Matematička logika

1. Defnicija suda (i osnovne oznake)

Defnicija: Sud je svaka smislena izjavna rečenica koja može biti samo **istinita** ili **lažna**.

Oznake:

- Sudove (obično) označavamo velikim slovoma A, B, C, ...
- Svakom sudu A pridružujemo vrijednost $\top$ ako je istinit, a vrijednost $\perp$ ako je lažan.
- Vrijednost istinitosti suda A označavamo sa τ (A) i nazivamo semantička ili istinitosna vrijednost. Dakle, $\tau(A) = \top$ znači: sud A je istinit, a $\tau(A) = \perp$ znači: sud A je lažan.
- Ponekad se umjesto $\top$ i $\perp$ koristi 1 ("istina") i 0 ("laž").
- Matematičku logiku ne zanima sadržaj suda već samo njegova istinitost, pa se ponekad umjesto $\tau(A) = \top$ piše $A \equiv \top$, a umjesto $\tau(A) = \perp$ piše $A \equiv \perp$, tj. identificiramo sud s njegovom istinitošću.

2. Koje su osnovne logičke operacije (definicije)? Što su to semantičke tablice? Što su unarne i binarnie operacije, a što općenito n-arne logičke operacije?

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

Negacija je tzv. **unarna logička operacija** na skupu { $\top$, $\bot$ }, tj. ima samo jednu varijablu. Postoje ukupno četiri unarne operacije.

Binarne logičke operacije: dvama sudovima A i B pridružujemo jedan novi sud. Ima ukupno 16 binarnih operacija.

Definicija: Neka su A i B sudovi.

- Sud A $\wedge$ B ("A i B", "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: ...
- Sud A $\vee$ B ("A ili B", "A vel B") nazivamo **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: ...
- 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: ...
- Sud A $\Rightarrow$ B ("iz A slijedi B", "B je posljedica od A", "A implicira B") nazivamo **implikacija**. Sud A $\Rightarrow$ B je lažan jedino ako je sud A istinit, a B lažan. Pripadna tablica istinitosti je: ...
- Sud A $\Leftrightarrow$ B (" A je ekvivalentan sa B") nazivamo **ekvivalencija** (jednakovrijednost). Sud A $\Leftrightarrow$ B je istinit ako su vrijednosti istinitosti sudova A i B jednake. Pripadna tablica istinitosti je: ...
- **Shefeferova operacija** A $\uparrow$ B ("A šefer B") ima značenje "nije istodobno A i B". Po definiciji, ona je lažna onda i samo onda ako su A i B istiniti. Pripadna tablica istinitosti je: ...
- **Lukasiewiczeva operacija** A $\downarrow$ B ("A lukasijevič B") ima značenje "niti je A niti je B". Po definiciji, ona je istinita onda i samo onda ako su A i B lažni. Pripadna tablica istinitosti je: ...

Općenito, **n-arna logička operacija** f svakoj uređenoj n-torci sudova (A_1, A_2, ..., A_n) pridružuje novi sud f (A_1, A_2, ..., A_n). Ukupan broj različitih n-arnih operacija je 2^{2^n} .

3. Logička ekvivalentnost dviju formula algebre sudova (znati ilustrirati primjerima).

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

Primjeri:

a) $A \Rightarrow B \equiv \neg A \vee B$

b) $\neg(A \Rightarrow B) \equiv A \wedge \neg B$

c) $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

d) $A \veebar B \equiv \neg(A \Leftrightarrow B)$

e) $A \uparrow B \equiv \neg(A \wedge B)$

f) $A \downarrow B \equiv \neg(A \vee B)$

4. Osnovna pravila algebre sudova (citirati teorem i dokazati pojedina pravila). Što je to svojstvo dualnosti?

Teorem: Neka su A, B i C sudovi. Tada vrijede ova pravila algebre sudova:

1. Idempotentnost disjunkcije i konjunkcije: $A \vee A \equiv A$, $A \wedge A \equiv A$
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: $A \vee B \equiv B \vee A$, $A \wedge B \equiv B \wedge A$
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: $\neg(A \vee B) \equiv \neg A \wedge \neg B$

   $\neg(A \wedge B) \equiv \neg A \vee \neg B$
6. $A \vee \perp \equiv A$, $A \wedge \top \equiv A$
7. $A \vee \top \equiv \top$, $A \wedge \perp \equiv \perp$
8. Komplementiranost: $A \vee \neg A \equiv \top$, $A \wedge \neg A \equiv \perp$
9. Pravilo dvostruke negacije: $\neg\neg A \equiv A$

Sva navedena pravila imaju **svojstvo dualnosti:** Ako u jednom pravilu zamijenimo svuda $\vee$ sa $\wedge$ i obratno, i isto tako $\top$ sa $\perp$ i obratno, dobivamo također valjano pravilo algebre sudova.

