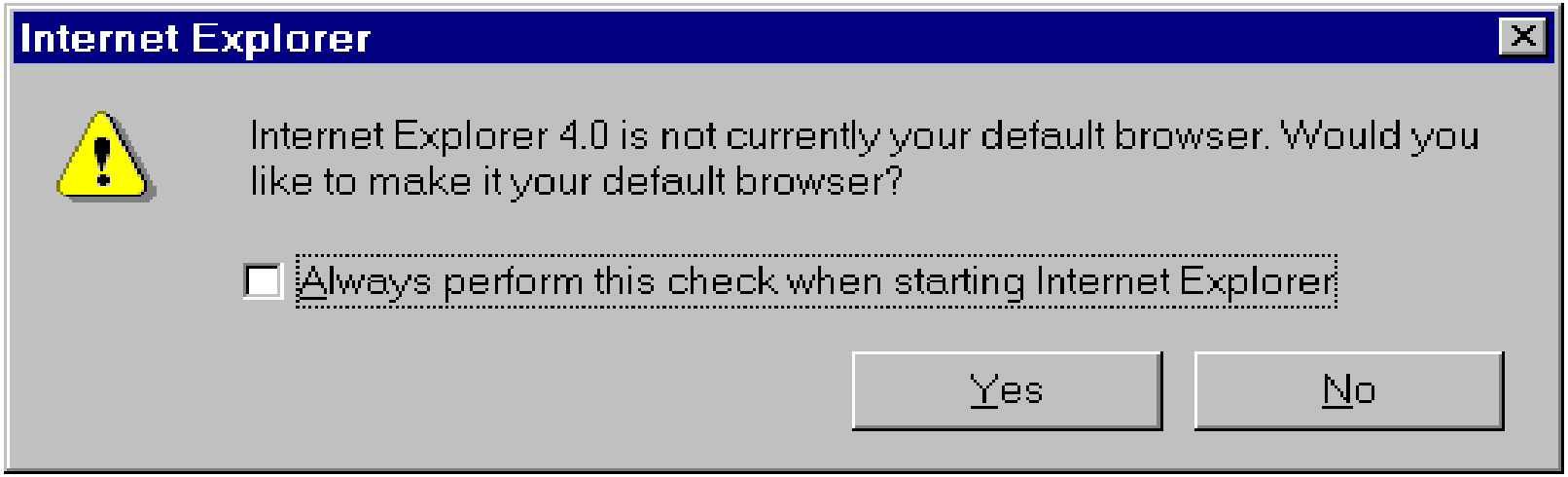
Punktiülesanne 2



Võrrelda pildi sisu ja valikute toimimist üldisuse kvantori definitsiooniga

Kahest valikust ühe sisu on üldisuse kvantoriga lause.

Kui t tähistab ajamomenti, siis positiivse valiku korral toimib:
$\forall t(KäivitatakseIE(t) \rightarrow Küsida(t))$.

Aga negatiivse valiku korral ei toimi selle lause eitus, vaid:
$\forall t(KäivitatakseIE(t) \rightarrow \neg Küsida(t))$.

Loeng 4

Predikaatloogika põhiseadused (järg)

Kvantorite ja lausearvutuse tehetega soetud tõestamistaktikad

Predikaatloogika põhiseadused

1. $\neg\forall x A(x) \equiv \exists x \neg A(x)$,
   $\neg\exists x A(x) \equiv \forall x \neg A(x)$.

2. $\forall x\big(A(x)\&B(x)\big) \equiv \forall x A(x)\ \&\forall x B(x)$,
   $\exists x\big(A(x)\vee B(x)\big) \equiv \exists x A(x)\vee \exists x B(x)$.

3. $\forall x\big(A\oplus B(x)\big) \equiv A\oplus \forall x B(x)$,
   $\exists x\big(A\oplus B(x)\big) \equiv A\oplus \exists x B(x)$ (kus $\oplus$ on $\&, \vee$ või $\supset$ (aga mitte $\sim$))

4. $\forall x(A(x) \supset B) \equiv \exists x A(x) \supset B$,
   $\exists x(A(x) \supset B) \equiv \forall x A(x) \supset B$.

