

Formalne metode

u softverskom inženjerstvu

01 Uvod

ETFBL 24-25

Dunja Vrbaški

Pregled nekih stvari opšte inženjerske kulture

Formalizacije

Ponavljjanje

LOGIČKA ARGUMENTACIJA

Aristotel

Ili je ulaz pogrešan ili program ima grešku.
Ulaz nije pogrešan.

Program ima grešku.

Svi kvadrati su pravougaonici.
Svi pravougaonici imaju četiri stranice.

Svi kvadrati imaju četiri stranice.

Neke mačke nisu kućni ljubimci.
Sve mačke su sisari.

Neki sisari nisu kući ljubimci.

2 premise + zaključak

Ako prihvatimo premise kao tačne i zaključak logički sledi iz premisa.
Prihvatamo zaključak.

Premise: prost ili složen iskaz

Iskaz: izjava koja je ili tačna ili netačna

“Ova izjava je netačna.”

Iskazna logika - iskaz je osnovni pojam, ne definiše se

Ili je ulaz pogrešan ili program ima grešku.
Ulaz nije pogrešan.

Program ima grešku.

Svi kvadrati su pravougaonici.
Svi pravougaonici imaju četiri stranice.

Svi kvadrati imaju četiri stranice.

Neke mačke nisu kućni ljubimci.
Sve mačke su sisari.

Neki sisari nisu kući ljubimci.

ISKAZNI RAČUN

\top, \perp

$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$

1. iskazi, (p, q, r...)
2. vrednosti: tačno ili netačno
3. veznici:
 - a. negacija NE, nije
 - b. konjukcija I
 - c. disjunkcija Ili
 - d. implikacija AKO-ONDA
 - e. ekvivalencija AKO i SAMO AKO, akko
4. zagrade

“naša” logika
logika u filozofiji
matematička logika

logička kola

\neg	
T	\perp
\perp	T

\wedge	T	\perp
T	T	\perp
\perp	\perp	\perp

\vee	T	\perp
T	T	T
\perp	\perp	\perp

\Rightarrow	T	\perp
T	T	\perp
\perp	T	T

\Leftrightarrow	T	\perp
T	T	\perp
\perp	\perp	T

\neg	
T	\perp
\perp	T

Ako je p tačno onda je negacija tog iskaza netačna, suprotan iskaz je netačan. I obrnuto.

Danas pada kiša.
Danas ne pada kiša.

\wedge	T	\perp
T	T	\perp
\perp	\perp	\perp

\vee	T	\perp
T	T	T
\perp	T	\perp

Danas pada kiša. Danas je 01.01.2022.

Ako su p i q tačni iskazi onda je i iskaz "p i q" tačan.

Ako je bar jedan iskaz netačan onda je i iskaz "p i q" netačan.

Danas pada kiša i danas je 01.01.2022.

Danas, 01.01.2022., pada kiša.

Iskaz "p ili q" je tačan ako je bar jedan iskaz tačan.

Ako je bar jedan iskaz tačan onda je iskaz "p ili q" tačan.

Danas je ili 01.01.2022. ili pada kiša.

Ne mešati ILI sa isključivim ILI

"ili p ili q"

\Rightarrow	T	\perp
T	T	\perp
\perp	T	T

Implikacija

Ne može iz tačnog slediti netačno, ali iz netačnog može slediti tačno.

x je pas.

x laje.

Drugi iskaz nije posledica, nije zaključak iz prvog.

\Rightarrow	T	\perp
T	T	\perp
\perp	T	T

Ako položiš ispit kupiću ti čokoladu.

- položen - čokolada
- položen - bez čokolade
- nije položen - čokolada
- nije položen - bez čokolade

Ako boca sadrži kiselinu onda boca ima oznaku za opasnost.

- Ako boca ne sadrži kiselinu - možda boca ima nešto drugo opasno (p je 0, q je 1)
- Ako boca ne sadrži kiselinu - možda ima nešto bezopasno pa zato nema oznaku (p je 0, q je 0)
- Ako boca sadrži kiselinu, a boca nema oznaku (p je 1, q je 0) onda $p \Rightarrow q$ je 0

\Rightarrow	T	\perp
T	T	\perp
\perp	T	T

logika \rightarrow *filozofija*
formalna logika \rightarrow *matematika*

Paradoks?