5. Definicija tautologije i kontradikcije. Zakon isključenja trećeg, pravilo silogizma, zakon neproturječnosti, zakon dvostruke negacije, pravilo kontrapozicije, zakoni apsorpcije.

Definicija: Za neku formulu P algebre sudova kažemo da je **tautologija** ako je identički istinita, tj. $P \equiv \top$. U tom slučaju pišemo $\models P$ i čitamo: P je tautologija. Formulu F algebre sudova koja je identički lažna, tj. $F \equiv \perp$, zove se **kontradikcija** (protuslovlje).

Neke važne tautologije:

a) $\models A \lor \neg A$ (**zakon isključenja trećeg**), svaki sud je ili istinit ili lažan, trećeg nema

b) $\models (A \Rightarrow B) \land (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$ (**pravilo silogizma** ili tranzivnost implikacije)

c) $\models \neg (A \land \neg A)$ (**zakon neproturječnosti**)

d) $\models \neg\neg A \Leftrightarrow A$ (**zakon dvostruke negacije**)

e) $\models (A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ (**pravilo kontrapozicije**)

f) $\models A \lor (A \land B) \Leftrightarrow A$ i $\models A \land (A \lor B) \Leftrightarrow A$ (**zakoni apsorpcije ili upijanja**)

6. Definicija logičke posljedice. Modus ponens. Modus tollens.

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 zovu premise (pretpostavke), a sud Q kozekvenca (posljedica, zaključak).

Teorem: Za sudove A i B vrijedi: $A,\ A \Rightarrow B \models B$.

Takvo pravilo zaključivanja zove se **modus ponens** ili pravilo otkidanja.

Dokaz: Iz tablice istinosti slijedi da je $A \wedge (A \Rightarrow B) \Rightarrow B$ tautologija.

Primjedba: Prema tome modus ponens je ekvivalentan s tautologijom

$$\models A \wedge (A \Rightarrow B) \Rightarrow B$$

Tradicionalni zapis modus ponensa glasi:

$$\begin{array}{l} A \Rightarrow B \\ A \\ \hline B \end{array}$$

Teorem: Za sudove A i B vrijedi: $A \Rightarrow B, \neg B \models \neg A$.

Takvo pravila zaključivanja nazivamo **modus tollens** (utvrđuje nešto što nije).

Tradicionalni zapis modus tollensa glasi:

$$\begin{array}{l} A \Rightarrow B \\ \neg B \\ \hline \neg A \end{array}$$

7. Objasniti što je to dokaz po kontrapoziciji i dokaz kontradikcijom (ilustrirati primjerom).

Tvrdnje oblika $\models A \Rightarrow B$ se dokazuje **<u>pravilom kontrapozicije</u>** ili **indirektno** tako da se pokaže istinitost tvrdnje $\models \neg B \Rightarrow \neg A$.

<u>Primjer:</u>

Propozicija: Neka je n bilo koji cijeli broj. Ako je n^2 paran broj, onda je i n paran broj.

Dokaz: Neka je sud A "n^2 je paran broj", a sud B "n je paran broj". Treba dokazati da je istinita tvrdnja $A \Rightarrow B$. Dokazat ćemo da je istinita njoj ekvivalentnu tvrdnja: $\neg B \Rightarrow \neg A$.

Ako je B lažna tvrdnja onda je n neparan, tj. $n = 2k + 1$ za $k \in Z$, onda je $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ također neparan broj, tj. A je laž.

<u>Dokaz kontradikcijom</u> zasniva se na pravilu **kontradikcije** ili protuslovlja $\neg A \Rightarrow \perp \models A$.

Dakle, ako je točno da negacija suda A implicira laž, onda je sud A istinit.

