 1$",

nisu sudovi dok simbole x i y smatramo varijablama, ali postaju sudovi (ili istiniti ili lažni) kad x i y poprime konkretne vrijednosti.

Definicija Izjavna rečenica koja sadrži jednu ili više varijabla, i koja za konkretne vrijednosti varijabla iz zadanog skupa D postaje sud, naziva se *predikat.*

Kažemo da je predikat:

- *jednomjesni* ako ima samo jednu varijablu $x \in D$;
- *dvomjesni* ako ima dvije varijable $x \in D_1$, $y \in D_2$;
- $n-$*mjesni* ako ima n varijabli $x_k \in D_k$, $k = 1, ..., n$.

  Skup $D = D_1 \times ... \times D_n$ nazivamo *domena predikata*.

Napomena

- Za svaku varijablu danog predikata pretpostavlja se da je poznat skup (domena) iz kojeg varijabla poprima svoje vrijednosti.

- Ako semantička (istinitosna) vrijednost nekog predikata ne ovisi o nekoj od varijabla, onda se ta varijabla naziva *fiktivna varijabla.*

- Iz jednostavnijih predikata, koristeći logičke operacije, gradimo *formule predikatnog računa*, koje su opet predikati;

Definicija Neka je $P(x)$ predikat i x iz zadane domene D.

- Tada je $\forall x P(x)$ *sud* koji je istinit onda i samo onda ako je sud $P(a)$ istinit za svaki $a \in D$. Sud $\forall x P(x)$ čitamo: " za svaki x je $P(x)$" ili " za svaki x vrjedi $P(x)$".
  Simbol $\forall$ nazivamo *univerzalni kvantifikator*.

- Tada je $\exists x P(x)$ *sud* koji je istinit onda i samo onda ako postoji barem jedan $a \in D$ za koji je sud $P(a)$ istinit. Sud $\exists x P(x)$ čitamo: " postoji x tako da je $P(x)$". Simbol $\exists$ nazivamo *egzistencijalni kvantifikator*.

Napomena

- Od svakog $n-$mjesnog predikata $P(x_1, ..., x_i, ..., x_n)$ s domenom $D = D_1 \times ... \times D_n$ možemo dobiti jednomjesni tako da varijablu $x_i \in D_i$ ostavimo slobodnu, a ostale fiksiramo. Dakle,

$$P(a_1, ..., a_{i-1}, x_i, a_{i+1}, ..., a_n)$$

je jednomjesni predikat, a

$$\forall x_i P(a_1, ..., a_{i-1}, x_i, a_{i+1}, ..., a_n) \qquad \text{i}$$

$$\exists x_i P(a_1, ..., a_{i-1}, x_i, a_{i+1}, ..., a_n)$$

sudovi. Prema tome, izrazi

$$\forall x_i P(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) \qquad \text{i}$$

$$\exists x_i P(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n)$$

su $(n-1)-$mjesni predikati koji *ne ovise* o varijabli x_i, tj. x_i je *vezana* kvantifikatorom.

Definicija Kažemo da je varijabla x_i u formuli predikatnog računa *vezana* ako uz nju dolazi kvantifikator $\forall$ ili $\exists$. Inače, kažemo da je x_i *slobodna* varijabla.

Napomena

- Semantička (istinitosna) vrijednost suda $\forall x P(x)$ (ili $\exists x P(x)$) ovisi o predikatu $P(x)$, dakle i o njegovoj domeni D.
  U slučaju kad treba istaknuti domenu pišemo: $(\forall x \in D)\, P(x)$ (ili $(\exists x \in D)\, P(x)$).

- Logiku predikata zanima kada će formule predikata, dobivene iz jednostavnijih predikata koristeći logičke operacije te kvantifikatore $\forall$ i $\exists$, biti ekvivalentne nad svakom domenom D ili kada će jedna formula imati drugu za logičku posljedicu nad svakom domenom D;

Teorem

a) $\rceil \forall x P(x) \equiv \exists x \rceil P(x)$;

b) $\rceil \exists x P(x) \equiv \forall x \rceil P(x)$.

Teorem

a) $\forall x \forall y R(x, y) \equiv \forall y \forall x R(x, y)$;

b) $\exists x \exists y R(x, y) \equiv \exists y \exists x R(x, y)$;

c) $\exists x \forall y R(x, y) \models \forall x \exists y R(x, y)$;

1. $\forall x \exists y R(x, y) \models \exists x \exists y R(x, y)$.

Pomoću predikata zadajemo skupove. Ako je zadan predikat $P(x)$ s domenom D, onda on definira skup A kao skup svih elemenata iz D za koji je $P(x)$ istinit, tj.

$$A = \{x \in D : P(x) \equiv \top\},$$

ili kraće $A = \{x \in D : P(x)\}$.