Diskretne strukture

Gašper Fijavž

Fakulteta za računalništvo in informatiko
Univerza v Ljubljani

3. oktober 2024

Indukcija, zgled

$$
\begin{array}{rcl}
1 & = & 1 \\
1+3 & = & 4 \\
1+3+5 & = & 9 \\
1+3+5+7 & = & 16 \\
1+3+5+7+9 & = & 25 \\
1+3+5+7+9+11 & = & 36
\end{array}
$$

$$1+3+5+\cdots+(2k-1) \stackrel{?}{=} k^2$$

Zdi se: vsota *prvih nekaj* lihih naravnih števil je *popoln kvadrat*. Natančneje: vsota prvih k lihih naravnih števil je enaka k^2.

Kako to pokazati?

Indukcija, mehanizem

Domnevo preoblikujemo v obliko:

Za vsako naravno število k velja, da je vsota najmanjših k lihih naravnih števil enaka izrazu k^2.

in dokazujemo

Baza indukcije: Trditev velja za najmanjše naravno število.

Vsota enega (najmanjšega) lihega števila je enaka 1^2.Vsota nič (najmanjših) lihih števil je enaka 0^2.

Indukcijski korak: Če trditev velja pri nekem naravnem številu n, potem velja tudi pri njegovem nasledniku $n+1$.

Če je vsota prvih n lihih naravnih števil enaka n^2, potem je vsota prvih $n+1$ lihih naravnih števil enaka $(n+1)^2$.

Fibonaccijeva števila

Zaporedje Fibonaccijevih števil $(f_n)_{n\in\mathbb{N}}$,

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots,$$

je definirano z začetnima členoma, $f_0 = 0$, $f_1 = 1$, in rekurzivno zvezo

$$f_n = f_{n-1} + f_{n-2}, \text{ ki velja za } n \geq 2.$$

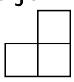
Naloga: Pokaži, da je Fibonaccijevo število f_{3n} vedno sodo.

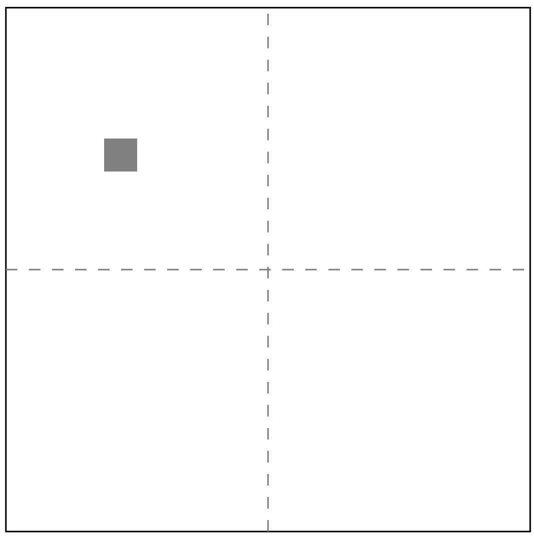
Vsota kubov

Naloga: Pokaži, da za vsoto prvih nekaj kubov naravnih števil velja zveza

$$0^3 + 1^3 + 2^3 + \cdots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$$

Prebodena šahovnica

Iz šahovnice velikosti $2^n \times 2^n$ izrežemo eno kvadratno polje. Pokaži, da lahko takó pokvarjeno igralno ploščo tlakujemo s *triominami* oblike .



Napačna indukcija - baza

Naloga: Pokaži, da je vsota poljubnih k sodih naravnih števil liho število.

Napačna indukcija - indukcijski korak

Naloga: Vsaka končna družina paroma nevzporednih premic v ravnini

$$q_1, q_2, q_3, \ldots, q_k$$

ima skupno točko P — točko, skozi katero gredo vse omenjene premice.

Uporabimo znani (pravilni) dejstvi:

- Če nevzporedni premici q in q' ležita v isti ravnini, potem imata natanko eno skupno točko P.
- Če sta P in P' različni točki v ravnini, potem obstaja natanko ena premica, ki vsebuje P in P'.