<u>Primjer:</u>

Propozicija: $\sqrt{2}$ je iracionalan broj.

Dokaz: Neka je sud A "$\sqrt{2}$ nije racionalan broj". Pretpostavimo, protivno tvrdnji propozicije, da je istinit sud $\neg$A. Onda postoje $m, n \in N$ takvi da je $2 = \left(\frac{m}{n}\right)^2$.

Možemo uzeti, bez gubitka općenitosti, da su **m** i **n** do kraja skraćeni. Onda je broj $m^2 = 2n^2$ paran broj. Prema prethodnoj propoziciji i **m** je paran broj, tj. $m = 2k$, $k \in N$. Dalje je: $(2k)^2 = 2n^2 \Rightarrow n^2 = 2k^2 \Rightarrow$ n paran broj. Dakle, kao posljedicu tvrdnje $\neg$ A dobivamo da m i n imaju zajednički faktor 2. Budući da m i n po pretpostavci nemaju zajednički faktor, dobili smo kontradikciju $\perp$. Prema tome sud A je istinit.

8. Objasniti što je to direktni dokaz, dokaz ekvivalencije, dokaz kontraprimjerom, dokaz indukcijom, dokaz egzistencije, dokaz jedinstvenosti (primjeri).

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

$$\models A \Rightarrow B$$

Primjer:

Teorem: Ako je n paran broj onda je i n^2 paran broj.

Dokaz: Neka je sud A "n je paran broj", a sud B "n^2 je paran broj".

Ako je n paran broj, onda možemo pisati $n = 2k$ za $k \in N$. Tada vrijedi da je $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ također paran broj.

Dokaz ekvivalencije: Ako je tvrdnja oblika $\models A \Leftrightarrow B$ onda tvrdnju dokazujemo tako da dokažemo je $\models A \Rightarrow B$ i $\models B \Rightarrow A$.

Primjer:

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

Dokaz: Neka je sud A "x je paran broj", a sud B " x^2 je paran broj".

Prvi korak je dokaz tvrdnje $\models A \Rightarrow B$, a drugi korak dokaz tvrdnje $\models B \Rightarrow A$.

Dokaz kontraprimjerom: tvrdnje oblika za svaki x vrijedi ..., pokazujemo da nisu točne kontraprimjerom, tj. nađemo x_o za koji tvrdnja ne vrijedi.

Tvrdnja: Svi višekratnici od 3 su neparni.

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

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

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

Primjer: Treba pokazati da formula

$$\sum_{i=1}^{n} i = 1 + 2 + \ldots + n = \frac{(n+1)n}{2} \qquad (\ P(n)\ )$$

vrijedi za svaki prirodni broj $n \in N$, tj. za $n \geq 1$.

Dokaz:

Baza indukcije (n=1) $\qquad \sum_{i=1}^{1} i = 1 = \frac{(1+1)1}{2}$ tvrdnja istinita

Pretpostavka indukcije (n = k) $\qquad \sum_{i=1}^{k} i = 1 + 2 + \ldots + k = \frac{(k+1)k}{2}$

Korak indukcije (n = k+1) $\qquad \sum_{i=1}^{k+1} i = 1 + 2 + \ldots + k + (k+1) = \frac{(k+2)(k+1)}{2}$

$$\Rightarrow \qquad \frac{(k+1)k}{2} + (k+1) = \frac{(k+2)(k+1)}{2}$$

$$\Rightarrow \qquad \frac{(k+2)(k+1)}{2} = \frac{(k+2)(k+1)}{2}$$

Dokaz postojanja (egzistencije): Tvrdnja je oblika: Postoji x tako da je... Ove tvrdnje dokazujemo tako da konstruiramo objekt x koji zadovoljava traženo svojstvo.

Primjer:

Tvrdnja: Neka je matrica $A \in M_n$. Ako je $\det A \neq 0$, onda je A regularna matrica (postoji A^{-1}).

Dokaz: (skica) Definiramo (konstruiramo) matricu $\qquad B = \frac{1}{\det(A)} \widetilde{A}^T$

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.

Primjer:

Tvrdnja: Neka je matrica $A \in M_n$. Ako postoji matrica $B \in M_n$ za koju vrijedi $A B = B A = I$ onda je ona jedinstvena.

