DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Veselo skaitļu teorija

11.lekcija (papildmateriāls, matemātisko pierādījumu teorija un tehnika)

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

1. Matemātisko pierādījumu teorija un tehnika

1.1. Ievads

Spēja izdarīt loģiski pareizus secinājumus un pietiekoši garas un saskaņotas šādu secinājumu virknes ir svarīga prasme, kas ir vajadzīga jebkuram cilvēkam.

Priekšzināšanas, kas ir nepieciešamas šīs nodaļas apgūšanai ir matemātiskās loģikas pamatjēdzieni -

- matemātiskie izteikumi,
- predikāti un operācijas ar tiem,
- matemātiskās loģikas formulas,
- Būla funkcijas, to normālās formas.

Matemātisko pierādījumu formalizācijas pirmos mēģinājumus veica matemātiķis G.Leibnics 17.gadsimta otrajā pusē, taču sistemātiska matemātisko pierādījumu kā matemātikas objekta pētīšana tika sākta 19.gadsimta beigās.

Matemātisko pierādījumu tehnikas pirmsākumi ir meklējami sengrieķu loģikā, kuras galvenos sasniegumus var redzēt Aristoteļa darbos.

Pārtulkojot šī perioda sasniegumus mūsdienu valodā, var izdarīt šādu loģikas kopsavilkumu. Veicot pamatotus (loģiskus) spriedumus, ir jāievēro šādi pamatlikumi:

1. *identificēšanas likums* - ja kādā spriedumā vairākas reizes jādomā par vienu un to pašu priekšmetu vai jēdzienu, tad ir jāseko, lai katru reizi tiktu domāts tieši tas pats priekšmets vai jēdziens, lai nenotiktu (apzināta vai neapzināta) jēdziena maiņa;
2. *pretrunas likums* - divi savstarpēji izslēdzošas nozīmes izteikumi nevar vienlaicīgi būt patiesi;
3. *izslēgtā trešā likums* - no diviem savstarpēji pretējas nozīmes izteikumiem viens ir patiess;

4. *pietiekošā pamatojuma likums* - nedrīkst apgalvot kāda izteikuma patiesumu, ja tam nav pietiekoša pamatojuma.

Loģikā tiek pētīti arī *jēdzieni*. Jēdziens ir ideja, kas izdala, apkopo vairākus konkrētus priekšmetus vai parādības (konkrētus vai iedomātus) pēc noteiktām pazīmēm.

Par *jēdziena saturu* sauksim tā pazīmju kopumu, par *jēdziena apjomu* sauksim objektus, kurus jēdziens izdala.

Diviem jēdzieniem ar atšķirīgu saturu var būt viens un tas pats apjoms.

Teiksim, ka pazīme A ir vājāka nekā pazīme B, ja A atbilstošais apjoms ir lielāks nekā B apjoms, citiem vārdiem sakot, ja priekšmetam piemīt pazīme B, tad tam obligāti piemīt pazīme A.

Ja jēdzienu X var iegūt no jēdziena Y atmetot vai pavājinot dažas pazīmes, tad teiksim, ka jēdziens X ir jēdziena Y vispārinājums. Atbilstošo operāciju ar jēdzieniem sauksim par *vispārināšanu*.

Cilvēka spēja izdarīt pareizus secinājumus un prognozes nākotnes paredzēšanas nolūkā ir augstākās nervu darbības funkcionalitāte, kas ir radusies evolucionārās atlases ceļā. Pamatproblēma, kas katru brīdi ir jārisina dzīviem organismiem, ir šāda: ja ir dota noteikta situācija laikā vai telpā, kāda būs šī situācija vēlākā laika momentā vai citos telpas punktos. Šī pamatproblēma liek definēt un pētīt saliktus izteikumus formā

$$"JA\ A(ir\ patiess\ izteikums), TAD\ B(ir\ patiess\ izteikums)",$$

kur A un B ir izteikumi.

Teiksim, ka predikāts q *seko (loğiski seko)* no predikāta p (apzīmē ar pierakstu $p \to q$), ja q ir patiess ar visām tām predikāta argumentu vertībām, ar kurām p ir patiess.

Citiem vārdiem sakot, ja predikāts p ir patiess ar kādu argumentu vērtību sarakstu x, tad predikāts q arī ir patiess ar šo vērtību sarakstu x . Šādā gadījumā izteikumu vai predikātu $p \to q$ sauksim par *nosacījuma apgalvojumu (NA)*.

Izteikuma vai predikāta $p \to q$ patiesumvērtība tiek definēta kā "patiess", ja tas ir NA un "nepatiess" pretējā gadījumā. Var domāt, ka

$$p \to q = \forall x(p(x) \Rightarrow q(x)),$$

kur $\Rightarrow$ ir matemātiskās loģikas implikācijas operācija.

Predikātu p sauc par *nosacījumu* vai *pietiekamo nosacījumu attiecībā uz* q, bet predikātu q - par *secinājumu* vai *nepieciešamo nosacījumu attiecībā uz* p.

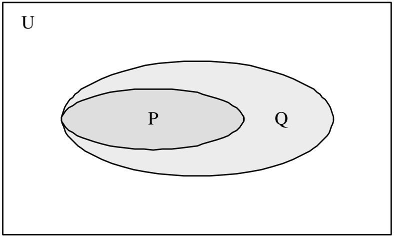
Par NA var domāt kā par predikātu, kura argumenti ir predikāti vai kā par attiecību (attieksmi) predikātu kopā, kurā tiek saistīts nosacījums un secinājums.

Izteikumu $p \to q$ formulē veidā "Ja p, tad q".

NA var saukt arī par *pareizu secinājumu*, šāds nosaukums labāk izsaka NA lomu.

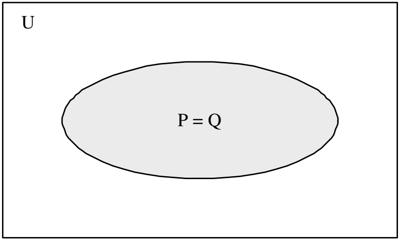
Izteikumu $(p \to q) \wedge (q \to p)$ formulēsim šādi: "p tad un tikai tad, ja q ", sauksim par *loģisko ekvivalenci* un un apzīmēsim ar $p \leftrightarrow q$.