Ako je trava crvena onda je sneg beo.

Da li uopšte ima smisla ako među iskazima nema veze?

Iskazni račun ne mešati sa rezonovanjem - pratiti pravila.

U formalnoj, matematičkoj logici, bavimo se samo istinosnim vrednostima i uvodimo operatore.

Ne zavisi od značenja - samo od istinitosti tvrdnji.

Matematičku logiku interesuje samo pod kojim uslovima istinost p povlači istinitost q.

Ne poklapa se uvek sa uslovnim rečenicama i rezonovanjem.
 Iz netačne pretpostavke može slediti bilo kakav iskaz.

U opštem slučaju, AKO-ONDA izjave u prirodnom jeziku \neq implikacija

\Leftrightarrow	T	\perp
T	T	\perp
\perp	\perp	T

Ekvivalencija

Ako su oba ista (tačna ili netačna) onda su ekvivalentni.

p akko q

Danas pada kiša ako i samo ako je danas 01.01.2023.
Boca sadrži kiselinu akko ima oznaku za opasnost.

\Rightarrow	T	\perp
T	T	\perp
\perp	T	T

\Leftrightarrow	T	\perp
T	T	\perp
\perp	\perp	T

Implikacija, još se čita i kao:

iz p sledi q
p samo ako q

p je dovoljno za q
q je potrebno za p

Ekvivalencija, još se čita i kao:

p je potrebno i dovoljno za q

P	Q	$\neg P$	$P \rightarrow Q$	$\neg P \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

P	Q	$\neg P$	$P \rightarrow Q$	$\neg P \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

$$P \Rightarrow Q \Leftrightarrow \neg P \vee Q$$

Šta nam omogućava ovaj zakon?

$$P \Rightarrow Q \Leftrightarrow \neg P \vee Q$$

Formula je **tautologija** ako je u svim evaluacijama tačna.

Formula je **kontradikcija** ako je u svim evaluacijama netačna.

Opšti logički zakoni.

$$p \Leftrightarrow p$$

$$p \vee \neg p$$

$$\neg\neg p \Leftrightarrow p$$

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$$

$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$$

$$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$$

$$p \wedge (p \Rightarrow q) \Leftrightarrow q$$

$$(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$$

$$(p \Rightarrow q) \Leftrightarrow \neg p \vee q$$

$$\neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q$$

Zaustavite se kod svake i razmislite da li poznajete ova pravila.

Da li ih prepoznajete kao zakone, da li su vam intuitivno jasni?

Da li ih i kad koristite u programiranju?

ZADATAK

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$$

Da li je tautologija?

- tablica
- diskusija redom po slovima p, q, r
- kontradikcija

TEOREMA

Ako su A i $A \Rightarrow B$ tautologije onda je i B tautologija.

Dokaz: Ako bi postojala valuacija formule B koja je netačna to bi impliciralo da je za tu valuaciju $A \Rightarrow B$ netačno što ne može biti jer je ta formula tautologija.

Pogledati tautologiju "modus ponens" i "modus ponens" kao formu argumentacije.

$\models A$

Oznaka da je A tautologija

Formula A je **semantička posledica** formula F_1, F_2, \dots, F_n ako u svakoj evaluaciji u kojoj su tačne F_1, F_2, \dots, F_n je i formula A je tačna.

$$F_1, F_2, \dots, F_n \models A$$

Niz pretpostavki iz kojih izvodimo zaključak vodeći računa o istinitosti tih hipoteza

Postoji i sintaksička posledica kad nas samo zanimaju pravila izvođenja.

ZADATAK

$$p \vee q, p \Rightarrow r \models q \vee r$$

Obe formule sa leve strane tačne - da li je i formula sa desne strane tačna?

TEOREMA

B je semantička posledica A akko je $A \Rightarrow B$ tautologija.