Dokaz: Pretpostavimo da postoji još jedna matrica $C \in M_n$ tako da je $A C = C A = I$. Tada je

$$C = C I = C (A B) = (C A) B = I B = B \quad \Rightarrow \quad C = B .$$

9. Skupovni prikaz algebre sudova (objasniti analogiju između operacija algebre skupova i operacija algebre sudova).

Definicija: Algebra sudova je skup svih sudova S zajedno sa tri operacije na S: dvije binarne $\wedge$ i $\vee$ i jednom unarnom $\neg$.

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:

- $A \cap B = \{ x \in X : x \in A \wedge x \in B \}$
- $A \cup B = \{ x \in X : x \in A \vee x \in B \}$
- $\overline{A} = \{ x \in X : \neg(x \in A) \}$
- $A \subseteq B \equiv$ za sve $x \in X$ vrijedi $x \in A \Rightarrow x \in B$
- $A = B \equiv$ za sve $x \in X$ vrijedi $x \in A \Leftrightarrow x \in B$
- $\overline{A} \cup B = \{ x \in X : x \in A \Rightarrow x \in B \}$
- $A \Delta B = \{ x \in X : x \in A \veebar x \in B \}$ (simetrična razlika)

Analogija između sudova i skupova:

Sudovi	Skupovi
$A \vee B$	$A \cup B$
$A \wedge B$	$A \cap B$
$\neg A$	$\overline{A}$
$A \Rightarrow B$	$\overline{A} \cup B$
$A \Leftrightarrow B$	$(\overline{A} \cup B) \cap (\overline{B} \cup A)$
$A \veebar B$	$A \Delta B = (\overline{A} \cap B) \cup (\overline{B} \cap A)$
$A \uparrow B$	$\overline{A \cap B}$
$A \downarrow B$	$\overline{A \cup B}$
$\top$	X univerzalni skup
$\perp$	$\emptyset$

10. Definicija Booleove algebre i primjeri. Dualnost operacija u Booleovoj algebri.

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 operacija $\bar{\ }$ (komplementiranje). Skup B s ove tri operacije naziva se Booleova algebra ako su zadovoljena svojstva:

1. Idempotentnost zbrajanja i množenja: $a + a = a$, $a \cdot a = a$
2. Asocijativnost: $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Komutativnost: $a + b = b + a$, $a \cdot b = b \cdot a$
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: $\overline{a + b} = \bar{a} \cdot \bar{b}$, $\overline{a \cdot b} = \bar{a} + \bar{b}$
6. $a + 0 = a$, $a \cdot 1 = a$
7. $a + 1 = 1$, $a \cdot 0 = 0$
8. Komplementiranost: $a + \bar{a} = 1$, $a \cdot \bar{a} = 0$
9. Involutivnost komplementiranja: $\bar{\bar{a}} = a$

Booleova algebra se obično definira kao uređena šestorka $(B, +, \cdot, \bar{\ }, 0, 1)$ s prethodno navedenim svojstvima. Često se Booleovu algebru označava kratko samo sa B.

Primjeri Booleovih algebri:

- Ako je $B = \{\perp, \top\}$, onda je $(B, \vee, \wedge, \neg, \perp, \top)$ Booleova algebra
- Ako je S bilo koji skup i $B = 2^S$ onda je $(B, \cup, \cap, \bar{\ }, \emptyset, S)$ Booleova algebra

Iz definicije je vidljivo da sva navedena pravila Booleove algebre imaju **svojstvo dualnosti**: ako u jednom pravilu zamjenimo svuda + sa · i obratno, i isto tako 0 sa 1 i obratno, dobivamo drugo valjano pravilo algebre sudova.

11. Jedinstvenost nule i jedinice u Booleovoj algebri i pravila apsorpcije (iskaz i dokaz propozicije).

Propozicija:

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

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

$$a + a \cdot b = a \qquad \text{i} \qquad a \cdot (a + b) = a$$

koja su međusobno dualna.

Dokaz:

a) Neka su 0_1 i 0_2 dvije nule u B. Onda iz svojstva $a + 0 = 0 + a = a$ slijedi:

$$0_2 + 0_1 = 0_1 + 0_2 = 0_2$$

$$0_1 + 0_2 = 0_2 + 0_2 = 0_1$$

odakle slijedi da je $0_1 = 0_2$.

