Математички доказ

Професор: Рака Јовановић

Асистент: Јелена Јовановић

Доказ контрадикцијом

- Код оваквих доказа најчешће се тежи да се проблем представи у следећем облику

$$C = \neg A \wedge A$$

- У случају доказивања, да не постоји рационалан број чији је квадрат једнак 2

$$\neg((\exists x \in \mathbb{Q})(x^2 = 2))$$

- У овом случају смо рекли да је $x = \frac{p}{q}$
- А логички исказ је био

A = p и q су узајамно прости

- Скуп S, који је скуп свих простих бројева је бесконачан

  p – S је скуп простих бројева

  q – S је бесконачан

$$p \Rightarrow q$$

- Негација тврђења је

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

- Постоји коначан број простих бројева

- Претпоставимо да је негативно тврђење тачно односно да је

$$S = \{p_1, p_2, p_3, \ldots, p_n\}$$

- Број $N = p_1p_2p_3...p_n$ је очигледно дељив са свим $p_1, p_2, p_3, ..., p_n$
- Дакле број $N+1$ није дељив ни са једним простим бројем јер ће за сваки дати остатак 1

$$N + 1 = p_1p_2p_3...p_n + 1$$

- Дакле $N+1$, се не може се представити у облику производа простих бројева
- Фундаментална теорема аритметике

  Сваки број већи од један се може представити као производ простих бројева или је прост

- Контрадикција $N+1$ је број није прост, а опет се не може представити као производ простих

Важна особина импликације

$$P \Rightarrow Q \;\Leftrightarrow\; \neg Q \Rightarrow \neg P$$

P	Q	$\sim Q$	$\sim P$	$P \Rightarrow Q$	$\sim Q \Rightarrow \sim P$
T	T	F	F	**T**	**T**
T	F	T	F	**F**	**F**
F	T	F	T	**T**	**T**
F	F	T	T	**T**	**T**

Ако P , онда важи Q $\Leftrightarrow$ Ако $\neg$Q , онда важи $\neg$P

Доказ контрапозицијом (индиректни доказ)

- Некад је тешко доказати директну импликацију

$$(\forall x)P(x) \Longrightarrow Q(x)$$

- Али је много лакше

$$(\forall x)\neg Q(x) \Longrightarrow \neg P(x)$$

- Пример:
- Доказати да ако је n целобројан број и 3n+2 је непаран, тада је и n непаран

Директни доказ

- P(n) – 3n+2 је непаран
- Q(n) – n је непаран
- Покушајмо прво директан доказ
  $(\forall n \quad \in \mathbb{Z})P(n) \Longrightarrow Q(n)$
- Претпоставимо да важи P, односно да постоји k

$$3n + 2 = 2k + 1 \iff 3n + 1 = 2k$$

- Овакав пут не делује лако јер треба још ствари да се доказује

Доказ контрапозицијом

- ¬P(n) – 3n+2 је паран
- ¬Q(n)– n је паран
- Покушајмо да докажемо контрапозицију

$$(\forall n \quad \in \mathbb{Z})\neg Q(n) \Longrightarrow \neg P(n)$$

- Односно,
- Доказати да ако је n целобројан број и n је паран, тада је и 3n+2 паран
- Претпоставимо да важи $\neg Q(n)$,

$$n = 2k \Longrightarrow 3n + 2 = 3 \cdot 2k + 2 \Longleftrightarrow 2(3nk + 1)$$

- Доказ је готов на врло једноставан начин

Још један пример

- Доказати да ако је $n = ab$, тада за позитивне целе бројеве важи $\mathrm{a} \leq \sqrt{n}$ или $b \leq \sqrt{n}$

$$P - n = ab$$

$$Q - \mathrm{a} \leq \sqrt{n} \vee b \leq \sqrt{n}$$

- Пошто не постоји очигледан директини доказ пробајмо доказати контрапозицију

$$\neg Q \Longrightarrow \neg P \Leftrightarrow$$

$$(\mathrm{a} > \sqrt{n}\,) \wedge (b > \sqrt{n}) \Longrightarrow n \neq ab$$

- Покушајмо сад

$$ab > \sqrt{n} \cdot \sqrt{n} \Leftrightarrow ab > n \Longrightarrow n \neq ab$$