Dokaz:

Prvi smer, neka je B posledica od A.

Implikacija može biti netačna jedino ako je B netačno, a A tačno. Međutim ako je A tačno onda je B tačno jer je B posledica.

Drugi smer, neka je implikacija tautologija.

Ako pretpostavimo da B nije posledica znači da postoji neka evaluacija u kojoj je A tačno, a B netačno. Međutim, time implikacija ne bi bila tautologija.

TEOREMA

B je semantička posledica A_1, A_2, \dots, A_n akko je
 $A_n \Rightarrow B$ semantička posledica A_1, A_2, \dots, A_{n-1}

Opštije tvrđenje

Dokaz - pokušati

Dobijamo metod:

Ako treba da dokažemo $A \Rightarrow B$

A priključimo postojećim pretpostavkama i onda dokazujemo B.

TEOREMA

B je semantička posledica A_1, A_2, \dots, A_n akko je
B semantička posledica $A_1 \wedge A_2 \wedge \dots \wedge A_n$

$(A_1 \wedge A_2 \wedge \dots \wedge A_n) \rightarrow B$ tautologija

$A_1 \wedge A_2 \wedge \dots \wedge A_n \wedge \neg B$ kontradikcija

PRAVILA KOJA SE KORISTE U DOKAZIMA

Želimo da pokažemo tačnost tvrđenja $p \Rightarrow q$.

Kontrapozicija - pretpostavimo da je q je netačno.

$$\neg q \Rightarrow \neg p \models p \Rightarrow q$$

Želimo da pokažemo tačnost tvrđenja p .

Svođenje na kontradikciju - pretpostavimo da je p netačno i utvrdimo da u isto vreme važe neko " q " i " $\neg q$ "

$$\neg p \Rightarrow q \wedge \neg q \models p$$

gde su zagrade?

Želimo da pokažemo tačnost tvrđenja q .

Rastavljanje na slučajeve - utvrdimo da važi p_1 ILI p_2 i pokažemo implikaciju q iz svakog slučaja (pokrijemo sve slučajeve)

$$p_1 \vee p_2, p_1 \Rightarrow q, p_2 \Rightarrow q \models q$$

Želimo da pokažemo tačnost tvrđenja p akko q.

Rastavljanje na smerove.

$$p \Rightarrow q, q \Rightarrow p \models p \Leftrightarrow q$$

PREDIKATSKI RAČUN

Iskazna logika

Pravila zaključivanja + istinitost premisa

Nije dovoljno izražajno

Ljudi su smrtni.

Svaki čovek je smrtnan.

Postoji čovek koji je besmrtnan.

Postoji tačno jedan čovek koji je smrtnan.

Ne postoji čovek koji je besmrtnan.

...

POSTOJI i SVAKI

Istinitost iskaza zavisi od unutrašnje strukture.

$$(\exists x)P(x)$$

$$(\forall x)P(x)$$

$$(\forall x)(\exists y)(P(x, y))$$

$$(\forall x)(\exists y)(P(x, y, z) \implies Q(z))$$

$$(\forall x)(\exists y)(P(x, y, z) \implies (\forall x)Q(x, z))$$

Znatno veća izražajnost

Teže dokazivanje i odlučivanje

Imamo konstante, ali i promenljive.

1. Svaki čovek je smrtan.
2. Sokrat je čovek.
-
3. Sokrat je smrtan

$((\forall x)(\text{Covek}(x) \rightarrow \text{Smrtan}(x)) \wedge \text{Covek}(\text{Sokrat})) \rightarrow \text{Smrtan}(\text{Sokrat}).$