Neka su 1_1 i 1_2 dvije jedinice u B. Iz svojstva $a \cdot 1 = 1 \cdot a = a$ slijedi:

$$1_1 \cdot 1_2 = 1_2 \cdot 1_1 = 1_1$$

$$1_2 \cdot 1_1 = 1_1 \cdot 1_1 = 1_2$$

odakle slijedi da je $1_1 = 1_2$.

b) Vrijedi da je: $a + a \cdot b = a \cdot 1 + a \cdot b = a \cdot (1 + b) = a \cdot 1 = a$

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

12. Definicija izomorfizma Booleovih algebri (ilustrirati primjerima dvočlanih Booleovih algebri, te Booleovih algebri D_{30} i $2^{\{x,y,z\}}$).

Definicija: Neka su zadane dvije Booleove algebre $(B_1, +, \cdot, \bar{\ }, 0_1, 1_1)$ i $(B_2, +, \cdot, \bar{\ }, 0_2, 1_2)$. 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:

$$f(a \cdot b) = f(a) \cdot f(b) \quad \text{i} \quad f(\bar{a}) = \overline{f(a)} \quad .$$

Za funkciju f vrijede i pravila: $f(a + b) = f(a) + f(b)$, $f(0_1) = 0_2$ i $f(1_1) = 1_2$.

Svake dvije **dvočlane Booleove algebre** su izomorfne.

Primjer: Neka su $B_1 = \{0, 1\}$ i $B_2 = \{\bot, \top\}$ dvočlani skupovi Booleovih algebri.
Tada je funkcija $f : B_1 \to B_2$ definirana sa: $\quad f(0) = \bot \quad , \quad f(1) = \top$
izomorfizam Booleovih algebri.

Primjer: Neka $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ skup svih djelitelja broja 30 te neka za svaki $a, b \in D_{30}$ vrijedi:

$$a \cdot b = \text{Nzm}(a, b) \quad ; \quad a + b = \text{nzv}(a, b) \quad ; \quad \bar{a} = \frac{30}{a} \quad ,$$

onda je $(D_{30}, +, \cdot, \bar{\ }, 1, 30)$ Booleova algebra.

Ako je $S = \{x, y, z\}$, tada je $(2^S, \cup, \cap, \bar{\ }, \emptyset, S)$ Booleova algebra, gdje je $2^S = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$.

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

$$f(1) = \emptyset \quad , \quad f(30) = \{x, y, z\}$$
$$f(2) = \{x\} \quad , \quad f(3) = \{y\} \quad , \quad f(5) = \{z\}$$
$$f(6) = f(2 + 3) = f(2) \cup f(3) = \{x, y\}$$
$$f(10) = f(2+5) = f(2) \cup f(5) = \{x, z\}$$
$$f(15) = f(3 + 5) = f(3) \cup f(5) = \{y, z\}$$

Lako se vidi da je $f : D_{30} \to 2^S$ izomorfizam Booleovih algebri. To nije jedini mogući izomorfizam, ima ih ukupno 6. Elementima 2, 3 i 5 se mogu x, y i z pridružiti na 6 različitih načina.

13. Definicija Booleove podalgebre (ilustrirati primjerom).

Definicija: Kažemo da je B_1 podalgebra Booleove algebre $(B, +, \cdot, \bar{\ }, 0, 1)$ ako je $B_1 \subseteq B$ i ako je B_1 Booleova algebra s obzirom na sve tri operacije naslijeđene iz B. To znači da za sve $a, b \in B_1$ vrijedi da je:

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

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

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

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

Primjer 2: Podalgebra Booleove algebre $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ je npr. $B_1 = \{1, 2, 15, 30\}$. Ima ukupno 5 različitih podalgebri.

14. Booleove funkcije n varijabli: koliko ih ima različitih i kakve operacije s njima možemo definirati?

Definicija: Booleova funkcija je bilo koja funkcija n varijabli $F : B^n \rightarrow B$, gdje je $B = \{0, 1\}$. Zove se još i **n-arna logička operacija**.

Teorem: Booleovih funkcija od n varijabli ima ukupno 2^{2^n}.