- Тврђење је доказано

Тривијалан и безизражајан доказ

- Када се доказује неко тврђење облика
- $(\forall x)P(x) \Longrightarrow Q(x)$
- Довољно је доказати
- $(\forall x)P(x) = \perp$ (безизражајан доказ)
- или $(\forall x)Q(x) = \top$ (тривијалан доказ)
- Овакви случајеви се не појављују пречесто али увек се треба сетити да је ово валидан доказ

Докази у којима се појављује еквиваленције

- Уместо доказивања $P \Leftrightarrow Q$, можемо доказати $P \Rightarrow Q \wedge Q \Rightarrow P$

$$(P \Leftrightarrow Q) \Leftrightarrow [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$$

- У случају да треба да докажемо већи број еквиваленција

$$P_1 \Leftrightarrow P_2 \Leftrightarrow P_3 \Leftrightarrow \cdots \Leftrightarrow P_n$$

- Обично је лакше доказати

$$(P_1 \Longrightarrow P_2) \wedge (P_2 \Longrightarrow P_3) \wedge \ldots \wedge (P_{n-1} \Longrightarrow P_n) \wedge (P_n \Longrightarrow P_1)$$

- Редослед импликација се може изабрати произвољним само да је затворен

- Докажимо да су за целобројан n, следећа тврђења еквивалентна

$$P_1 - \ \mathrm{n} \text{ је паран број}$$

$$P_2 - (\mathrm{n} - 1) \text{ је непаран број}$$

$$P_3 - \ n^2 \text{ је паран број}$$

- $P_1 \Rightarrow P_2$:

$$n = 2k \Leftrightarrow n - 1 = 2k - 1 \Leftrightarrow 2(k-1) + 1$$

- $P_2 \Rightarrow P_3$:

$$n - 1 = 2k + 1 \Leftrightarrow n^2 = (2k + 1 + 1)^2 = \big(2(k+1)\big)^2 = 2 \cdot 2(k+1)^2$$

- $P_3 \Rightarrow P_1$: Доказано на прошлом предавању

Конструктивни математички доказ

- Најчешће се користи у проблемима где се појављује егзистенцијални квантификатор
- Некада је најлакше доказати одређено математичко тврђење, конструкцијом одговарајућег примера
- Често се даје и генералан метод констукције одговарајућег примера
- Пример:
- Доказати да постоје ирационални бројеви a, b такви да је a^b рационалан број

Не конструктивни доказ

- Познато је да је $\sqrt{2}$ ирационалан број
- Рецимо да је

$$q = \sqrt{2}^{\sqrt{2}}$$

- Ако је q рационалан број, тврђење је доказано

$$\mathrm{a} = \sqrt{2}, b = \sqrt{2}$$

- Ако је q ирационалан

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}*\sqrt{2})} = \sqrt{2}^{2} = 2$$