NA var mēģināt vizualizēt, izmantojot Eilera-Venna diagrammas šādā veidā. Ja ir doti divi predikāti p un q, tad uzskatīsim, ka katrai argumentu vērtībai atbilst punkts universā, un piekārtosim katram no predikātiem to universa apakškopu, ar kuras elementu vērtībām predikāts ir patiess, apzīmēsim šīs apakškopas ar P un Q. Apakškopas P, Q sauc par predikātu p, q *patiesumvērtību kopām*. Viegli saskatīt, ka izteikuma $p \to q$ patiesums nozīmē, ka $P \subseteq Q$.



1.1. attēls. NA vizualizācija ar predikātu patiesumvērtību kopu palīdzību

Izteikuma $p \leftrightarrow q$ patiesums nozīmē, ka $P = Q$ (predikātu patiesumvērtību kopas ir vienādas).



1.2. attēls. Loģiskās ekvivalences vizualizācija ar predikātu patiesumvērtību kopu palīdzību

NA interpretācija ar patiesumvērtību kopu izmantošanu ļauj noformulēt NA kritēriju gadījumā, kad predikātu argumenti ir Būla mainīgie un predikāti ir izteikti PDNF.

1.1. teorēma. $p \to q$ ir NA $\Longleftrightarrow$ katra elementārā konjunkcija, kas piedalās predikāta p PDNF, piedalās arī predikāta q PDNF.

PIERĀĪJUMS

Pieņemsim, ka $p \to q$ ir NA, tātad, ja $p(X_1^{\varepsilon_1}, X_2^{\varepsilon_2}, ..., X_n^{\varepsilon_n})$ ir patiess, tad arī $q(X_1^{\varepsilon_1}, X_2^{\varepsilon_2}, ..., X_n^{\varepsilon_n})$ ir patiess.

Izteikums $p(X_1^{\varepsilon_1}, X_2^{\varepsilon_2}, ..., X_n^{\varepsilon_n})$ ir patiess $\Longleftrightarrow$ elementārā konjunkcija $X_1^{\varepsilon_1} X_2^{\varepsilon_2} ... X_n^{\varepsilon_n}$ piedalās predikāta p PDNF.

$q(X_1^{\varepsilon_1}, X_2^{\varepsilon_2}, ..., X_n^{\varepsilon_n})$ ir patiess $\Longleftrightarrow$ tā pati konjunkcija piedalās arī predikāta q PDNF.

Tātad, ja $X_1^{\varepsilon_1}, X_2^{\varepsilon_2}, ..., X_n^{\varepsilon_n}$ piedalās predikāta p PDNF, tad tā piedalās arī predikāta q PDNF.■

Par divu NA $p \to q$ un $q \to r$ *kompozīciju* sauksim izteikumu $p \to r$. Par *pierādījumu* sauksim vairāku NA kompozīciju:

$$(p \mapsto q) = (p = p \to p_2 \to ... \to p_{n-1} \to p_n = q).$$

Var redzēt, ka pierādījums arī ir NA: ja visi izteikumi

$$p_1 \to p_2, p_2 \to p_3, ..., p_{n-1} \to p_n$$

ir patiesi, tad, ja izteikums $p_1(x)$ ir patiess, tad $p_2(x)$ ir patiess; ja $p_2(x)$ ir patiess, tad $p_3(x)$ ir patiess; ...; ja $p_{n-1}(x)$ ir patiess, tad $p_n(x)$ ir patiess. Tātad kompozīcija $p_1 \to p_n$ arī ir NA.

Par *teorēmu* (no grieķu valodas) sauksim izteikumu, kas tiek iegūts pareiza pierādījuma ceļā no *aksiomām* (dotiem predikātiem vai izteikumiem, kas tiek definēti par patiesiem, grieķu valodā atbilstošā vārda nozīme ir "vērtīgs"). Parasti teorēmas veido formā $p \to q$ ("no p seko q") vai $p \leftrightarrow q$ ("p tad un tikai tad, ja q" vai "$p \to q$ un $q \to p$ ").

Par *lemmu* sauksim teorēmu, kas ir starpposms kādas svarīgākas teorēmas pierādījumā.

Par *secinājumu no teorēmas* sauksim izteikumu, ko var relatīvi viegli pierādīt, pieņemot šo teorēmu.

Par apgalvojuma/teorēmas $p \to q$

- *apgriezto apgalvojumu* sauksim $\overline{q} \rightarrow \overline{p}$,
- *pretējo apgalvojumu* sauksim $q \rightarrow p$,
- *pretējam apgriezto (inverso) apgalvojumu* sauc $\overline{p} \rightarrow \overline{q}$.

Par *matemātisku teoriju* vai *pierādījumu sistēmu* sauksim struktūru, kas satur

- fiksētu alfabētu,
- apgalvojumu veidošanas likumus,
- fiksētu aksiomu kopu,
- fiksētu NA veidu (likumu) kopu.

Aksiomas var būt gan vispārīgas (loģiskas), gan arī specifiskas dotajai teorijai (neloģiskas). Aksiomu kopa var būt gan galīga, gan arī bezgalīga. Aksiomu kopu sauksim par neatkarīgu, ja neviena no aksiomām nav pierādāma, izmantojot pārējās aksiomas.

Parasti dotajā teorijā atļauto NA veidu kopa ir galīga.

Katras matemātiskās teorijas attīstība sastāv no tās objektu un valodas koordinatizēšanas un formalizēšanas, teorēmu pierādīšanas, teorijas galamērķu noteikšanas un sasniegšanas.

Matemātisku teoriju sauksim par

- *nepretrunīgu* ja nav iespējams pierādīt kādu apgalvojumu s un tā noliegumu $\neg s$,
- pilnu, ja tajā katra patiesa teorēma ir pierādāma.
- atrisināmu, ja eksistē algoritms (piemēram, Tjūringa mašīna), kas katram teorijas apgalvojumam nosaka, vai tas ir pierādāms.

