

Diskrétní matematika a logika

Zápisy přednášek ~~1-12~~ 1-14

ZS 2004/05

KOMPLETNÍ VERZE

Obsahuje vše, co bylo napsáno na tabuli kromě některých obrázků, které se mi kvůli proseté lenosti nechtělo kreslit.

Autor nenese odpovědnost za chyby, jakékoliv symboly na ně poznámky budou při zkoušce pravděpodobně ignorovány.

bulemp1@fel.cvut.cz
atlas.cz

Výroková logika

výrok

A.. množina elementárních výroků
— " — logických proměnných

logické spojky:

unární	- negace $\neg$	není pravda, že...
binární	- a, konjunkce $\wedge$ (&)	... a ...
	- disjunktce $\vee$	... nebo ...
	- implikace $\Rightarrow$ ($\rightarrow$)	jestliže ..., pak ...
	- ekvivalence $\Leftrightarrow$ ($\leftrightarrow$)	... právě tehdy, když ...

formule výrokové logiky

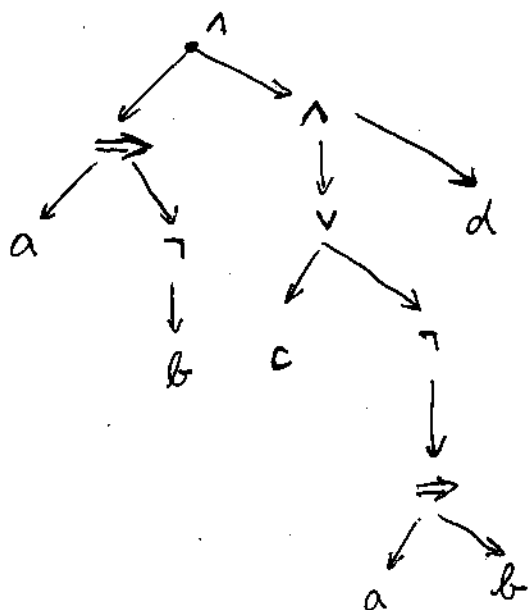
Řetězec (konečná posloupnost) logických proměnných, log. spojky a závorek je formulí výrokové logiky, jestliže vznikla podle těchto pravidel:

- 1) Každá logická proměnná je formule.
- 2) jsou-li α, β formule, je $(\neg \alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ také formule.

Př. $a \vee b \Rightarrow c$ není formule - nepou závorek
 $((a \vee b) \Rightarrow c)$ $(a \vee (b \Rightarrow c))$ jsou formule
 $\neg a \vee b$ rozumíme jako $(\neg a) \vee b$

Derivační strom formule

$$(a \Rightarrow \neg b) \wedge ((c \vee \neg(a \Rightarrow b)) \wedge d)$$



podformule je formule odpovídající podstromu

Pravdivostní hodnota

0... nepravda 1... pravda

pravdivostní ohodnocení je zobrazení n , které každé formulě přiřazuje 0, nebo 1 a splňuje:

1) $\neg \alpha$ je pravdivá iff α nepravdivá

α	$\neg \alpha$
0	1
1	0

2) $\alpha \wedge \beta$ je pravdivá iff α, β jsou pravdivé

3) $\alpha \vee \beta$ je nepravdivá iff α, β nepravdivé

4) $\alpha \Rightarrow \beta$ je nepravdivá iff α pravdivé, β nepravdivé

5) $\alpha \Leftrightarrow \beta$ je pravdivá iff α, β jsou buď pravdivé, nebo obě nepravdivé

α	β	$\alpha \wedge \beta$	$\alpha \vee \beta$	$\alpha \Rightarrow \beta$	$\alpha \Leftrightarrow \beta$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

$\alpha \Rightarrow \beta$ α je postačující podmínka pro β ,
 β je nutná podmínka pro α

Jestliže ve formuli α známe pravdivostní hodnotu všech log. proměnných, ~~pak~~ tak je pravdivostní hodnota α určena jednoznačně

Platí: Jestliže dvě pravdivostní ohodnocení se shodují na všech logických proměnných, tak jsou stejné.

