TEORIJSKE OSNOVE INFORMATIKE(2010/11),
KOLOKVIJUM I, 26. novembar 2010.
GRUPA I

1. Da li postoji iskazna formula $F$ takva da važi $(F \Rightarrow p) \sim (q \Rightarrow (\neg p \vee q))$ i $((r \Rightarrow q) \Rightarrow p) \sim (F \Rightarrow \neg p)$? Ako postoji takva iskazna formula dati jedan primer.

2. Naći model za skup formula: $\{(\forall x)\neg R(x,x), (\exists x)(\forall y)\neg R(y,x), (\forall x)(\exists y)(\exists z)(R(x,y) \wedge \neg R(x,z)), (\exists x)(\exists y)(x \neq y \wedge \neg R(x,y) \wedge \neg R(y,x))\}$, gde je $R$ relacijski simbol.

**Rešenja.**

1. Primetimo da za valuaciju $\alpha : \begin{pmatrix} p & q & r \\ \bot & \top & \top \end{pmatrix}$ važi da je $v_\alpha((r \Rightarrow q) \Rightarrow p) = \bot$, i $v_\alpha(F \Rightarrow \neg p) = \top$, Odakle sledi da formule $(r \Rightarrow q) \Rightarrow p$ i $F \Rightarrow \neg p$ nisu tautološki ekvivelentne. Prema tome, ne postoji iskazna formula $F$ koja ispunjava uslove zadatka.

2. 
   - $(\forall x)\neg R(x,x)$ je tačna u interpretaciji u kojoj $(a,a) \notin \overline{R}$ za sve elemente $a$ iz domena (u tablici relacije $\overline{R}$ na glavnoj dijagonali se nalaze samo $\bot$);
   - $(\exists x)(\forall y)\neg R(y,x)$ je tačna u interpretaciji u kojoj relacija $\overline{R}$ ima osobinu da postoji elemenat $a$ iz domena takav da se ne pojavljuje u uredjenim parovima relacije $\overline{R}$ kao druga koordinata (u tablici relacije $\overline{R}$ postoji kolona u kojoj sva polja imaju vrednost $\bot$);
   - $(\forall x)(\exists y)(\exists z)(R(x,y) \wedge \neg R(x,z))$ je tačna u interpretaciji u kojoj relacija $\overline{R}$ ima osobinu da za svaki elemenat $a$ iz domena postoje elementi $b$ i $c$ iz domena takvi da $(a,b) \in \overline{R}$ i $(a,c) \notin \overline{R}$ (u tablici relacije $\overline{R}$ u svakoj vrsti postoji polje sa vrednosti $\top$ i polje sa $\bot$);
   - $(\exists x)(\exists y)(x \neq y \wedge \neg R(x,y) \wedge \neg R(y,x))$ je tačna u interpretaciji u kojoj relacija $\overline{R}$ ima osobinu da postoje različiti elementi $a$ i $b$ iz domena takvi da $(a,b),(b,a) \notin \overline{R}$ (u tablici relacije $\overline{R}$ postoje dva polja van dijagonale koja su simetrična u odnosu na glavnu dijagonalu i imaju vrednost $\bot$).

   Tada je $(\{a,b,c\}, \overline{R})$ traženi model gde je $\overline{R} = \{(a,b),(b,a),(c,a)\}$ (

   | $\overline{R}$ | a | b | c |
   |---|---|---|---|
   | a | $\bot$ | $\top$ | $\bot$ |
   | b | $\top$ | $\bot$ | $\bot$ |
   | c | $\top$ | $\bot$ | $\bot$ |

   )

# DRUGI KOLOKVIJUM IZ TEORIJSKIH OSNOVA INFORMATIKE I

## kod prof. Gradimira Vojvodića
## januar 2011

**Grupa P.Djapić**

1. Relacija $\rho_n$ na skupu prirodnih brojeva $\mathbb{N}$ definisana je (za fiksiran prirodan broj $n$) na sledeći način:
$$(x,y) \in \rho_n \text{ ako i samo ako } x < y - 2n.$$
Dokazati za $n, m \in \mathbb{N}$:
   (a) $\rho_n$ je tranzitivna relacija;
   (b) $\rho_m \circ \rho_n \subseteq \rho_{m+n}$;
   (c) $\rho_m \circ \rho_n \neq \rho_{m+n}$;