5. $\forall x A(x) \equiv \forall y A(y)$,
   $\exists x A(x) \equiv \exists y A(y)$ (kus $A(x)$ ei sisalda muutujat y)

6. $\forall x \forall y A(x,y) \equiv \forall y \forall x A(x,y)$,
   $\exists x \exists y A(x,y) \equiv \exists y \exists x A(x,y)$.

7. $\exists x \forall y A(x,y) \supset \forall y \exists x A(x,y)$ on samaselt tõene

8. $\forall x A(x) \vee \forall x B(x) \supset \forall x\big(A(x)\vee B(x)\big)$,
   $\exists x\big(A(x)\&B(x)\big) \supset \exists x A(x) \& \exists x B(x)$ on samaselt tõesed.

9. $\forall x A(x) \supset A(t)$, $A(t) \supset \exists x A(x)$, $\forall x A(x) \supset \exists x A(x)$
   on samaselt tõesed (kus t ei sisalda valemis A seotud muutujaid)

Tehete avaldamine predikaatloogika valemites

Teor. 1. Järgmised kvantorist ja tehetest koosnevad hulgad on piisavad, et leida iga predikaatloogika valemi jaoks loogiliselt samaväärne valem:
$\{\forall, \neg, \&\}$, $\{\forall, \neg, \vee\}$, $\{\forall, \neg, \supset\}$,
$\{\exists, \neg, \&\}$, $\{\exists, \neg, \vee\}$, $\{\exists, \neg, \supset\}$.

Tõestus: leiduvad lausearvutuse ja predikaatarvutuse samaväärsused ülejäänud tehete/kvantorite elimineerimiseks.

Teoreemi kasutatakse juhtude arvu vähendamiseks induktiivsetes jm tõestustes.

Prefikskuju

Def. Predikaatarvutuse valem A on prefikskujul, kui
$A = Q_1 x_1 \ldots Q_n x_n B(x_1, \ldots x_n, y_1, \ldots y_m)$,
kus $Q_1, \ldots, Q_n$ on kvantorid ja valem B ei sisalda kvantoreid.

Teor. 2. Iga predikaatarvutuse valemi jaoks leidub temaga loogiliselt samaväärne prefikskujul valem.

Tõestus. On olemas samaväärsused kvantorite välja toomiseks eituse ja binaarsete lausearvutuse tehete alt (vajadusel võib binaarse tehte ühes argumendis muutujaid ümber nimetada).

Näide: $\forall x A(x) \sim \exists x B(x)$

Rakendus: automaattõestamise süsteemides viiakse valemid prefikskujule ja siis asendatakse kvantorid nn Skolemi funktsioonidega

Veel mõned tõestused

§ 5. Loogikal baseeruvad tõestustaktikad

Räägime nüüd tõestuse otsimisest.

Täpsemini – sellest, milliseid tõestamise taktikaid pakub loogika: **kuidas eelduse või väite peatehe ütleb meile ette võimaliku järgmise sammu teoreemi tõestuses.**

Peale siin vaadeldavate on olemas ka teisi üldisi tõestamise võtteid (näiteks **lemma sissetoomine** ja **induktsioon**), aga ka tõestamise taktikaid, mida pakuvad **konkreetsed teadaolevad teoreemid** (näiteks kolmnurkade kongruentsuse tunnused).

Teoreemi üldkuju

Tavaliselt on matemaatikas teoreemid sellisel kujul:

Kui on täidetud eeldused $A_1, \dots, A_n$, **siis** kehtib väide B.

Mõnikord nad pole küll seose „kui … , siis …“ abil sõnastatud, aga neid saab sellisele kujule ümber sõnastada.

Kasutades järeldumise märki, võib tüüpilise teoreemi üles kirjutada nii:

$$A_1, \dots, A_n \vdash B \quad (1)$$

Meenutame, et valemitest $A_1, \dots, A_n$ järeldub valem B parajasti siis, kui valem $A_1 \& \dots \& A_n \supset B$ on samaselt tõene.
St komad mängivad siin konjunktsiooni rolli ja järeldumise märgile vastab implikatsioon.

Avaldisi kujul (1) nimetatakse loogikas ka sekventsideks.