1.2. Svarīgākie nosacījuma apgalvojumu veidi

Pārskatīsim dažus vienkāršākos NA konstruēšanas veidus. Vairāki no tiem ir aprakstīti jau Senās Grieķijas vai Romas filozofu darbos, tāpēc to nosaukumi ir pārņemti no latīņu valodas.

Pēc savas būtības NA konstruēšanas veidi seko no kopu teorijas, tāpēc ir lietderīgi apskatīt atbilstošos apgalvojumus par predikātu patiesumvērtību kopām un vizualizēt šos NA veidus, izmantojot Eilera-Venna diagrammas.

NA konstruēšanas likumus apzīmē ar *kanonisko pierakstu*

$$\frac{p_1, ..., p_n}{q},$$

kas nozīmē NA $\left(p_1 \wedge ... \wedge p_n\right) \rightarrow q$.

1.2.1. Modus ponens

Kanoniskais pieraksts -

$$\frac{p \rightarrow q, p}{q}.$$

Šis NA veids ir ekvivalents NA definīcijai.

1.2.2. Modus tollens

Kanoniskais pieraksts -

$$\frac{p \to q, \neg p}{\neg q}.$$

Šis NA veids ir ekvivalents NA definīcijai.

1.2.3. Kontrapozīcijas likums

Kanoniskais pieraksts -

$$\frac{p \to q}{\neg q \to \neg p}.$$

Šis NA veids ir ekvivalents NA definīcijai.

1.2. teorēma. Teorēma ir patiesa $\iff$ apgrieztā teorēma ir patiesa.

1.2.4. Ekvivalences secināšanas likums

Kanoniskais pieraksts -

$$\frac{p \to q, q \to p}{p \leftrightarrow q}.$$

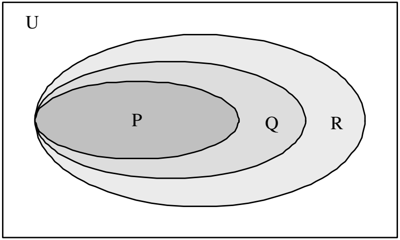
Šis NA veids atbilst kopu īpašībai $P \subseteq Q$ un $Q \subseteq P \implies P = Q$.

1.2.5. Hipotētiskais silloģisms

Kanoniskais pieraksts -

$$\frac{p \to q, q \to r}{p \to r.}$$

Šis NA veids atbilst faktam, ka NA kompozīcija ir NA.



1.3. attēls. Hipotētiskā silloģisma vizualizācija

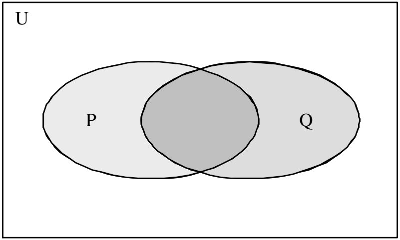
1.1. piemērs. Ja katrs DU students mācās sekmīgi un katrs sekmīgs students saņem stipendiju, tad katrs DU students saņem stipendiju.

1.2.6. Disjunktīvais silloģisms

Kanoniskais pieraksts -

$$\frac{p \vee q, \neg p}{q}.$$

Šis NA atbilst kopu īpašībai $(P \cup Q) \cap \overline{P} \subseteq Q$.



1.4. attēls. Disjunktīvā silloģisma vizualizācija

1.2. piemērs. Jānis dzīvo vai nu Daugavpilī, vai Rīgā. Ja Jānis nedzīvo Rīgā, tad Jānis dzīvo Daugavpilī.

1.2.7. Disjunktīvā pievienošana

Kanoniskais pieraksts -

$$\frac{p}{p \vee q}.$$

Šis NA veids atbilst kopu īpašībai $P \subseteq P \cup Q$.

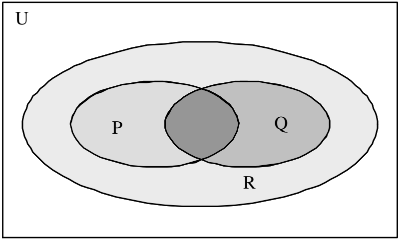
1.3. piemērs. Ja reāls skaitlis ir lielāks par 0, tad tas ir lielāks vai vienāds ar 0. Ja Jānis dzīvo Daugavpilī, tad Jānis dzīvo kādā no Latvijas pilsētām.

1.2.8. Dilemma

Kanoniskais pieraksts -

$$\frac{p \vee q, p \rightarrow r, q \rightarrow r}{r}.$$

Šis NA veids atbilst šādai kopu īpašībai: ja $P \subseteq R$ un $Q \subseteq R$, tad $P \cup Q \subseteq R$.



1.5. attēls. Dilemmas vizualizācija

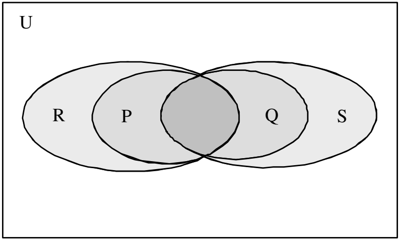
1.4. piemērs. Ir dots, ka, ja $x > 1$, tad $f(x) < 0$, un, ja $x < -1$, tad $f(x) < 0$. Var secināt, ka, ja $|x| > 1$, tad $f(x) < 0$.

1.2.9. Konstruktīvā dilemma

Kanoniskais pieraksts -

$$\frac{p \vee q, p \rightarrow r, q \rightarrow s}{r \vee s}.$$

Šis NA veids atbilst šādai kopu īpašībai: ja $P \subseteq Q$ un $R \subseteq S$, tad $P \cup R \subseteq Q \cup S$.



1.6. attēls. Konstruktīvās dilemmas vizualizācija

1.5. piemērs. Ir dots, ka ja $x > 1$, tad $f(x) < 0$ un ja $x < -1$, tad $f(x) > 1$. Var secināt, ka, ja $|x| > 1$, tad $f(x) < 0$ vai $f(x) > 1$.