2. Neka je $A$ neprazan skup. Definiše se preslikavanje $f : \mathcal{P}(A^3) \to \mathcal{P}(A^3)$ na sledeći način: $f(X) = \{(a,b,c) \in A^3 : (\exists d \in A)(a,b,d) \in X\}$. Ako je $D = \{(a,b,b) : a,b \in A\}$, dokazati da je $f(D \cap X) \cap f(D \cap \overline{X}) = \emptyset$ za svaki skup $X \subseteq A^3$.

**Rešenja.**

1. (a) Neka je $(a,b),(b,c) \in \rho_n$. Pokažimo da $(a,c) \in \rho_n$. Na osnovu definicije relacije $\rho_n$ imamo da je $a < b - 2n$ i $b < c - 2n$, odakle sledi da je $a < (c-2n) - 2n < c - 2n$, tj. $(a,c) \in \rho_n$.
   (b) Neka $(a,b) \in \rho_m \circ \rho_n$. Tada postoji prirodan broj $c$ takav da je $(a,c) \in \rho_m$ i $(c,b) \in \rho_n$, odakle sledi da je $a < c - 2m$ i $c < b - 2n$. Kombinovanjem ove dve nejednakosti dobijamo da je $a < (b-2n) - 2m = b - 2(m+n)$, pa je $(a,b) \in \rho_{m+n}$.
   (c) Primetimo da $(1, 2(m+n)+2) \in \rho_{m+n}$ i pretpostavimo da $(1, 2(m+n)+2) \in \rho_m \circ \rho_n$, tj. da postoji prirodan broj $a$ takav da $(1,a) \in \rho_m$ i $(a, 2(m+n)+2) \in \rho_n$. Tada važi da je $2m < a-1$ i $2n < 2(m+n)+2-a$, tj. $2m \leq a-2$ i $2n \leq 2(m+n)+1-a$. Direktno sledi da je $2m+2n \leq a-2+2(m+n)+1-a = 2(m+n)-1$, kontradikcija.

2. Neka $(x,y,z) \in f(D \cap X) \cap f(D \cap \overline{X})$, tj. $(x,y,z) \in f(D \cap X)$ i $(x,y,z) \in f(D \cap \overline{X})$. Na osnovu definicije funkcije $f$ zaključujemo da postoje $t, v \in A$ takavi da $(x,y,t) \in D \cap X$ i $(x,y,v) \in D \cap \overline{X}$, ali tada sledi da $(x,y,t),(x,y,v) \in D$, pa je $t = y = v$. Medjutim, tada $(x,y,y) = (x,y,t) \in X$ i $(x,y,y) = (x,y,v) \in \overline{X}$, kontradikcija.

TEORIJSKE OSNOVE INFORMATIKE(2010/11),
POPRAVNI KOLOKVIJUM - **Deo I**, 2. februar 2011.
**Grupa P.Djapić**

1. Da li postoji iskazna formula $F$ takva da važi $(F \Rightarrow (p \vee \neg q)) \sim (F \vee (q \vee \neg r))$ ? Ako postoji takva iskazna formula dati jedan primer.

2. Da li je valjana formula: $(\exists x)(\forall y)R(x,y) \wedge (\exists x)(\exists y)(x \neq y \wedge \neg R(x,y) \wedge \neg R(y,x)) \Rightarrow (\forall x)(\exists y)(\exists z)(R(x,y) \wedge \neg R(x,z))$.