- Тврђење је доказано

$$a = \sqrt{2}^{\sqrt{2}}, \mathrm{b} = \sqrt{2}$$

Конструктивни доказ

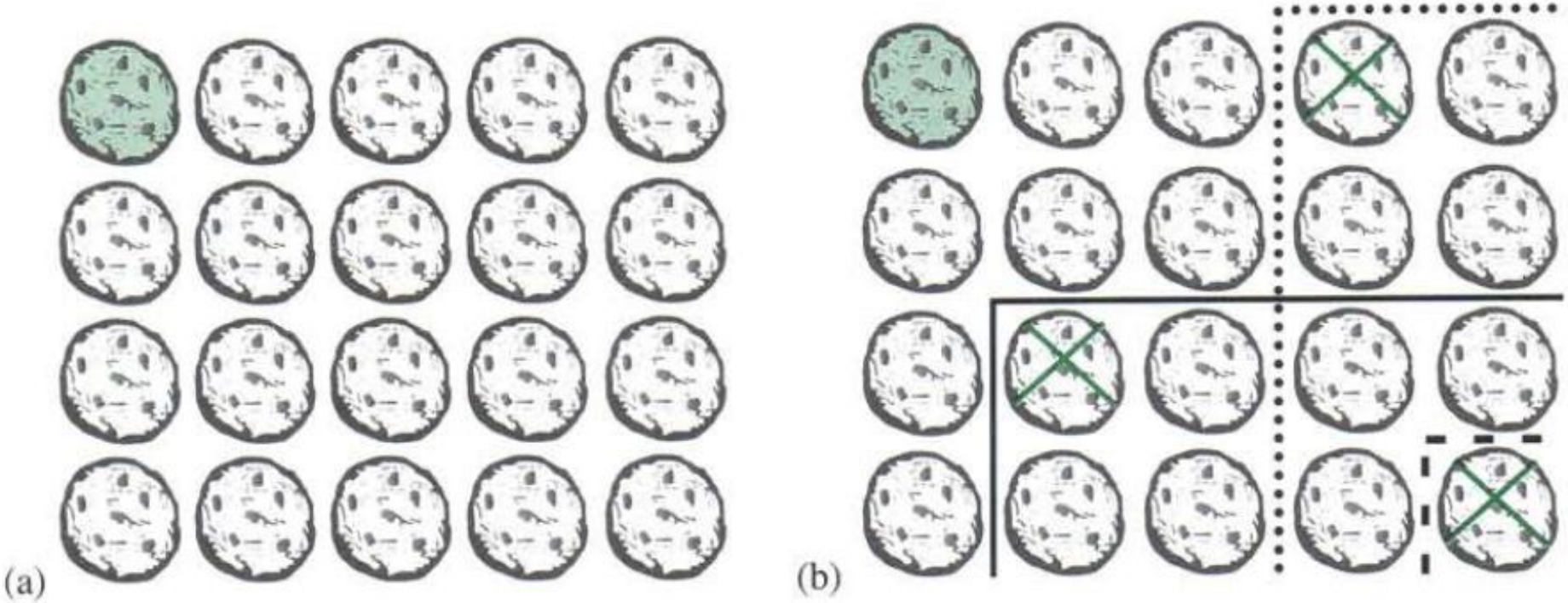
$$\mathrm{a} = \sqrt{2}, \qquad \mathrm{b} = \log_2 9, \qquad a^b = 3$$

- Јасно је да је $\sqrt{2}$ ирационалан, а 3 рационалан број
- $\log_2 9$ је такође ирационалан јер ако би могао да се представи у облику $\frac{m}{n}$, имали би да је

$$9^n = \left(2^{log_2 9}\right)^n = \left(2^{\frac{m}{n}}\right)^n = 2^m$$

- Односно да је 9^n паран број шта је не могуће

- **Игра чомп**: У игри учествују два играча. На табли је постављено n x m колача од којих је онај у горњем левом углу отрован. Играчи један за другим , бирају појединачно колачић и морају да поједу све који се налазе испод и десно од њега.
- Доказати да постоји победничка стратегија за првог играча



Конструктивни доказ није увек најлакши

- Игра сигурно има победника јер укупно има nm колачића тако да ће након највише толико корака неко морати да поједе отровни колачић
- Нека први играч у првом кораку поједе колачић колачић у доњем десном углу
- Ово је или први корак победничке стратегије у ком случају је доказано тврђење
- Ако није
- Онда први корак другог играча доноси победу.
- Ако први играч уместо доњег десног колача поједе први онај колач који је изабрао други играч онда побеђује
- Значи доказано је да постоји победничка стратегија, али се не зна која

Доказ контрапримером

- Користи се за оповргавање тврђење у којима се појављује универзални квантификатор
- Конструише се један контрапример, и почетно тврђење је доказано
- Треба доказати

  Сви студенти су лењи
- Довољно је наћи једног вредног студента и тврђење је оповргнуто
- Сви прости бројеви су непарни
  - 2 је контрапример јер је прост број и паран је
  - 7, 10 нису контра примери
- Сетите се негације предикатског рачуна

- Оповргнути следеће тврђење

Ако је аритметички производ две функције f, g нула функција тада је бар једна од њих мора бити нула функција