Izjave

Izjava je stavek, ki je bodisi resničen bodisi neresničen.

Vsak stavek ni izjava:

- *Zapri vrata!*
- *Ta stavek ni resničen.*

Kaj pa:

- *Zunaj sveti Luna.*

Izjave

Izjave delimo po *vsebini* na

- *resnične* (imajo vrednost 1) in
- *neresnične* (imajo vrednost 0)

ter *obliki* na

- *osnovne* (tudi *enostavne*) in
- *sestavljene*.

Izjave

Zgleda osnovnih izjav:

- *Zunaj sije Sonce.*
- *Peter sedi na vrtu.*

Zgledi sestavljenih izjav:

- *Če zunaj sije Sonce, Peter sedi na vrtu.*
- *Peter sedi na vrtu in zunaj sije Sonce.*
- *Ni res, da zunaj sije Sonce.*

Izjavni vezniki

Izjave sestavljamo s pomočjo *izjavnih veznikov* (tudi *izjavnih povezav, logičnih veznikov*).

Izjavni vezniki so:

- *enomestni* (npr. *ne*)
- *dvomestni* (npr. *in, ali, če... potem..., niti... niti...*)
- *tromestni,...*

Izjavni vezniki

Resničnost sestavljene izjave je odvisna samo od resničnosti sestavnih delov. Zato izjavne veznike definiramo s pomočjo *resničnostnih tabel*.

- negacija $\neg$
- konjunkcija $\wedge$
- disjunkcija $\vee$
- ekskluzivna disjunkcija $\veebar$
- implikacija $\Rightarrow$
- ekvivalenca $\Leftrightarrow$

Negacija

Negacija izjave A, $\neg A$, beremo "*Ne A*".

$\neg A$ je resnična natanko tedaj, ko je A neresnična.
Definirana je z naslednjo pravilnostno tabelo:

A	$\neg A$
0	1
1	0

Negacija je *enomestni* izjavni veznik.

Konjunkcija

Konjunkcija izjav A in B, označimo jo z $A \wedge B$, in beremo "*A in B*".

$A \wedge B$ je resnična n.t., ko sta obe izjavi A in B resnični.

Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

Disjunkcija

Disjunkcija izjav A in B, označimo jo z $A \vee B$, in beremo "*A ali B*".

$A \vee B$ je resnična n.t., ko je vsaj ena od izjav A ali B resnična.

Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Ekskluzivna disjunkcija

Ekskluzivna disjunkcija izjavnih izrazov A in B, označimo jo z $A \veebar B$, in beremo "*A ekskluzivni ali B*".

$A \veebar B$ je resnična n.t., ko je natanko eden od izjavnih izrazov A in B resničen.

Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \veebar B$
0	0	0
0	1	1
1	0	1
1	1	0

Implikacija

Implikacija izjav A in B, označimo jo z $A \Rightarrow B$, in beremo
"*Iz A sledi B*" "*Če A potem B*" "*A implicira B*"

Izjavi A pravimo *antecedens* implikacije, izjavi B pa *konsekvens* implikacije $A \Rightarrow B$.
$A \Rightarrow B$ je neresnična samo v primeru, ko je izjava A resnična in izjava B neresnična.
Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Ekvivalenca

Ekvivalenca izjav A in B, označimo jo z $A \Leftrightarrow B$, in beremo
"*A ekvivalentno B*"
"*A natanko tedaj, ko B*"
"*A , če in samo če B*".
$A \Leftrightarrow B$ je resnična n.t., ko imata obe izjavi A in B isto logično vrednost.
Definirana je z naslednjo pravilnostno tabelo:

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Izjavni vezniki

- negacija $\neg$
- konjunkcija $\wedge$
- disjunkcija $\vee$
- ekskluzivna disjunkcija $\veebar$
- implikacija $\Rightarrow$
- ekvivalenca $\Leftrightarrow$

Dogovor o opuščanju oklepajev

Če ni z oklepaji drugače naznačeno, potem:

1. Negacija veže močneje kot konjunkcija, konjunkcija veže močneje kot disjunkcija, disjunkcija (katerakoli) veže močneje kot implikacija in implikacija veže močneje kot ekvivalenca.
2. Istovrstni (dvomestni) vezniki vežejo od *leve proti desni*.
3. Disjunkcije ravno tako združujemo od *leve proti desni*.