**Rešenja.**

1. *Prvo rešenje:* Formula $p \vee \neg q$ je netačna za valuaciju $v(p) = \perp$, $v(q) = \top$ i proizvoljno $v(r)$, pa ako uzmemo da je formula $F$ netačna samo za te dve valuacije slediće da su formule $F \Rightarrow (p \vee \neg q)$ i $F \vee (q \vee \neg r)$ tautologije, odakle sledi da su te dve formule tautološki ekvivalentne. Za iskaznu formulu $F$ možemo uzeti $(p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r)$.

   *Drugo rešenje:* Neka je
   $A \equiv p \vee \neg q$,
   $B \equiv F \Rightarrow (p \vee \neg q)$,
   $C \equiv (q \vee \neg r)$,
   $D \equiv F \vee (q \vee \neg r)$,
   $E \equiv B \Leftrightarrow D$. Tada je:

| $p$ | $q$ | $r$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
|---|---|---|---|---|---|---|---|---|
| $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top/\underline{\perp}$ |
| $\top$ | $\top$ | $\perp$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top/\underline{\perp}$ |
| $\top$ | $\perp$ | $\top$ | $\top$ | $\top$ | $\perp$ | $F$ | $F$ | $\underline{\top}$ |
| $\top$ | $\perp$ | $\perp$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top/\underline{\perp}$ |
| $\perp$ | $\top$ | $\top$ | $\perp$ | $\neg F$ | $\top$ | $\top$ | $\neg F$ | $\underline{\perp}$ |
| $\perp$ | $\top$ | $\perp$ | $\perp$ | $\neg F$ | $\top$ | $\top$ | $\neg F$ | $\underline{\perp}$ |
| $\perp$ | $\perp$ | $\top$ | $\top$ | $\top$ | $\perp$ | $F$ | $F$ | $\underline{\top}$ |
| $\perp$ | $\perp$ | $\perp$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top$ | $\top/\underline{\perp}$ |

   Da bi formula $E$ bila tautologija za izbor formule $F$ postoji $2^4$ do na ekvivalenciju mogućnosti. Jedno rešenje za formulu $F$ u KDF obliku bi bilo $(p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$ čija funkcija odgovara koloni $F$ u tabeli sa podvučenim simbolima. Ovako izabrana formula je jedno rešenje za $F$.

2. 
   - $(\exists x)(\forall y)R(x,y)$ je tačna u interpretaciji u kojoj relacija $\overline{R}$ ima osobinu da postoji elemenat $a$ koji je u relaciji sa svim elementima domena (u tablici relacije $\overline{R}$ postoji vrsta u kojoj sva polja imaju vrednost $\top$);
   - $(\exists x)(\exists y)(x \neq y \wedge \neg R(x,y) \wedge \neg R(y,x))$ je tačna u interpretaciji u kojoj relacija $\overline{R}$ ima osobinu da postoje različiti elementi $a$ i $b$ iz domena takvi da $(a,b),(b,a) \notin \overline{R}$ (u tablici relacije $\overline{R}$ postoje dva polja van dijagonale koja su simetrična u odnosu na glavnu dijagonalu i imaju vrednost $\perp$).
   - $(\forall x)(\exists y)(\exists z)(R(x,y) \wedge \neg R(x,z))$ je tačna u interpretaciji u kojoj relacija $\overline{R}$ ima osobinu da za svaki elemenat $a$ iz domena postoje elementi $b$ i $c$ iz domena takvi da $(a,b) \in \overline{R}$ i $(a,c) \notin \overline{R}$ (u tablici relacije $\overline{R}$ u svakoj vrsti postoji polje sa vrednosti $\top$ i polje sa $\perp$);

   Tada je $(\{a,b,c\},\overline{R})$ traženi kontra model gde je $\overline{R} = \{(a,a),(b,b),(c,c),(a,b),(b,a),(a,c),(c,a)\}$

| $\overline{R}$ | a | b | c |
|---|---|---|---|
| a | $\top$ | $\top$ | $\top$ |
| b | $\top$ | $\top$ | $\perp$ |
| c | $\top$ | $\perp$ | $\top$ |

   ), zato što je prva formula tačna jer prva vrta svuda ima vrednost $\top$, druga formula je tačna jer postoje dva $\perp$ koja su postavljena simetrično u odnosu na glavnu dijagonalu, i treća formula nije tačna jer u prvoj vrsti ne postoji $\perp$.