Mis on tõestus

- Tõestus on tekst, kus sammude kaupa liikudes jõutakse arusaamiseni, et teoreem kehtib.
- Kui tekst esitatakse eeldustest alates järeldumise järjekorras, siis igal sammul esitatakse
  1) järjekordne väide,
  2) millistest eelmistest väidetest ta järeldub,
  3) millise tuletusreegli, teoreemi, samasuse vms põhjal ta neist järeldub.
- Kui sammul esitatav väide on aksioom või varem teadaolev teoreem, siis osad 2) ja 3) seisnevad ainult päritolule viitamises

$$A_1, \dots, A_n \vdash B \quad (1)$$

- Tavaliselt me mõtleme tõestustest nii, et seal tehakse samm-sammult järeldusi eeldustest ja juba tõestatud väidetest, kuni on näidatud, et väide kehtib.
- Eelduste rollis saab kasutada ka valdkonna aksioome ja varem tõestatud teoreeme
- Tegelikult me aga teisendame mõnel sammul ka väidet ja asendame mingi kujul (1) oleva sekventsi tõestamise mingi(te) teis(t)e sekventsi(de)te tõestamisega.
- Tõestuse käigus võidakse lisaks algsetele eeldustele $A_1,\dots,A_n$ kasutusele võtta teisi teadaolevaid fakte, mille kehtimist me tohime järgmistel sammudel kasutada.

- Taktikate leidmiseks vaatame läbi **loogilised seosed**: kvantorid, konjunktsioon, disjunktsioon, implikatsioon, ekvivalents, eitus.
- Iga loogilise seose jaoks uurime, kuidas saab
  1) tõestada **väidet, milles see seos on peatehteks**,
  2) kasutada **eeldust, milles see seos on peatehteks.**
- **Loogiliste seostega seotud taktikad** võimaldavad saada tõestust otsides suure osa samme rutiinselt (automaatselt). Lühemates tõestustes on tavaliselt 0-2 mitterutiinset sammu, kus tuleb midagi muud peale loogikaseostest tulenevate teisenduste välja mõelda/meelde jätta).

Liikumissuund - osavalemitele

Meie poolt siin vaadeldavad tõestustaktikad lihtsustavad valemeid. Nad asendavad vaadeldava valemi tema osavalemi(te)ga, jättes ära välimise tehte/kvantori.

See tähendab, et pärast lõplikku arvu samme on meil lootus jõuda atomaarsete valemiteni, mille korral on selge, kas miski millestki järeldub.

Reaalselt õpikutes, artiklites jm esinevates tõestustes tehakse tihti korraga paar ühetehtelist sammu.

Väide kujul $\forall x B(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_n \vdash \forall x B(x)$$

Tavaline üldisuse kvantoriga väite tõestamise esimene samm on selline:

Tähistagu a suvalist interpretatsiooni kandja elementi.
Piisab, kui tõestame $A_1, \dots, A_n \vdash B(a)$

- Siinjuures tähendab a suvalisus seda, et eeldustes $A_1, \dots, A_n$ ei ole a kohta midagi väidetud.
- Fikseeritud interpretatsiooniga tegeledes me ei kasuta sõnu „interpretatsiooni kandja element“, vaid ütleme „Olgu a suvaline naturaalarv/reaalarv/tasandi punkt /...“

Eeldus kujul $\forall x A(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$A_1, \dots, A_{n-1}, \forall x A(x) \vdash B$ (1)

Kui tõestuses on vaatluse all mingi term t, siis

üldisuse kvantoriga eeldusest saab järeldada , et
väide A kehtib ka t kohta st (1) tõestamiseks võime tõestada

$$A_1, \dots, A_{n-1}, A(t) \vdash B$$

Märkus. Üldisuse kvantoriga eelduse võib ka alles jätta (kui teda edaspidi veel vaja on).

Väide kujul $\exists x B(x)$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_n \vdash \exists x B(x)$$

Teoreemi saab tõestada sellise taktikaga:

Valime interpretatsiooni kandja sellise elemendi b, mille korral kehtib $B(b)$, ja tõestame, et kehtib

$$A_1, \dots, A_n \vdash B(b)$$

Olenevalt olukorrast võib b olla valitud mingi konstandi, muutuja või avaldise kujul.

Tihti ei saa sellist sammu tõestuses esimesena teha, sest on vaja teada sellist elementi/avaldist, mille korral $B(b)$ on tõene.