- Нула функција

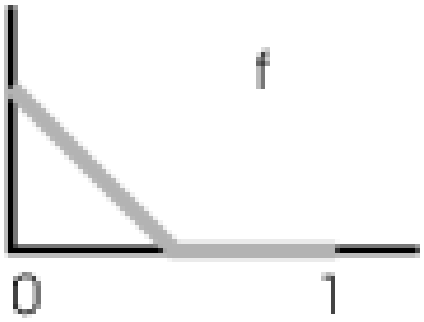
$$(\forall x)0(x) = 0$$

- Аритметички производ функција

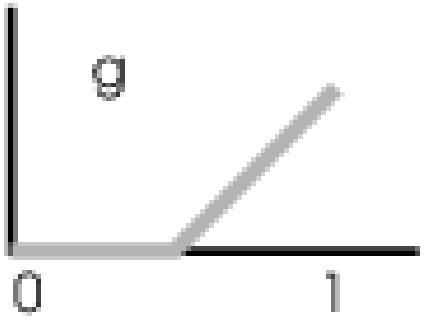
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

- Покушајмо да констуишемо контра пример

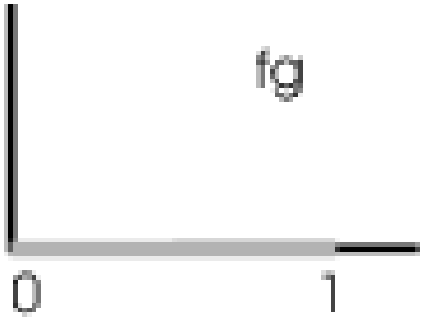
$$f(x) = \begin{cases} \frac{1}{2} - x & \text{if } 0 \le x \le \frac{1}{2} \\ 0 & \text{if } \frac{1}{2} < x \le 1 \end{cases}$$



$$g(x) = \begin{cases} 0 & \text{if } 0 \le x \le \frac{1}{2} \\ x - \frac{1}{2} & \text{if } \frac{1}{2} < x \le 1 \end{cases}.$$



Јасно је да функције f и g оповргавају почетно тврђење
Обе су различите од нула функције а њих производ је једнак нула функцији



Доказ јединствености

- Често је потребно доказати исказ облика
- Постоји јединствено x које задовољава услов P(x)
- Доказ се састоји из два дела
  - Доказати да постоји x које испуњава услов P(x)
  - Доказати да ако је $y \neq x$ онда није испуњен услов P(y)

$$\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$$

- Нека су a, b реални бројеви и нека је a≠0. Тада постоји јединствен реални број r за који важи

$$\mathrm{a}r + b = 0$$

- Доказ:
- Решење дате једначине је $r = -\frac{b}{a}$,

$$\mathrm{a}\left(-\frac{b}{a}\right) + b = -b + b = 0$$

- односно постоји r које задовољава услов

- Претпоставимо да постоји још неко s за које важи

$$\mathrm{a}s + b = 0$$

- Докажимо да је оно једнако r

$$\mathrm{a}s + b = \mathrm{a}r + b \Leftrightarrow as = ar \Leftrightarrow s = r$$

- Шта заправо значи да

$$s \neq r \Rightarrow \mathrm{a}s + b \neq 0$$

- Доказано је жељено тврђење

Доказ исцрпљивањем

- Често се зове и доказ по случајевима, или доказ бруталном силом
- Почетно тврђење је могуће поделити на случајеве
- Постоје два корака
  - Доказати да изабрани случајеви покривају све могуће ситуације
  - Доказати да је сваки од случајева задовољен

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

- Куб било ког природног броја n је или дељив са 9, или је има остатак 1 или -1 при дељењу са 9
- Случај 1:

$$n = 3p \Leftrightarrow n^3 = (3p)^3 = 27p^3$$

- Случај 2:

$$n = 3p + 1 \Leftrightarrow n^3 = (3p + 1)^3$$
$$= 27p^3 + 27p^3 + 9p + 1$$

- Случај 3:

$$n = 3p - 1 \Leftrightarrow n^3 = (3p - 1)^3$$
$$= 27p^3 - 27p^2 + 9p - 1$$

Смерови доказивања

- Доказивање у напред. Креће се од премиса, аксиома, теорема и полако се израз преводи у жељени закључак
- Доказивање у назад. Крећемо од закључка и опет на основу познатих теорема и аксиома долазимо до премиса