1.2.10. Destruktīvā dilemma

Kanoniskais pieraksts -

$$\frac{(\neg q) \vee (\neg s), p \to q, r \to s}{(\neg p) \vee (\neg r)}.$$

Šis NA veids atbilst šādai kopu īpašībai: ja $P \subseteq Q$ un $R \subseteq S$, tad $\overline{Q} \cup \overline{S} \subseteq \overline{P} \cup \overline{R}$.

1.6. piemērs. Ir dots, ka, ja $x > 1$, tad $f(x) < 0$ un, ja $x < -1$, tad $f(x) > 1$. Var secināt, ka, ja $f(x) \geq 0$ vai $f(x) \leq 1$, tad $x \leq 1$ vai $x \geq -1$.

1.2.11. Nosacītais pierādījums

Kanoniskais pieraksts -

$$\frac{p, (p \wedge q) \to r}{q \to r}.$$

Šis NA veids atbilst šādai kopu īpašībai: ja $P \cap Q \subseteq R$, tad $P \cap Q \subseteq P \cap R$.

1.7. piemērs. Ir dots, ka, ja $x > 1$ un $y < -1$, tad $f(x, y) > 1$. Var secināt, ka, ja $x > 1$, tad no tā, ka $y < -1$, seko $f(x, y) > 1$.

1.8. piemērs. Pieņemsim, ka $p(x) =$"x ir strādīgs cilvēks", $q(x) =$"x ir matemātiski apdāvināts cilvēks" un $r(x) =$"x ir izcils mūziķis". Pieņemsim, ka cilvēks ir izcils matemātiķis, ja viņš ir gan strādīgs, gan matemātiski apdāvināts. Izmantojot nosacītās secināšanas likumu, var secināt, ka, ja cilvēks ir strādīgs, tad, lai šis cilvēks būtu izcils matemātiķis, pietiek ar to, ka viņš ir matemātiski apdāvināts.

1.2.12. Konjunktīvā vienkāršošana

Kanoniskais pieraksts -

$$\frac{p \wedge q}{p}.$$

Šis NA veids atbilst kopu īpašībai $P \cap Q \subseteq P$.

1.2.13. Pretrunas likums

Kanoniskais pieraksts -

$$\frac{p \to c}{\neg p},$$

kur c ir pretruna (identiski aplams izteikums). Šis NA veids atbilst šādai kopu īpašībai: ja $P = \emptyset$, tad $\overline{P} = U$.

1.9. piemērs. Ja no tā, ka $x > 1$ seko, ka $2 + 2 = 5$, tad var secināt, ka $x \leq 1$.

Nākamie NA veidi satur universālos vai eksistences kvantorus. Pieņemsim, ka predikātu argumenti ir kādas kopas A elementi.

1.2.14. Patvaļīga elementa konkretizācija

Kanoniskais pieraksts -

$$\frac{\forall x \in X \;\; P(x)}{P(a)}, \text{ kur } a \in A \text{ ir patvaļīgs.}$$

1.2.15. Vispārināšana sākot no patvaļīga elementa

Kanoniskais pieraksts -

$$\frac{P(a)}{\forall x \in X \ P(x)}, \text{ kur } a \in A \text{ ir patvaļīgs.}$$

Šo NA likumu bieži izmanto pierādījumos. Ja predikāts ir patiess ar patvaļīgu argumentu vērtību, tad tas ir patiess ar jebkuru argumenta vērtību.

1.2.16. Eksistenciālā specifikācija

Kanoniskais pieraksts -

$$\frac{\exists\, x \in X \ P(x)}{P(a)} \text{ vismaz vienam } a \in A.$$

1.2.17. Eksistenciālā vispārināšana

Kanoniskais pieraksts -

$$\frac{P(a) \text{ } vismaz \text{ } vienam \text{ } a \in A}{\exists \, x \in A \; P(x)}.$$

1.2.18. Universālais modus ponens

Kanoniskais pieraksts -

$$\frac{P(a) \to Q(a) \text{ } jebkuram \text{ } a \in A}{\forall \, x \in A \; (P(x) \to Q(x))}.$$

1.3. Pierādījumu veidi

Šajā nodaļā mēs apskatīsim dažas biežāk pielietotās vispārīgās teorēmu pierādīšanas stratēģijas.

1.3.1. Tiešais pierādījums

$\underline{p \to q}$ Pieņemam, ka izteikums vai predikāts p ir patiess ar vispārīgiem predikātu argumentiem, un pierādām, ka pierādāmais izteikums vai predikāts q ir patiess.

1.10. piemērs. Pierādīsim šādu apgalvojumu: "Ja n un m ir pāra skaitļi, tad arī $n+m$ ir pāra skaitlis". Šo apgalvojumu var pierādīt ar šādu nosacījuma apgalvojumu virkni. Ja n un m ir pāra skaitļi, tad $n = 2n_1$ un $m = 2m_1$. Ja $n = 2n_1$ un $m = 2m_1$, tad $n+m = 2(n_1+m_1)$. Ja $n+m = 2(n_1+m_1)$, tad $n+m = 2s$, kur s ir vesels skaitlis. Ja $n+m = 2s$, tad $n+m$ ir pāra skaitlis.

$\underline{(\forall\, x \in A)P(x)}$ Pieņemam, ka x ir patvaļīgs elements, un pierādam, ka $P(x)$ ir patiess.

1.11. piemērs. Patvaļīgs pāra skaitlis x ir izsakāms formā $x = 2y$, kur $y \in \mathbb{Z}$, tātad jebkurš pāra skaitlis ir izsakāms šādā formā.

1.3.2. Konstruktīvais tiešais pierādījums

Šo pierādījuma veidu parasti izmanto, ja ir jāpierāda apgalvojumi, kuros ir iesaistīti eksistences kvantori.