TEORIJSKE OSNOVE INFORMATIKE(2010/11),
POPRAVNI KOLOKVIJUM - **Deo II**, 2. februar 2011.
**Grupa P.Djapić**

1. Neka je $\rho$ relacija na skupu $A$ takva da je $\rho = (\rho \circ \rho^{-1}) \cup \triangle_A$. Dokazati da je $\rho$ relacija ekvivalencije.

2. Funkcije $g : R \to R^+$ i $h : R^+ \to R^+$ ($R^+$ je skup pozitivnih realnih brojeva) date su sa $g(x) = e^{-x}$ i $h(x) = \frac{1}{x}$. Da li je $h \circ g : R \to R^+$ bijekcija?

**Rešenja.**

1. Pokažimo da je $\rho$ relacija ekvivalencije.

   R: Kako je $\triangle \subseteq (\rho \circ \rho^{-1}) \cup \triangle = \rho$ sledi da je $\rho$ refleksivna relacija.

   S: $\rho^{-1} = ((\rho \circ \rho^{-1}) \cup \triangle)^{-1} = (\rho \circ \rho^{-1})^{-1} \cup \triangle^{-1} = ((\rho^{-1})^{-1} \circ \rho^{-1}) \cup \triangle = (\rho \circ \rho^{-1}) \cup \triangle = \rho$, odakle sledi da je $\rho$ simetrična relacija.

   T: Iz simetričnosti relacije $\rho$ ($\rho = \rho^{-1}$) sledi da je $\rho \circ \rho = \rho \circ \rho^{-1} \subseteq (\rho \circ \rho^{-1}) \cup \triangle = \rho$, odakle sledi da je $\rho$ tranzitivna relacija.

2. Pogledati kako smo na vežbama pokazali da su funkcije $f$ i $g$ bijekcije, a kako znamo da je kompozicija funkcija koje su bijekcije ponovo bijekcija sledi da je $h \circ g$ bijekcija.

ALGEBRA ZA INFORMATIČARE(2010/11),
Prvi deo, 21. april 2011.

1. Da li je moguće dopuniti Kejlijevu tablicu

| $\star$ | a | b | c |
|---|---|---|---|
| a | | | |
| b | | a | |
| c | | | b |

tako da $(\{a, b, c\}, \star)$ bude grupa? Obrazložiti.

2. Ako je $(P, +, \cdot)$ prsten, dokazati da je $Z(P) = \{r \in P : (\forall x \in P) rx = xr\}$ (tzv. centar prstena) njegov potprsten.

**Rešenja.**

1. Pretpostavimo da se data Kejlijeva tablica može dopuniti tako da dobijemo grupu. Svaka grupa ima neutralni element. Kako je $b \star b = a$ i $c \star c = b$ sledi da $b$ i $c$ nisu neutralni elementi, dakle, sledi da je $a$ neutralni element, pa imamo

| $\star$ | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | a | |
| c | c | | b |

.

   Na vezbama smo pokazali da je svaka grupa kvazigrupa i da vaze zakoni kancelacije, odakle sledi da su u Kejlijevoj tablici u svakoj vrsti i svakoj koloni različiti elementi. Medjutim, kako god izabrali vrednost izraza $b \star c$ dobijamo da će se u drugoj vrsti ili trećoj koloni ponavljati elementi.

   Na primer, jednačina $b \star x = c$ ima jedinstveno rešenje, a na osnovu gore dopunjene tablice dobijamo da mora biti $x = c$, ali tada važi da je $a \star c = b \star c = c$ pa na osnovu kancelacije je $a = b$, kontardikcija. Dakle, $(\{a, b, c\}, \star)$ ne može biti grupa.