Izjavni izrazi

1. *Izjavni konstanti* 0 in 1, ki jima pravimo tudi *laž* in *resnica*, sta izjavna izraza.
2. *Izjavne spremenljivke* $p, q, r, \ldots$ so izjavni izrazi.
3. Če je A izjavni izraz, potem je tudi $(\neg A)$ izjavni izraz.
4. Če sta A in B izjavna izraza, potem so tudi

$$(A \wedge B)\ , \quad (A \vee B)\ , \quad (A \veebar B)\ , \quad (A \Rightarrow B) \quad \text{in} \qquad (A \Leftrightarrow B)$$

   izjavni izrazi.

Konstrukcijsko drevo in resničnostna tabela

Konstrukcijsko drevo opiše, kako izjavni izraz zgradimo iz bolj enostavnih izjavnih izrazov.

Resničnostna tabela izjavnega izraza za vsak *nabor* logičnih vrednosti izjavnih spremenljivk pove logično vrednost izjavnega izraza.

Tavtologija in protislovje

Tavtologija je izjavni izraz, ki je "vedno" resničen.

Protislovje je izjavni izraz, ki je "vedno" neresničen.

Izjavni izraz, ki ni niti tavtologija niti protislovje, imenujemo *nevtralni izjavni izraz*.

Enakovredni izjavni izrazi

Izjavna izraza A in B sta *enakovredna*, če imata pri vseh naborih vrednosti izjavnih spremenljivk enako vrednost.

V tem primeru pišemo $A \sim B$.

Enakovredni izjavni izrazi

Izrek

Izjavna izraza A in B sta enakovredna natanko tedaj, ko je izraz $A \Leftrightarrow B$ tavtologija.

Izrek

Za enakovrednost izjavnih izrazov veljajo naslednje zveze:

1. $A \sim A$
2. *Če* $A \sim B$, *potem* $B \sim A$.
3. *Če* $A \sim B$ *in* $B \sim C$, *potem* $A \sim C$.

Zakoni izjavnega računa

Nekateri pari enakovrednih izjavnih izrazov imajo posebna imena. To so *zakoni izjavnega računa*.

1. Zakon dvojne negacije: $\neg\neg A \sim A$
2. Idempotenca: $A \wedge A \sim A \qquad A \vee A \sim A$
3. Komutativnost: $A \wedge B \sim B \wedge A \qquad A \vee B \sim B \vee A$
   $A \Leftrightarrow B \sim B \Leftrightarrow A$
4. Asociativnost: $(A \wedge B) \wedge C \sim A \wedge (B \wedge C)$
   $(A \vee B) \vee C \sim A \vee (B \vee C)$
   $(A \Leftrightarrow B) \Leftrightarrow C \sim A \Leftrightarrow (B \Leftrightarrow C)$
5. Absorpcija: $A \wedge (A \vee B) \sim A \qquad A \vee (A \wedge B) \sim A$
6. Distributivnost: $(A \vee B) \wedge C \sim (A \wedge C) \vee (B \wedge C)$
   $(A \wedge B) \vee C \sim (A \vee C) \wedge (B \vee C)$
7. de Morganova zakona: $\neg(A \vee B) \sim \neg A \wedge \neg B$
   $\neg(A \wedge B) \sim \neg A \vee \neg B$