Eeldus kujul $\exists x B(x)$

Tõestatav teoreem on kujul

$$A_1, \dots, A_{n-1}, \exists x A(x) \vdash B$$

Kui $\exists x A(x)$ on tõene, siis tingimust A rahuldav element leidub. Tähistame ta c -ga ja asendame eelduse $\exists x A(x)$ eeldusega A(c). Seega:

piisab, kui tõestame

$$A_1, \dots, A_{n-1}, A(c) \vdash B$$

Siinjuures peab c olema uus tähis. Ta ei tohi esineda teistes eeldustes ega väites B.

Väide kujul $B\&C$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_n \vdash B\&C$$

Teoreemi saab tõestada sellise taktikaga:

Tõestame

$$A_1, \dots, A_n \vdash B \quad \text{ja} \quad A_1, \dots, A_n \vdash C$$

Eeldus kujul $B\&C$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_{n-1}, B\&C \vdash D$$

Konjunktsiooni tõesusest järeldub konjunktsiooni liikmete tõesus. Seega piisab, kui tõestame

$$A_1, \dots, A_{n-1}, B, C \vdash D$$

Väide kujul $B \vee C$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \ldots, A_n \vdash B \vee C$$

Teoreemi tõestamiseks piisab, kui näitame, et
eeldustest järeldub B või eeldustest järeldub C, st

$$A_1, \ldots, A_n \vdash B \quad \text{või} \quad A_1, \ldots, A_n \vdash C$$

Tavaliselt ei saa väites olevat disjunktsiooni asendada ühe liikmega kohe tõestuse alguses, sest kumbki disjunktsiooni liige ei järeldu eeldustest.

Näiteks kui meil on tegemist lausearvutuse valemitega, siis kehtib küll $C \vee B \vdash B \vee C$, aga B ega C kumbki ei järeldu eeldustest. Kui aga ka eeldused sisaldavad disjunktsioone, siis jaguneb tõestus harudeks, kus väites oleva disjunktsiooni saab asendada sobiva liikmega.

Eeldus kujul $B \vee C$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \ldots, A_{n-1}, B \vee C \vdash D$$

Piisab, kui tõestame, et kehtivad:

$A_1, \ldots, A_{n-1}, B \vdash D$ ja $A_1, \ldots, A_{n-1}, C \vdash D$

Kui kehtivad teised eeldused ja disjunktsioon $B \vee C$, siis kehtib ka vähemalt üks lausetest B ja C ning vastavast eelduste komplektist järeldub D.

- Siin lõppes 1. märtsi loeng, järgmiste slaidide sisuga jätkatakse 8. märtsil

Punktiülesanne 4

Väide kujul $B \supset C$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_n \vdash B \supset C$$

Teoreemi saab tõestada sellise taktikaga:

Piisab, kui eeldame, et kehtib ka B, ja tõestame C, st võime teoreemi tõestamiseks tõestada

$$A_1, \dots, A_n, B \vdash C$$

Eeldus kujul $B \supset C$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_{n-1}, B \supset C \vdash D$$

Sellist eeldust/fakti saame kasutada siis, kui meil on teada, et implikatsiooni eeldus B on täidetud. Siis saame kasutada, et kehtib ka C.

Oluline näide:

Me teame paljusid juba tõestatud teoreeme. Tavaliselt on nad samuti implikatsiooni/järeldumisseose kujul:
$Eeldused \supset Väide$.

Mingit teoreemi saame oma tõestuses kasutada siis, kui oleme näidanud, et selle teoreemi eeldused on täidetud.

Väide kujul $\neg B$

Vaatleme olukorda, kus tõestatav teoreem on kujul

$$A_1, \dots, A_n \vdash \neg B$$

Eituse tõestamise levinuim võte on vastuolule viimine.
Eeldatakse vastuväiteliselt, et lisaks eeldustele kehtib ka B.
Tõestatakse, et siis saab **mingi väite** C jaoks tõestada, et kehtivad C ja $\neg C$, st piisab, kui tõestame mingi C jaoks

$$A_1, \dots, A_n, B \vdash C \quad \text{ja} \quad A_1, \dots, A_n, B \vdash \neg C$$

Millise väite C abil me vastuolu tekitame, tuleb igal korral eraldi otsustada.