2. Na predavanju je pokazano da je dovoljno pokazati da $0 \in Z(P)$ i $(\forall a, b \in Z(P)) a - b, ab \in Z(P)$.

   Kako je $0x = 0 = x0$ sledi da $0 \in Z(P)$. Neka $a, b \in Z(P)$, pa za svako $x \in P$ važi $ax = xa$ i $bx = xb$. Tada važi $(a - b)x = ax - bx = xa - xb = x(a - b)$, pa $a - b \in Z(P)$, i $abx = axb = xab$, pa $ab \in Z(P)$.

ALGEBRA ZA INFORMATIČARE(2010/11),
Drugi deo, 3. jun 2011.

1. Faktorisati polinom $x^5 - 3x^3 - 6x^2 - 28x - 24$ na nesvodljive faktore nad poljem realnih i kompleksnih brojeva, ako se zna da ima bar dve racionalne nule.

2. Odrediti ostatak pri deljenju broja $2005^{2011} + 2011^{2005}$ sa 7.

**Rešenja.**

1. Posto je polinom neparnog stepena (petog) i ima bar dve realne nule, sledi da taj polinom ima bar tri realne nule (jer ne može imati tri nerealne nule). Kako polinom ima bar dve racionalne nule, sledi da su potencijalni kandidati za racionalne nule delioci broja 24 (jer je koeficijent uz $x^5$ jednak jedinici). Hornerovom šemom dobijamo:

| | 1 | 0 | −3 | −6 | −28 | −24 |
|---|---|---|---|---|---|---|
| −1 | 1 | −1 | −2 | −4 | −24 | 0 |
| −2 | 1 | −3 | 4 | −12 | 0 | |
| 3 | 1 | 0 | 4 | 0 | | |

, tj. $x^5 - 3x^3 - 6x^2 - 28x - 24 = (x + 1)(x + 2)(x - 3)(x^2 + 4)$, a $x^2 + 4$ se ne može faktorisati nad poljem realnih brojeva, dok nad poljem kompleksnih brojeva tražena faktorizacija izgleda ovako $(x + 1)(x + 2)(x - 3)(x + 2i)(x - 2i)$.

2. Kako je

$$
\begin{array}{rlrl}
2005 & \equiv 3 (mod\ 7) & 2011 & \equiv 2 (mod\ 7) \\
3^1 & \equiv 3 (mod\ 7) & 2^1 & \equiv 2 (mod\ 7) \\
3^2 & \equiv 2 (mod\ 7) & 2^2 & \equiv 4 (mod\ 7) \\
3^3 & \equiv -1 (mod\ 7) & 2^3 & \equiv 1 (mod\ 7) \\
(3^3)^{670} & \equiv (-1)^{670} (mod\ 7) & (2^3)^{668} & \equiv 1^{668} (mod\ 7) \\
3^{2010} & \equiv 1 (mod\ 7) & 2^{2004} & \equiv 1 (mod\ 7) \\
3^{2011} & \equiv 3 (mod\ 7) & 2^{2005} & \equiv 2 (mod\ 7) \\
2005^{2011} & \equiv 3 (mod\ 7) & 2011^{2005} & \equiv 2 (mod\ 7)
\end{array}
$$

   sledi da je $2005^{2011} + 2011^{2005} \equiv 3 + 2 (mod\ 7)$, pa je traženi ostatak 5.

ALGEBRA ZA INFORMATIČARE(2010/11),
Prvi deo, 23. jun 2011.

1. Dokazati da je $f : Z \to \{\top, \bot\}$ zadato sa

$$f(x) = \begin{cases} \top, & x \text{ je paran} \\ \bot, & x \text{ je neparan} \end{cases}$$

homomorfizam grupoida $(Z, \cdot)$ i $(\{\top, \bot\}, \vee)$.

2. Neka je $f : P \to R$ homomorfizam prstena $(P, +, \cdot)$ i $(R, +, \cdot)$. Dokazati da je $K(f) = \{x \in P : f(x) = 0\}$ (jezgro homomorfizma $f$) ideal prstena $(P, +, \cdot)$.