$(\exists x \in A)P(x)$ Lai pierādītu šādu izteikumu, ir jāpierāda vismaz viena tāda elementa x eksistence, ar kuru predikāts $P(x)$ ir patiess. Šajā stratēģijā mēs atrodam vai konstruējam konkrētu elementu x, ar kuru $P(x)$ ir patiess.

1.12. piemērs. Ir jāpierāda šāds apgalvojums: "Eksistē pirmskaitlis, kas ir mazāks nekā 20 un lielāks nekā 10". Lai pierādītu šo apgalvojumu, pietiek uzrādīt skaitli 13.

$\forall x \in A\ \exists x \in A\ P(x, y)$ Lai pierādītu šādu izteikumu, katram x ir jāpierāda vismaz viena tāda elementa y eksistence, ar kuru predikāts $P(x, y)$ ir patiess. Mēs fiksējam patvaļīgu elementu x un atrodam konkrētu elementu y, kuram $P(x, y)$ ir patiess.

1.13. piemērs. Ir jāpierāda apgalvojums $\forall n\ \exists m : m > n$. Ja n

ir fiksēts, tad definēsim $m_0 = n + 1$, skaitļu pāris (n, m_0) apmierina pierādāmo apgalvojumu.

1.3.3. Nekonstruktīvais tiešais pierādījums

Šo pierādījumu veidu arī izmanto tādu apgalvojumu pierādīšanā, kas satur eksistences kvantorus, bet atšķirībā no konstruktīvā veida, šajā gadījumā pierāda apgalvojumus, neuzrādot konkrētus kopu elementus.

1.14. piemērs. Ir jāpierāda apgalvojums: "$\forall n\ \exists p : p > n$ un p ir pirmskaitlis". Šo apgalvojumu var pierādīt, izmantojot pirmskaitļu kopas bezgalību: eksistē bezgalīgi daudz pozitīvu pirmskaitļu, tātad vismaz viens no tiem ir lielāks nekā n.

1.3.4. Pierādījums apskatot speciālgadījumus

Šo stratēģiju izmanto, pierādot apgalvojumus formā

$$p \to q, \text{ kur } p = p_1 \vee p_2 \vee ... \vee ...p_n.$$

Izmantojot dilemmas secināšanas likumu, redzam, ka šāds apgalvojums ir pierādīts, ja pierāda, ka katram i izpildās $p_i \to q$.

1.15. piemērs. Ir jāpierāda apgalvojums: "Ja $n = 2m + 1$, tad $8|n^2 - 1$". Ja n ir nepāra skaitlis, tad $n = 4k + 1$ vai $n = 4k + 3$, ir jāpierāda, ka katrā no šiem gadījumiem izpildās $8|n^2-1$. Ja $n = 4k+1$, tad

$$n^2 - 1 = (4k + 1)^2 - 1 = 16k^2 + 8k = 8(2k^2 + k),$$

tātad $8|n^2 - 1$. Ja $n = 4k + 3$, tad

$$n^2 - 1 = (4k + 3)^2 - 1 = 16k^2 + 24k + 8 = 8(2k^2 + 3k + 1),$$

tātad arī šajā gadījumā $8|n^2 - 1$.

1.3.5. Netiešais pierādījums jeb pierādījums izmantojot kontrapozīciju

Lai pierādītu apgalvojumu $p \to q$, var izmantot kontrapozīcijas secināšanas likumu: pieņemam, ka $\bar{q}$ ir patiess, un pierādām, ka $\bar{p}$ ir patiess.

1.16. piemērs. Ir jāpierāda apgalvojums: "Ja n^2 ir pāra skaitlis, tad n ir pāra skaitlis". Pieņemsim, ka $n = 2k + 1$. Tādā gadījumā

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Ir pierādīts, ka, ja n ir nepāra skaitlis, tad arī n^2 ir nepāra skaitlis, līdz ar to sākotnējais apgalvojums ir pierādīts.

1.3.6. Pierādījumi ar pretrunas palīdzību

Šajā stratēğijā pieņem, ka pierādāmā apgalvojuma noliegums ir patiess, un no šī pieņēmuma secina identiski nepatiesu izteikumu (pretrunu).

$\underline{p \to c}$ Šajā stratēgijā pieņem, ka pierādāmā apgalvojuma noliegums ir patiess, un pierāda, ka no tā seko pretruna, citiem vārdiem sakot, pierāda, ka secinājums

$$\neg(p \to q)) \to c,$$

kur c ir pretruna, ir NA.

1.17. piemērs. Pierādīsim, ka $\sqrt{3} \notin \mathbb{Q}$. Pieņemsim, ka $\sqrt{3}$ ir racionāls skaitlis $\frac{m}{n}$. Pieņemsim, ka $3 \nmid m$, vai arī $3 \nmid n$. Iegūstam, ka $3n^2 = m^2 \implies 3|m$ un $3|n$, kas ir pretruna.

$\underline{(\exists x \in A)P(x)}$ Pieņem, ka visiem x izteikums $P(x)$ ir nepatiess un parāda, ka tas noved pie pretrunas.

1.18. piemērs. $n+1$ balodis tiek likts n būros. Pierādīt, ka eksistē būris, kurā ir vismaz 2 baloži. Ja katrā būrī būtu 0 vai 1 balodis, tad kopā būtu ne vairāk kā n baloži, kas ir pretruna.

$\underline{(\forall x \in A)P(x)}$ Pieņem, ka eksistē x, kuram ir $P(x)$ nepatiess, un parāda, ka tas noved pie pretrunas.