8. Kontrapozicija: $A \Rightarrow B \sim \neg B \Rightarrow \neg A$
9. Lastnosti 0 in 1: $A \Rightarrow A \sim 1 \qquad A \Leftrightarrow A \sim 1$
   $A \vee \neg A \sim 1 \qquad A \wedge \neg A \sim 0$
10. Še lastnosti 0 in 1: $A \wedge 0 \sim 0 \qquad A \vee 0 \sim A$
    $A \wedge 1 \sim A \qquad A \vee 1 \sim 1$
    $A \Rightarrow 0 \sim \neg A \qquad 0 \Rightarrow A \sim 1$
    $A \Rightarrow 1 \sim 1 \qquad 1 \Rightarrow A \sim A$
11. Lastnosti implikacije: $A \Rightarrow B \sim \neg A \vee B$
    $\neg(A \Rightarrow B) \sim A \wedge \neg B$
12. Lastnosti ekvivalence: $A \Leftrightarrow B \sim (A \Rightarrow B) \wedge (B \Rightarrow A)$
    $A \Leftrightarrow B \sim (A \wedge B) \vee (\neg A \wedge \neg B)$
    $\neg(A \Leftrightarrow B) \sim \neg A \Leftrightarrow B$

Enakovrednost izjavnih izrazov

Kako pokazati, da sta izjavna izraza A in B enakovredna?

Kako pokazati, da izjavna izraza A in B nista enakovredna?

Naloga

Poišči izjavni izraz s predpisano resničnostno tabelo:

p	q	r	A
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Disjunktivna normalna oblika

Disjunktivna normalna oblika (DNO) izjavnega izraza A je izjavni izraz A_{DNO}, za katerega velja:

- $A \sim A_{DNO}$
- A_{DNO} je disjunkcija osnovnih konjunkcij.

Osnovna konjunkcija je konjunkcija izjavnih spremenljivk in/ali njihovih negacij.
A_{DNO} *lahko* zgradimo tako, da za vsak nabor pravilnostne tabele, pri katerem je izraz A resničen, pripravimo eno osnovno konjunkcijo. V njej nastopajo v tem naboru resnične spremenljivke in negacije v tem naboru lažnih spremenljivk.

Konjunktivna normalna oblika

Konjunktivna normalna oblika (KNO) izjavnega izraza A je izjavni izraz A_{KNO}, za katerega velja:

- $A \sim A_{KNO}$
- A_{KNO} je konjunkcija osnovnih disjunkcij.

Osnovna disjunkcija je disjunkcija izjavnih spremenljivk in/ali njihovih negacij.
A_{KNO} *lahko* zgradimo tako, da za vsak nabor pravilnostne tabele, pri katerem je izraz A neresničen, pripravimo eno osnovno disjunkcijo. V njej nastopajo v tem naboru lažne spremenljivke in negacije v tem naboru resničnih spremenljivk.

Kdaj KNO in DNO

Trditev

Vsak izjavni izraz ima DNO in
Vsak izjavni izraz ima KNO.

Posledica

Za vsak izjavni izraz A obstaja enakovreden izjavni izraz B, ki vsebuje samo veznike $\neg$, $\wedge$, $\vee$.

Polni nabori izjavnih veznikov

Družina izjavnih veznikov $\mathcal{N}$ je *poln nabor izjavnih veznikov*, če za vsak izjavni izraz A obstaja enakovreden izjavni izraz B, ki vsebuje samo veznike iz $\mathcal{N}$.

$\{\neg, \wedge, \vee\}$ je poln nabor izjavnih veznikov.

Polni nabori izjavnih veznikov

Nekaj drugih polnih naborov izjavnih veznikov:

$$\{\neg, \vee\}\ , \quad \{\neg, \wedge\}, \quad \{\neg, \Rightarrow\}\ , \quad \{0, \Rightarrow\}$$

Polni nabori izjavnih veznikov

Vprašanje:
Kako v praksi pokazati, da je nabor izjavnih veznikov $\mathcal{N}$ poln?

1. Izberemo znan poln nabor izjavnih veznikov $\mathcal{Z}$.
2. Vsak veznik iz znanega nabora $\mathcal{Z}$ izrazimo samo z uporabo veznikov iz $\mathcal{N}$.