**Rešenja.**

1. Treba pokazati da za svako $x, y \in Z$ važi da je $f(x \cdot y) = f(x) \vee f(y)$. Razmotrimo sve slučajeve.

Prvi slučaj: Neka su $x$ i $y$ iste parnosti. Tada je i $x \cdot y$ iste parnosti kao i $x$ i $y$, pa je $f(x \cdot y) = f(x) = f(y)$, ali kako je operacija $\vee$ idempotentna ($a \vee a = a$)sledi da je $f(x \cdot y) = f(x) = f(x) \vee f(x) = f(x) \vee f(y)$.

Drugi slučaj: Neka su $x$ i $y$ različite parnosti. Tada je $x \cdot y$ paran broj, pa je $f(x \cdot y) = \top$, i $f(x)$ i $f(y)$ imaju različite vrednosti ($\{f(x), f(y)\} = \{\top, \bot\}$), pa je $f(x) \vee f(y) = \top$, odakle sledi da je $f(x \cdot y) = \top = f(x) \vee f(y)$.

2. Kako je $f(0_P) = 0_R$ sledi da $0_P \in K(f)$.

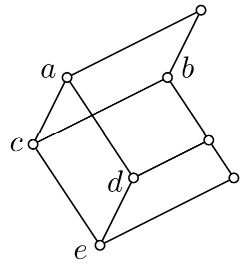
Neka $a, b \in K(f)$, tada je $f(a - b) = f(a + (-b)) = f(a) + f(-b) = f(a) + (-f(b)) = f(a) - f(b) = 0_R - 0_R = 0_R$,odakle sledi da $a - b \in K(f)$.

Neka $a \in K(f)$ i $b \in P$, tada je $f(a \cdot b) = f(a) \cdot f(b) = 0_R \cdot f(b) = 0_R$, odakle sledi $a \cdot b \in K(f)$.

Dakle, $K(f)$ je ideal prstena $(P, +, \cdot)$.

ALGEBRA ZA INFORMATIČARE(2010/11),
Drugi deo, 23. jun 2011.

1. Da li je uredjeni skup kome odgovara sledeći Hase-dijagram mreža? Obrazložiti.




2. U polju $\mathbb{Z}_3$ rešiti sistem jednačina:

$$\begin{aligned} y + t &= 2 \\ x + y + z &= 0 \\ x + z + t &= 0 \\ 2y + z + t &= 1 \end{aligned}$$

**Rešenja.**

1. Uredjeni skup kome odgovara dati Hase-dijagram nije mreža jer za elemente $a$ i $b$ ne postoji infimum, preciznije, elementi $c$, $d$ i $e$ su jedini elementi koji su manji i od $a$ i od $b$, a medju njima nema najvećeg elementa.

2. Rešimo Gausovim metodom:

$$\begin{aligned} y + t &= 2 \\ x + y + z &= 0 \\ x + z + t &= 0 \\ 2y + z + t &= 1 \end{aligned}$$

Zamenimo mesta prvim dvema jednacinama.

$$\begin{aligned} x + y + z &= 0 \\ y + t &= 2 \\ x + z + t &= 0 \\ 2y + z + t &= 1 \end{aligned}$$

Pomnožimo prvu jednačinu sa 2 i dodamo trećoj.

$$\begin{aligned} x + y + z &= 0 \\ y + t &= 2 \\ 2y + t &= 0 \\ 2y + z + t &= 1 \end{aligned}$$

Zatim drugu jednačinu pomnozimo sa 1 i dodamo trećoj i četvrtoj.

$$\begin{aligned} x + y + z &= 0 \\ y + t &= 2 \\ 2t &= 2 \\ z + 2t &= 0 \end{aligned}$$

Dalje iz treće jednačine dobijamo da je $t = 1$, zatim iz četvrte $z = -2t = t = 1$, iz druge $y = 2 - t = 2 + 2t = 2 + 2 = 1$, i iz prve $x = -y - z = 2y + 2z = 2 + 2 = 1$. Dobili smo da je sistem odredjen i važi da je $(x, y, z, t) = (1, 1, 1, 1)$.