1.3.7. Disjunkcijas $p \to (q \vee r)$ pierādīšana

Lai pierādītu šādu apgalvojumu, pietiek pierādīt, ka vismaz viens no apgalvojumiem $p \to q$ vai $p \to r$ ir patiess. Vispārīgā gadījumā neviens no šiem apgalvojumiem var nebūt patiess, tāpēc, analizējot disjunkcijas apgalvojumu ar patiesumvērtību kopu palīdzību, varam iegūt vismaz divas disjunkcijas apgalvojumam ekvivalentas apgalvojumu sistēmas:

- $p \to (q \vee r)$ tad un tikai tad, ja

$$((p \wedge (\neg q)) \to r) \vee ((p \wedge (\neg r)) \to q)$$

  ir patiess, citiem vārdiem sakot, lai pierādītu disjunkciju, ir pietiekoši un nepieciešams pierādīt, ka vismaz viens no apgalvojumiem $((p \wedge (\neg q)) \to r)$ vai $((p \wedge (\neg r)) \to q)$ ir patiess,

- $p \to (q \vee r)$ tad un tikai tad, ja

$$p \wedge (\neg q) \wedge (\neg r)$$

  ir identiski aplams izteikums.

1.3.8. Vairāku apgalvojumu ekvivalences pierādīšana ar cikla palīdzību

Šo metodi izmanto, lai pierādītu vairāku apgalvojumu loģisko ekvivalenci:

$$p_i \leftrightarrow p_j,\ \forall i, j. \tag{1}$$

Pierādām, ka visi izteikumi

$$p_1 \to p_2, p_2 \to p_3, ..., p_i \to p_{i+1}, ..., p_{n-1} \to p_n, p_n \to p_1 \tag{2}$$

ir NA. Tā kā NA kompozīcija ir NA, tad eksistē pierādītu NA virkne, kas savieno jebkurus divus apgalvojumus p_i un p_j.

1.19. piemērs. Ir doti trīs divu naturālu argumentu predikāti:

$$P_1(a,b) = \text{"}a|b\text{"}, P_2(a,b) = \text{"}MKD(a,b) = b\text{"}, P_3(a,b) = \text{"}\lfloor \frac{b}{a} \rfloor = \frac{b}{a}\text{"}.$$

Ir jāpierāda, ka tie ir ekvivalenti, tas ir, to patiesumvērtību kopas sakrīt. Pierādīsim šo apgalvojumu ar cikla palīdzību - pierādīsim 3 nosacījuma apgalvojumus:

$$P_1 \to P_2, P_2 \to P_3, P_3 \to P_1.$$

Tiešām, ja $a|b$, tad $MKD(a,b) = b$. Ja $MKD(a,b) = b$, tad b dalās ar a un $\lfloor \frac{b}{a} \rfloor = \frac{b}{a}$. Ja $\lfloor \frac{b}{a} \rfloor = \frac{b}{a}$, tad b dalās ar a un cikls ir noslēgts.

1.4. Apgalvojumu atspēkošana

Pierādot matemātiskus apgalvojumus, nereti gadās, ka sākotnējais NA, kuru mēģina pierādīt, nav patiess. Ja nav saskatāms ceļš sākotnējā apgalvojuma pierādīšanai, ir lietderīgi sākt domāt par tā nolieguma pierādīšanu. To var mēģināt darīt, apskatot speciālgadījumus vai piemērus.

Apgalvojumu nepatiesuma pierādīšanas tehnika ir daļa no matemātisko pierādījumu tehnikas.

Apgalvojuma atspēkošana ir apgalvojuma nepatiesuma pierādījums. Apgalvojuma

$$(\forall x \in A)P(x)$$

pretpiemērs ir elements $c \in A$ tāds, ka $P(c)$ ir nepatiess izteikums.

Lai atspēkotu kādu apgalvojumu formā $(\forall x \in A)P(x)$, pietiek atrast vienu pretpiemēru.

Pretpiemēra eksistences pierādīšana var tikt veikta konstruktīvi vai nekonstruktīvi. Konstruktīvajā gadījumā ir lietderīgi meklēt pretpiemēru ar ekstremālām īpašībām, piemēram, kā kopas maksimālu vai minimālu elementu ar noteiktu īpašību.

Lai atspēkotu apgalvojumu formā $(\exists x \in A)P(x)$, ir jāpierāda apgalvojums $(\forall x \in A)(\neg P(x))$.

1.20. piemērs. Apskatīsim "apgalvojumu" $a^2 < b^2 \to a < b$. Lai atspēkotu šo apgalvojumu, pietiek atrast vienu skaitļu pāri ar šādām īpašībām: $a^2 < b^2$ un $a > b$. Par šādu skaitļu pāri var ņemt pāri $(1, -2)$.

1.21. piemērs. Apskatīsim šādu izteikumu: "*vienādojumam* $2x = 1$ *eksistē atrisinājums veselos skaitļos*". Lai atspēkotu šo apgalvojumu, ir jāpierāda, ka nekādam veselam skaitlim x vienādojums $2x = 1$ nevar izpildīties. To var viegli redzēt, apskatot atlikumus pēc moduļa 2.

1.5. Matemātiskā indukcija

1.5.1. Vienkāršā indukcija

Relatīvi bieži ir jāpierāda apgalvojumi formā

$$\forall n \; P(n), \; kur \; n \in \mathbb{N} \; vai \; n \in \mathbb{N} \backslash \{1, 2, ..., n_0\}.$$

Ir skaidrs, ka nav iespējams galīgā laikā pierādīt visus apgalvojumus $P(n)$, ja mēs pieņemam, ka katra šāda apgalvojuma pierādīšanai cilvēkam vai skaitļošanas mašīnai ir nepieciešams no apakšas ierobežots laika intervāls.

Apgalvojumu $\forall n \; P(n)$ pierādīšanai ir izstrādāta pierādījumu tehnika, ko sauc par *matemātisko indukciju*.

Matemātiskās indukcijas pamatideja ir pierādīt, ka katram n izteikums

$$P(n) \to P(n+1)$$

ir NA.

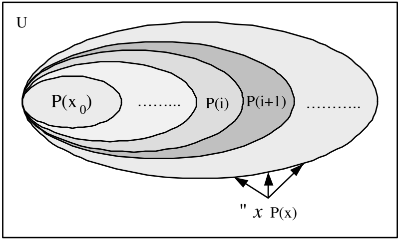
Matemātiskās indukcijas princips ir secināšanas likums, ar kuru pierāda, ka predikātam $P(n)$ ar definīcijas apgabalu $\mathbb{N}$ vai, vispārīgā gadījumā, $\mathbb{N}\backslash F$, $|F| < \infty$, atbilstošais universālais kvantors $\forall n\ P(n)$ ir patiess.