Sklepanje v izjavnem računu

Predpostavki:	1.	*Če dežuje, je oblačno.*
	2.	*Dežuje.*
Zaključek:	3.	*Oblačno je.*

Ali je sklep pravilen?

Še en zgled

Predpostavke:	1.	*Ta žival ima krila ali pa ni ptič.*
	2.	*Če je ta žival ptič, potem leže jajca.*
	3.	*Ta žival nima kril.*
Zaključek:	4.	*Torej ta žival ne leže jajc.*

Ali je ta sklep pravilen?

Tretji zgled

Predpostavke:	1.	*Io je Jupitrov satelit.*
	2.	*Titan je Saturnov satelit.*
Zaključek:	3.	*Zemlja je tretji planet od Sonca.*

Ali je ta sklep pravilen?

Formalizacija

dežuje	...	d
oblačno je	...	o

1.	$d \Rightarrow o$
2.	d
3.	o

Formalizacija, znova

ta žival ima krila	...	k
ta žival je ptič	...	p
ta žival leže jajca	...	j

1.	$k \vee \neg p$
2.	$p \Rightarrow j$
3.	$\neg k$
4.	$\neg j$

Pravilen sklep

Zaporedje izjavnih izrazov $A_1, A_2, \ldots, A_n, B$ je *pravilen sklep* s *predpostavkami* $A_1, A_2, \ldots, A_n$ in *zaključkom* B, če je zaključek B resničen pri vseh tistih naborih vrednosti izjavnih spremenljivk, pri katerih so resnične vse predpostavke.

Pišemo: $A_1, A_2, \ldots, A_n \models B$

in beremo:
Iz predpostavk $A_1, A_2, \ldots, A_n$ logično sledi zaključek B.

Četrti zgled

Predpostavke:	1.	*Šel bom na tekmo, zvečer pa bom naredil domačo nalogo.*
	2.	*Če grem na tekmo in nato še v kino, zvečer ne bom mogel narediti domače naloge.*
Zaključek:	3.	*Ne morem iti v kino.*

Ta sklep je pravilen. Zakaj?

Formalizacija

grem na tekmo	...	t
grem v kino	...	k
naredim domačo nalogo	...	d

1.	$t \wedge d$
2.	$t \wedge k \Rightarrow \neg d$
3.	$\neg k$

Nepravilen sklep

Kako pokažemo, da sklep ni pravilen?
Poiščemo *protiprimer*, tj. nabor vrednosti izjavnih spremenljivk, pri katerem so vse predpostavke resnične, zaključek pa ne.

Nepravilen sklep

ta žival ima krila	...	k
ta žival je ptič	...	p
ta žival leže jajca	...	j

1. $k \vee \neg p$
2. $p \Rightarrow j$
3. $\neg k$
4. $\neg j$

Vstavimo $k \sim 0$, $p \sim 0$ in $j \sim 1$ ter pridelamo:

$$\begin{array}{rcll} k \vee \neg p & \sim & 1 & \\ p \Rightarrow j & \sim & 1 & \\ \neg k & \sim & 1 & \text{in} \\ \neg j & \sim & 0 & \end{array}$$

Protiprimer je žival, ki

- nima kril,
- ni ptič in
- leže jajca.

Pravilen sklep

Izrek

$A_1, A_2, \ldots, A_n \models B$ natanko tedaj, ko je izjavni izraz $(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \Rightarrow B$ tavtologija.