Eeldus kujul $\neg B$

Tõestatav teoreem on kujul

$$A_1, \dots, A_{n-1}, \neg B \vdash C$$

Eeldus $\neg B$ tähendab, et me teame, et B on väär. Mingi väite väärus annab meile tavaliselt üsna vähe informatsiooni.

Tüüpiline eitusega eelduse tekkimise/kasutamise koht on vastuväiteline tõestus, kui teoreemi väide on ilma eituseta. Siis vastuväiteline oletus tähendab eitusega eelduse tekkimist vastuolu tõestamisel, sest me asendame

$$A_1, \dots, A_n \vdash B$$

tõestamise vastuolu tõestamisega:

$$A_1, \dots, A_n, \neg B \vdash C \quad \text{ja} \quad A_1, \dots, A_n, \neg B \vdash \neg C$$

Teoreem vastuväitelisest tõestusest

- Teoreem. Teoreemi $P \supset Q$ tõestamiseks piisab, kui tõestame $\neg Q \supset \neg P$.

See teoreem järeldub triviaalsest lausearvutuse samaväärsusest $\neg Q \supset \neg P \equiv P \supset Q$

- Teoreemi võib kirja panna sellise sekventsina:

$$\neg Q \supset \neg P \vdash P \supset Q$$

Väide kujul $B \sim C$

Tõestatav teoreem on kujul

$$A_1, \ldots, A_n \vdash B \sim C$$

Ekvivalentsi tõestamiseks tõestatakse tavaliselt kaks implikatsiooni:

$$A_1, \ldots, A_n \vdash B \supset C \quad \text{ja} \quad A_1, \ldots, A_n \vdash C \supset B$$

Eeldus kujul $B{\sim}C$

Tõestatav teoreem on kujul

$$A_1, \dots, A_{n-1}, B{\sim}C \vdash D$$

Ekvivalentsi kehtimist kasutatakse **kahel viisil:**

1) Ekvivalentsist võime järeldada mõlemasuunalised implikatsioonid, st ekvivalentsiga sekventsi tõestamiseks on piisav tõestada sekvents

$$A_1, \dots, A_{n-1}, B{\supset}C, C{\supset}B \vdash D$$

2) Kui tõestuses esineb üks valemitest B ja C, siis võime ta asendada teisega.

Kvantoriga väidete tõestamine ja ümberlükkamine

- Väite $\exists xB(x)$ **tõestamiseks** piisab, kui esitame sobiva muutuja väärtuse a ja tõestame, et kehtib B(a).
- Väite $\forall xB(x)$ **tõestamiseks** peame tõestama, et B(a) kehtib vaadeldava hulga iga elemendi a korral.

  Näited ei tõesta väite $\forall xB(x)$ kehtimist!
- Väite $\exists xB(x)$ **ümberlükkamiseks** peame tõestama, et kehtib $\forall x\neg B(x)$.

  Näited ei lükka väidet $\exists xB(x)$ ümber!
- Väite $\forall xB(x)$ **ümberlükkamiseks** piisab nn kontranäitest: esitame sobiva muutuja väärtuse a ja tõestame, et kehtib $\neg B(a)$.

$$\neg\exists xB(x) \equiv \forall x\neg B(x)$$
$$\neg\forall xB(x) \equiv \exists x\neg B(x)$$

Teoreemide kasutamisest tõestustes

Tõestustes kasutatakse peale teoreemi eeldustena kirja pandud väidete ka teadaolevaid **teoreeme**.

See, milliseid väiteid saab mingis tõestuses teadaolevate faktidena kasutada, sõltub kontekstist: mis on juba teada ja mis mitte.

- **Teadusartiklis** võib kasutada kõiki teaduslikus kirjanduses avaldatud teoreeme. Kui pole tegemist "õpikuteoreemidega", siis peab viitama allikale.
- **Loengus** saab kasutada kursuses juba esitatud teoreeme. Mõnikord kasutatakse ka kursuses tõestamata väiteid, viidates kirjandusele.
- **Eksami** sooritaja peab peale kursuses olevate üksikute teoreemide teadma ka seda, kuidas aine sisu on üles ehitatud ja mitte kasutama hilisemaid teoreeme varasemate põhjendamiseks.
- **Praktikumi/kontrolltöö ülesannete** puhul tavaliselt fikseeritakse, mida võib kasutada.