Matemātiskās indukcijas princips balstās uz hipotētiskā silloģisma (NA kompozīcijas) secināšanas likumu.

Realizējot matemātiskās indukcijas principu, ir jāveic šādas darbības:

- jāpierāda, ka izteikums $P(n_0)$ ir patiess kādam pietiekoši lielam $n_0 \in \mathbb{N}$,
- jāpierāda, ka izteikums $P(i) \to P(i+1)$ ir NA visiem $i \geq n_0$, citiem vārdiem sakot, jāpieņem, ka izteikums $P(i)$ ir patiess, un jāpierāda, ka no tā seko, ka $P(i+1)$ ir patiess.

Izmantojot patiesumvērtību kopas matemātiskās indukcijas principu, var vizualizēt šādā veidā.



1.7. attēls. Matemātiskās indukcijas principa vizualizācija

Formāli matemātiskās indukcijas principu var pierakstīt šādā NA likuma formā

$$\frac{P(n_0), (\forall i \geq n_0)[P(i) \to P(i+1)]}{(\forall n \geq n_0)P(n)}.$$

- Apgalvojumu $P(n_0)$ sauksim par *indukcijas bāzi*,
- apgalvojuma $P(i)$ patiesuma pieņemšanu sauksim par *indukcijas pieņēmumu*,

- apgalvojuma $P(i) \to P(i+1)$ pierādīšanu sauksim par *indukcijas soļa* pierādīšanu,
- predikāta P argumentu sauksim par *indukcijas argumentu* vai *indukcijas parametru*.

1.22. piemērs. Pierādīsim šādu apgalvojumu: "katram naturālam skaitlim n izpildās vienādība $1 + 2 + ... + n = \frac{n(n+1)}{2}$". Ja $n = 1$, tad vienādība ir pareiza. Pieņemsim, ka vienādība ir pareiza ar kādu argumentu $n = i$, un pierādīsim, ka tad formula ir pareiza ar argumenta vērtību $n = i + 1$. Varam redzēt, ka

$1 + 2 + ... + i + (i + 1) = (1 + 2 + ... + i) + (i + 1) = \frac{i(i+1)}{2} + i + 1 = \frac{(i+1)(i+2)}{2}$, kas arī pierāda apgalvojumu.

1.5.2. Pastiprinātā indukcija

Pastiprinātās matemātiskās indukcijas princips predikātam P (vienkāršākajā speciālgadījumā) - $\forall\, n$ pierādīt, ka

$$P(1) \wedge P(2) \wedge ... \wedge P(n) \to P(n+1)$$

ir NA.

Pastiprinātais matemātiskās indukcijas princips ir tāds secināšanas likums, ar kuru pierāda, ka predikāts $P(n)$ ir patiess visiem $n \geq n_0$:

$$\frac{P(n_0), (\forall k \geq n_0)[(\bigwedge_{i=n_0}^{k} P(i)) \to P(k+1)]}{(\forall n \geq n_0) P(n)}. \quad (3)$$

Tātad, lai ar matemātiskās indukcijas metodi pastiprinātajā formā pierādītu, ka predikāts $P(n)$ ir patiess visiem $n \geq n_0$, ir jāveic šādas darbības:

- jāpierāda, ka $P(n_0)$ ir patiess,
- jāpieņem, ka $P(i)$ ir patiess visiem $n_0 \leq i \leq k$ (tas ir, visi izteikumi $P(n_0), ..., P(k)$ ir patiesi), un jāpierāda, ka tad izteikums $P(k+1)$ ir patiess.

1.23. piemērs. Pierādīsim apgalvojumu: "$\forall\ n \geq 2\ \exists p : p|n$" (katram naturālam skaitlim, kas lielāks nekā 2, eksistē pirmskaitlis, kas to dala). Pieņemsim, ka apgalvojums ir patiess visiem naturāliem skaitļiem, kas ir stingri mazāki nekā k. Katrs naturāls skaitlis dalās ar vismaz diviem skaitļiem - ar 1 un pats ar sevi. Ja k dalās tikai ar diviem skaitļiem, tad tas ir pirmskaitlis un apgalvojums ir pierādīts. Ja k dalās vēl ar kādu skaitli a, tad $a < k$ un saskaņā ar indukcijas pieņēmumu eksistē pirmskaitlis p, kas dala a un tātad arī k.

Sarežģītu apgalvojumu pierādīšanai tiek izmantotas arī citas matemātiskās indukcijas metodes shēmas, kuras atšķiras no aprakstītajām ar indukcijas soli.

Jebkurš pierādījums ar parasto matemātiskās indukcijas metodi var tikt uzskatīts par pierādījumu ar pastiprinātās indukcijas metodi, jo parastās indukcijas metodes pieņēmums ir pastiprinātās indukcijas pieņēmuma secinājums. Izrādās, ka arī pastiprinātās indukcijas pierādījums var tikt pārveidots par parastās indukcijas pierādījumu.

1.3. teorēma. Apgalvojuma $(\forall n \geq n_0)P(n)$ pierādījumu ar pastiprinātās matemātiskās indukcijas metodi var pārveidot par tā pierādījumu ar parasto matemātiskās indukcijas metodi.

PIERĀDĪJUMS Definēsim jaunu predikātu

$$Q(n) = (\forall k : n_0 \leq k \leq n) P(k),$$

ievērosim, ka

$$(\forall n \geq n_0)[Q(n) \to P(n)].$$

Konstruēsim parastās matemātiskās indukcijas pierādījumu apgalvojumam

$$(\forall n \geq n_0) Q(n).$$

Indukcijas bāze ir $Q(n_0) = P(n_0)$, tāpēc te nekas nav jāpierāda.