S Booleovim funkcijama možemo definirati operacije:

$$(F + G)(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n) + G(x_1, x_2, \ldots, x_n)$$

$$(F \cdot G)(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n) \cdot G(x_1, x_2, \ldots, x_n)$$

$$\overline{F}(x_1, x_2, \ldots, x_n) = \overline{F(x_1, x_2, \ldots, x_n)}$$

15. Minterm i maksterm Booleove funkcije. Disjunktivna i konjunktivna normalna forma (citirati teoreme).

Neka je Booleova funkcija $F : B^3 \to B$ zadana tablicom.
Svakoj uređenoj trojci (x_1, x_2, x_3), za koju je F=1, pridružujemo umnožak varijabli poput umnoška $x_1 \cdot x_2 \cdot \overline{x}_3$ koji se pridružuje trojci (1, 1, 0). Ovakav produkt varijabli zovemo **minterm** funkcije F. **Svaka Booleova funkcija jednaka je zbroju svih svojih minterma.**

Slično, ako gledamo retke za koje je F = 0, onda se npr. trojci (0, 1, 0) pridruži zbroj varijabli $x_1 + \overline{x}_2 + x_3$. Ovakav zbroj varijabli zovemo **maksterm** funkcije F. **Svaka Booleova funkcija jednaka je umnošku svih svojih maksterma.**

Ista procedura vrijedi općenito. Da bismo je točno opisali, uvodimo nove oznake. Naka je $x \in \{0, 1\}$. Onda definiramo $x^0 = \overline{x}$, $x^1 = x$.

Teorem: Neka je $F : B^n \to B$ Booleova 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:

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

Ovaj izraz se zove **disjunktivna normalna forma** Booleove funkcije F.

Teorem: Neka je $F : B^n \to B$ Booleova 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:

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

Ovaj izraz se zove **konjunktivna normalna forma** Booleove funkcije F.

16. Problem ispunjivosti za Booleovu funkciju.

Problem ispunjivosti za Booleovu funkciju $F : B^n \rightarrow B$ je slijedeći: postoji li barem jedna n-torka $(x_1, x_2, ..., x_n) \in B^n$ takva da je $F(x_1, x_2, ..., x_n) = 1$.

17. Koji su osnovni logički sklopovi? Što su ekvivalentni logički sklopovi? Realizacija logičkih izraza pomoću logičkih sklopova.

Osnovni logički sklopovi su: a) I (konjunkcija)

b) ILI (disjunkcija)

c) NI

d) NILI

e) Invertor (negacija)

Definicija: Za dva logička sklopa kažemo da su **ekvivalentni sklopovi** ako imaju isti broj ulaznih varijabli, te ako uz ista ulazna stanja daju jednake izlaze.

Pomoću logičkih sklopova mogu se realizirati vrlo složeni logički izrazi koji ovise o velikom broju varijabli.

18. Predikati, kvantifikatori, negacija predikata.

Definicija: Izjavna rečenica koja sadrži jednu ili više varijabli, i koja za konkretne vrijednosti varijabli iz zadanog skupa D postaje sud, naziva se **predikat**. Skup D se zove **karakteristični skup predikata**.

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 $x_k \in D_k$, $k = 1, 2, \dots n$

Skup $D = D_1 \times D_2 \times \dots \times D_n$ nazivamo **domena predikata**.

Definicija: Neka je P (x) predikat i $x \in D$.

- Onda sa $\forall x\ P(x)$ označavamo **sud** koji je istinit onda i samo onda ako je sud P(a) istinit za svaki $a \in D$. Simbol $\forall$ nazivamo **univerzalni kvantifikator**.
- Sa $\exists x\ P(x)$ označavamo sud koji je istinit onda i samo onda ako postoji barem jedan $a \in D$ za koji je sud P (a) istinit. Simbol $\exists$ nazivamo **egzistencijalni kvantifikator**.

Teorem: Za predikate P(x) vrijede DeMorganove formule:

a) $\neg \forall x\ \ P(x) \equiv \exists x\ \ \neg P(x)$

b) $\neg \exists x\ \ P(x) \equiv \forall x\ \ \neg P(x)$

Primjedba: Sud $\forall x \left[\exists y\, P(x, y) \right]$ kraće pišemo $\forall x\, \exists y\, P(x, y)$. Njegova negacija je $\exists x\, \forall y\ \ \neg P(x, y)$.