- Доказати да је аритметичка средина ($\frac{x+y}{2}$) два различита позитивна броја увек већа од њихове геометријске средине ($\sqrt{xy}$)

- Кренимо од закључка и дођимо до нечег тачног

$$(x+y)/2 > \sqrt{xy},$$
$$(x+y)^2/4 > xy,$$
$$(x+y)^2 > 4xy,$$

- Сада можемо доказ написати у супротном смеру

$$x^2 + 2xy + y^2 > 4xy,$$
$$x^2 - 2xy + y^2 > 0,$$
$$(x-y)^2 > 0.$$

Постоји велик број правила који се могу користити приликом доказивања

	Rule of Inference	Related Logical Implication	Name of Rule
1)	p $p \to q$ $\therefore q$	$[p \wedge (p \to q)] \to q$	Rule of Detachment (Modus Ponens)
2)	$p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Law of the Syllogism
3)	$p \to q$ $\neg q$ $\therefore \neg p$	$[(p \to q) \wedge \neg q] \to \neg p$	Modus Tollens
4)	p q $\therefore p \wedge q$		Rule of Conjunction
5)	$p \vee q$ $\neg p$ $\therefore q$	$[(p \vee q) \wedge \neg p] \to q$	Rule of Disjunctive Syllogism
6)	$\neg p \to F_0$ $\therefore p$	$(\neg p \to F_0) \to p$	Rule of Contradiction
7)	$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Rule of Conjunctive Simplification
8)	p $\therefore p \vee q$	$p \to p \vee q$	Rule of Disjunctive Amplification
9)	$p \wedge q$ $p \to (q \to r)$ $\therefore r$	$[(p \wedge q) \wedge [p \to (q \to r)]] \to r$	Rule of Conditional Proof
10)	$p \to r$ $q \to r$ $\therefore (p \vee q) \to r$	$[(p \to r) \wedge (q \to r)] \to [(p \vee q) \to r]$	Rule for Proof by Cases
11)	$p \to q$ $r \to s$ $p \vee r$ $\therefore q \vee s$	$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to (q \vee s)$	Rule of the Constructive Dilemma
12)	$p \to q$ $r \to s$ $\neg q \vee \neg s$ $\therefore \neg p \vee \neg r$	$[(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s)] \to (\neg p \vee \neg r)$	Rule of the Destructive Dilemma

Стандардне грешке приликом доказивања

Доказати да је 1=2

“Доказ”:

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Сви кораци су исправни осим корака 5, једна грешка и докаже се глупост

- Доказати: Ако је $n^2 > 0$, тада је и $n > 0$
- “Доказ”:

Претпоставимо да је $n^2 > 0$. Пошто знамо да

$$n > 0 \Longrightarrow n^2 > 0$$

- Значи, јасно је да је $n > 0$

- **<u>Грешка</u>** је следећа

$$\text{P(n) - } n^2 > 0$$

$$\text{Q(n) - } n > 0$$

- Требало је доказати

$$(\forall n)P(n) \Longrightarrow Q(x)$$

- А доказано је

$$(\forall n)Q(n) \Longrightarrow P(x)$$

- Доказати:

Ако n није позитивно, онда није позитивно ни n^2

- “Доказ”:

Познато је да важи

$$(\forall n)(n > 0 \Longrightarrow n^2 > 0)$$

Пошто је $n < 0$ можемо закључити да n^2 није позитивно

- **<u>Грешка</u>** је што се не може из

$$(\forall n)\big(P(n) \Longrightarrow Q(n)\big)$$

- Закључити

$$(\forall n)\big(\neg P(n) \Longrightarrow \neg Q(n)\big)$$

- Доказати:
- Ако квадрат сваког целог броја је већи од 0

$$(\forall x \in \mathbb{R})(x^2 > 0)$$

- “Доказ”:

Докажимо по случајевима

x<0

- Производ два позитивна броја је позитиван

x>0

- Производ два негативна броја је негативан

Значи тврђење је доказано јер у свим случајевима важи

- **<u>Грешка</u>** је у томе што је заборављен случај x=0