Valjane predikatske formule su one koji su tačne u svakoj interpretaciji

$$\neg(\forall x)A \leftrightarrow (\exists x)\neg A$$

$$\neg(\exists x)A \leftrightarrow (\forall x)\neg A$$

$$(\exists x)(A \vee B) \leftrightarrow (\exists x)A \vee (\exists x)B$$

$$(\forall x)(A \wedge B) \leftrightarrow (\forall x)A \wedge (\forall x)B$$

$$(\forall x)(\forall y)A \leftrightarrow (\forall y)(\forall x)A$$

$$(\exists x)(\exists y)A \leftrightarrow (\exists y)(\exists x)A$$

Valjane predikatske formule su one koji su tačne u svakoj interpretaciji

$$\neg(\forall x)A \leftrightarrow (\exists x)\neg A$$

$$\neg(\exists x)A \leftrightarrow (\forall x)\neg A$$

$$(\exists x)(A \vee B) \leftrightarrow (\exists x)A \vee (\exists x)B$$

$$(\forall x)(A \wedge B) \leftrightarrow (\forall x)A \wedge (\forall x)B$$

$$(\forall x)(\forall y)A \leftrightarrow (\forall y)(\forall x)A$$

$$(\exists x)(\exists y)A \leftrightarrow (\exists y)(\exists x)A$$

Šta znači interpretacija?

$$(\forall y)(\exists x)(x < y)$$

Kada je ovo tačno?

Pojmovi: domen interpretacije i valuacija.

- sintaksno značenje
- semantičko značenje

Valjane formule u predikatskoj logici - neodlučiv problem
Tautologije u iskaznoj logici - odlučiv problem

Šta znači “odlučiv”?

Koja formula je valjana?

$$(\exists y)(\forall x)P(x, y) \rightarrow (\forall x)(\exists y)P(x, y)$$

$$(\forall x)(\exists y)P(x, y) \rightarrow (\exists y)(\forall x)P(x, y)$$

Kako programiramo?
Kako pokazujemo da ne važi?

$$(\forall x)(\forall y)P(x, y)$$

$$(\forall x)(\exists y)P(x, y)$$

$$(\exists x)(\forall y)P(x, y)$$

$$(\exists x)(\exists y)P(x, y)$$

PRIMENA

- formalno dokazivanje
- softver - tačan ili elegantniji algoritam
- rešenja zasnovana na odlučivanju ili zaključivanju
- hardver - operacije
- formiranje formalnih teorija

PAR NAPOMENA

```
if (x < 5)
    ...
else
    ...
```

```
if !(x >= 5)
    ...
else
    ...
```

Česta greška: neispravna negacija
(dok smišljamo algoritam)

Suprotno od manje je veće ili jednako, ne veće.
Važan je domen.

```
if (uslov == true)
if (uslov)

if (uslov == false)
if (!uslov)
```

```
if !(x % 3 == 0 && x % 5 == 0)
if !(x % 3 == 0) || !(x % 5 == 0)
if x % 3 != 0 || x % 5 != 0
```

```
if !(x % 3 == 0 || x % 5 == 0)
if !(x % 3 == 0) && !(x % 5 == 0)
if x % 3 != 0 && x % 5 != 0
```

lazy, short-circuit evaluation?



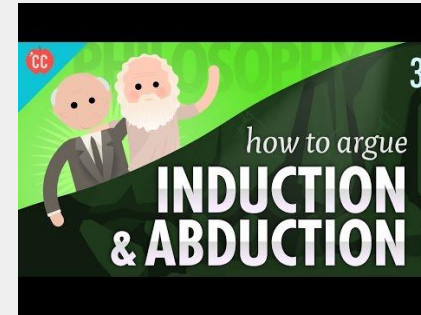
https://en.wikipedia.org/wiki/List_of_fallacies



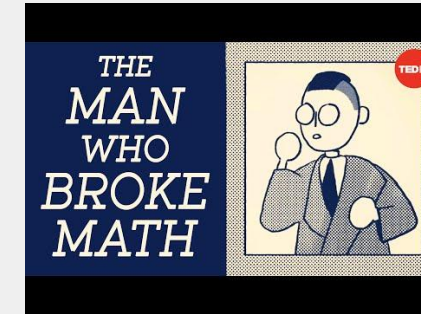
<https://youtu.be/NKEhdsnKKHs>



<https://youtu.be/kJzSzGbfc0k>



<https://youtu.be/-wrCpLJ1XAW>



<https://youtu.be/l4pQbo5MQOs>