Pravilen sklep

Izrek

- *Če je $B \sim C$, potem $A \models B$ natanko tedaj, ko $A \models C$.*
- *Če z 1 označimo tavtologijo, potem $A \models 1$.*
- *Velja $A_1, A_2, \ldots, A_n \models A_k$ (za $k \in \{1, \ldots, n\}$)*
- *Če z 1 označimo tavtologijo, potem $A_1, A_2, \ldots, A_n \models B$ natanko tedaj, ko $A_1, A_2, \ldots, A_n, 1 \models B$*

Pravila sklepanja

$A, A \Rightarrow B \models B$	*modus ponens* (MP)
$A \Rightarrow B, \neg B \models \neg A$	*modus tollens* (MT)
$A \vee B, \neg B \models A$	*disjunktivni silogizem* (DS)
$A \Rightarrow B, B \Rightarrow C \models A \Rightarrow C$	*hipotetični silogizem* (HS)
$A, B \models A \wedge B$	*združitev* (Zd)
$A \wedge B \models A$	*poenostavitev* (Po)
$A \models A \vee B$	*pridružitev* (Pr)

Pravilom sklepanja pravimo tudi *osnovni pravilni sklepi*.

Dokaz pravilnosti sklepa

Pravilnost sklepa $A_1, A_2, \ldots, A_n \models B$ pokažemo tako, da sestavimo zaporedje izjavnih izrazov $C_1, C_2, \ldots, C_m$, kjer je $C_m = B$ in za $i = 1, 2, \ldots, m$ velja:

(a) C_i je ena od predpostavk ali
(b) C_i je tavtologija ali
(c) C_i je enakovreden enemu od predhodnih izrazov v zaporedju ali
(d) C_i logično sledi iz predhodnih izrazov po enem od osnovnih pravilnih sklepov.

Zgled

Ali iz predpostavk $p \Rightarrow q, p \vee r, q \Rightarrow s, r \Rightarrow t, \neg s$ sledi t?

1.	$p \Rightarrow q$	predpostavka
2.	$p \vee r$	predpostavka
3.	$q \Rightarrow s$	predpostavka
4.	$r \Rightarrow t$	predpostavka
5.	$\neg s$	predpostavka
6.	$p \Rightarrow s$	HS(1,3)
7.	$\neg p$	MT(6,5)
8.	r	DS(2,7)
9.	t	MP(4,8)

Zgled, še en

Ali iz predpostavk

1. *Če sije sonce, nosim sončna očala.*
2. *Nosim kapo ali sončna očala.*
3. *Sončnih očal ne nosim.*

sledi zaključek

Nosim kapo in sonce ne sije.

$A, A \Rightarrow B \models B$	*modus ponens* (MP)
$A \Rightarrow B, \neg B \models \neg A$	*modus tollens* (MT)
$A \vee B, \neg B \models A$	*disjunktivni silogizem* (DS)
$A \Rightarrow B, B \Rightarrow C \models A \Rightarrow C$	*hipotetični silogizem* (HS)
$A, B \models A \wedge B$	*združitev* (Zd)
$A \wedge B \models A$	*poenostavitev* (Po)
$A \models A \vee B$	*pridružitev* (Pr)

Pogojni sklep

Pogojni sklep (PS) uporabljamo, kadar ima zaključek sklepa obliko implikacije.

Izrek

$A_1, A_2, \ldots, A_k \models B \Rightarrow C$ natanko tedaj, ko
$A_1, A_2, \ldots, A_k, B \models C$.

Zgled

Pokaži, da iz predpostavk $p \Rightarrow q \vee r$ in $\neg r$ logično sledi zaključek $p \Rightarrow q$.

Sklep s protislovjem

Sklep s protislovjem (RA) lahko uporabljamo kadarkoli.

Izrek

$A_1, A_2, \dots, A_k \models B$ *natanko tedaj, ko*
$A_1, A_2, \dots, A_k, \neg B \models 0.$

Zgled

Pokaži, da iz $p \Rightarrow \neg(q \Rightarrow r)$, $s \wedge q \Rightarrow r$ in s sledi $\neg p$.

Analiza primerov

Analizo primerov (AP) lahko uporabljamo, kadar ima ena od predpostavk obliko disjunkcije.

Izrek

$A_1, A_2, \ldots, A_k, B_1 \vee B_2 \models C$ *natanko tedaj, ko*

$A_1, A_2, \ldots, A_k, B_1 \models C$ *in*

$A_1, A_2, \ldots, A_k, B_2 \models C$.