Pastiprinātās indukcijas solis ir NA $\Longrightarrow$ $((\forall k \leq n)P(k)) \to P(n+1)$ jeb $Q(n) \to P(n+1)$. $Q(n) \to P(n+1)$ ir NA $\Longrightarrow$

$$Q(n) \to (Q(n) \wedge P(n+1)) = Q(n+1)$$

arī ir NA, un tātad ir pierādīts, ka

$$(\forall n \geq n_0)[Q(n) \to Q(n+1)],$$

kas ir parastās indukcijas solis. Līdz ar to apgalvojums

$$(\forall n \geq n_0) Q(n)$$

un tātad arī

$$(\forall n \geq n_0)P(n)$$

ir pierādīts ar parastās indukcijas metodi. ■

Apgalvojuma $(\forall n \geq n_0)P(n)$ pierādīšanai var izmantot arī citas matemātiskās indukcijas principa modifikācijas, kas atšķiras no klasiskās ar bāzi un indukcijas soli. Piemēram, varam uzskatīt, ka indukcijas bāze ir trīs izteikumu

$$P(n_0), P(n_0+1), P(n_0+2)$$

konjunkcija un indukcijas solis ir

$$P(k) \to P(k+3).$$

Tiek izmantota arī matemātiskā indukcija, kurā indukcijas parametrs pieder skaitļu kopas Dekarta reizinājumam.

1.5.3. Minimālā pretpiemēra metode

Matemātiskās indukcijas principam ekvivalenta pierādīšanas tehnika ir *minimāla pretpiemēra metode*. Šajā metodē izmanto to faktu, ka katra netukša naturālo skaitļu kopas apakškopa satur minimālo elementu.

Pieņemsim, ka ir jāpierāda apgalvojums $(\forall n \geq n_0)P(n)$. Pieņemsim pretējo - $\exists$ netukša kopa $F \subseteq \mathbb{N} : (\forall n \in F)(\neg P(n))$. Apskatīsim šīs kopas vismazāko elementu m. Ja $m = n_0$, tad to var viegli pārbaudīt. Ja $m > n_0$, tad $m - 1$ nepieder kopai F. Lai pierādītu apgalvojumu $(\forall n \geq n_0)P(n)$, mums atkal ir jāpierāda, ka $P(n_0)$ ir patiess un ka, ja $P(m-1)$ ir patiess, tad $P(m)$ ir patiess visiem $m > n_0$.

1.5.4. Strukturālā indukcija

Matemātiskās indukcijas principu var vispārināt, ja predikāta argumentu kopā var definēt noteikta veida daļēji sakārtotas kopas struktūru.

1.24. piemērs. Kopā $\mathbb{N}$ var dabiski definēt daļēji sakārtotas kopas struktūru, ja sakārtojuma attiecība ir skaitļu salīdzināšanas attiecība, šai attiecībai atbilstošais Hasses grafs ir grafs, kura vienīgās šķautnes ir veidā $x \leftarrow x+1$, skaitlis 1 ir vienīgais minimālais elements, katram naturālam skaitlim eksistē galīgs skaits šķautņu ķēdē, kas to savieno ar skaitli 1. Matemātiskās indukcijas princips pēc būtības sastāv no NA

$$P(k) \to P(k+1)$$

pierādīšanas katrai $\mathbb{N}$ Hasses grafa šķautnei $k \leftarrow k+1$.

Pieņemsim tagad, ka mums ir jāpierāda apgalvojums $(\forall x \in X)P(x)$, kur kopa X ir tāda, ka tajā var uzdot daļēja sakārtojuma attiecību ar šādām īpašībām (*galīgu dilstošo ķēžu nosacījumu*): katrai kopas X elementu virknei $x \geq x_1 \geq ... \geq x_n \geq ...$ $\exists n \in \mathbb{N}: \ \forall\ m \geq n$ izpildās nosacījums $x_m = x_n$ (katra dilstoša elementu virkne stabilizējas pēc galīga soļu skaita).

1.25. piemērs. $\mathbb{N}$ šo īpašību apmierina, jo par katru skaitli n mazāki ir tikai galīgās kopas $\{1, 2, ..., n-1\}$ elementi.

Apgalvojumu $(\forall x \in X)P(x)$ var mēģināt pierādīt ar *strukturālās indukcijas metodi*:

- jāpierāda, ka apgalvojums $P(x)$ ir patiess, ja x ir minimāls elements kopā X (vispārīgā gadījumā minimālo elementu kopa var būt pat bezgalīga, taču pierādīt apgalvojumu $P(x)$, ja x ir minimāls elements, iespējams, var relatīvi viegli),
- jāpierāda *strukturālās indukcijas soļi* $P(x) \to P(z)$, kur elementi x un z ir tādi, ka kopas X Hasses grafā eksistē šķautne $x \leftarrow z$.

Dilstošo ķēžu nosacījums šajā metodē ir svarīgs tāpēc, ka tas nodrošina jebkura kopas elementa sasniegšanu no kāda minimāla elementa ar galīga soļu skaita palīdzību.

Bieži vien strukturālās indukcijas solis sastāv no galīga skaita NA $P(x) \to P(f_i(x))$ pierādīšanas, kur pārveidojumi f_i raksturo daļēji sakārtotās kopas Hasses grafa uzbūvi, piemēram, matemātiskās indukcijas gadījumā ir tikai viens pārveidojums $f(x) = x + 1$, ar kura palīdzību var aprakstīt visas Hasses grafa šķautnes kopā $\mathbb{N}$.

Strukturālajā indukcijā soļu skaitu var minimizēt, nodrošinot tikai to, lai līdz katram parametru kopas elementam var nokļūt no kāda minimāla elementa izmantojot tikai pierādītos soļus.

Strukturālās indukcijas ideju izmanto arī *rekursīvajās definīcijās:*

- no sākuma definē kādu matemātisku jēdzienu vai objektu daļēji sakārtotas kopas minimālajiem elementiem,
- pēc tam katram elementu pārim (x, y), kuram eksistē šķautne Hasses grafā, parāda, kā definēt šo jēdzienu elementam y, ja tas ir definēts elementam x.