2^n je počet různých pravdivostních ohodnocení formule s n log. proměnnými

Sautologie je formule pravdivá ve všech ohodnoceních $\alpha \vee \neg \alpha$
 $\alpha \Rightarrow \alpha$

Kontradikce — " — nepravdivá — " — $\alpha \wedge \neg \alpha$

Splnitelná formule je formule pravdivá v alespoň 1 ohodnocení $\alpha \vee \beta$

Def: Formule α a β jsou sautologicky ekvivalentní $\Leftrightarrow$ mají stejnou hodnotu v každém pravdivostním ohodnocení
 $\alpha \models \beta \quad (\alpha \equiv \beta)$

Platí: $\alpha \models \beta$ $\Leftrightarrow$ $\alpha \Rightarrow \beta$ je sautologie

Pro každé formule α, β, γ platí:

$$1) \alpha \wedge \alpha \models \alpha \quad \alpha \vee \alpha \models \alpha$$

$$2) \alpha \wedge \beta \models \beta \wedge \alpha \quad \alpha \vee \beta \models \beta \vee \alpha$$

$$3) \alpha \wedge (\beta \wedge \gamma) \models (\alpha \wedge \beta) \wedge \gamma \quad \alpha \vee (\beta \vee \gamma) \models (\alpha \vee \beta) \vee \gamma$$

$$4) \alpha \wedge (\beta \vee \alpha) \models \alpha \quad \alpha \vee (\beta \wedge \alpha) \models \alpha$$

$$5) \alpha \wedge (\beta \vee \gamma) \models (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \quad \alpha \vee (\beta \wedge \gamma) \models (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$$

$$6) \alpha \Rightarrow \beta \models \neg \alpha \vee \beta \quad \neg(\alpha \Rightarrow \beta) \models \alpha \wedge \neg \beta$$

$$7) \alpha \Rightarrow \beta \models (\neg \beta \Rightarrow \neg \alpha)$$

$$8) \neg(\alpha \wedge \beta) \models \neg \alpha \vee \neg \beta \quad \neg(\alpha \vee \beta) \models \neg \alpha \wedge \neg \beta$$

$$9) \neg \neg \alpha \models \alpha$$

T... libovolná tautologie, F... libovolná kontradikce

$$9) T \wedge \alpha \models \alpha \quad T \vee \alpha \models T \quad F \wedge \alpha \models F \quad F \vee \alpha \models \alpha$$

literál... logická proměnná nebo negace log. proměnné ($a, \neg a, b, \dots$)

minterm... literál nebo konjunkce konečné mnoha literálů
 $\neg a, a \wedge \neg b, \neg(a \wedge b)$ není

maxterm... literál nebo disjunkce literálů (konečné mnoha)
 $\neg a, \neg a \vee b \vee c$

CNF... maxterm nebo konjunkce konečné mnoha maxtermů

DNF... minterm nebo disjunkce konečné mnoha mintermů

$$\text{CNF: } (a \vee b \vee \neg c) \wedge a$$

$$\text{DNF: } (a \wedge b) \vee (\neg a \wedge b \wedge c) \vee (c \wedge \neg f)$$

minterm $a \wedge \neg b \wedge c$ - bere se "minimum" - staťi jedro
 a je do 0

maxterm $a \vee \neg b \vee c$ - bere se "maximum"

$$\mu(a) = x \quad x, y \in \{0, 1\}$$

$$\mu(b) = y$$

	-
0	1
1	0

min	0	1
0	0	0
1	0	1

max	0	1
0	0	1
1	1	1

nejmenší
 Boolova
 algebra

Boolova algebra $(\{0, 1\}; \cdot, +, -)$

$$\mathcal{P}\{a\} = \{\emptyset, \{a\}\}$$

(2)

$\cap$	$\emptyset$	$\{a\}$
$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$

$\cup$	$\emptyset$	$\{a\}$
$\emptyset$	$\emptyset$	$\{a\}$
$\{a\}$	$\{a\}$	$\{a\}$

$$\overline{\emptyset} = \{a\}$$

$$\overline{\{a\}} = \emptyset$$

Formule

minterm
 $a \wedge \neg b \wedge c$

maxterm (klausule)

$$\neg a \vee b \vee c$$

Booleovský kalkul

$$a \cdot \bar{b} \cdot c$$

$$\bar{a} + b + c$$

$$f(x, y, z) : \{0, 1\}^3 \rightarrow \{0, 1\}$$

$$f(x, y, z) = x\bar{y} + \bar{y}z = \bar{y}(x+z)$$

DNF CNF
 (dis. norm. forma)

Věta: Ke každé formuli α existují formule β a γ tak,
že $\alpha \equiv \beta$, $\alpha \equiv \gamma$ a β je DNF (disjunktce ^{min} ~~max~~termů)
a γ je $\neg$ CNF (konjunktce maxtermů)

D: α má pravdivostní tabulku

$\overline{P\alpha}$	$x \ y \ z$	α	DNF	CNF
	0 0 0	0		$\neg(\neg x \wedge \neg y \wedge \neg z) \wedge$
	0 0 1	1	$(\neg x \wedge \neg y \wedge z) \vee$	
	0 1 0	0		$\neg(\neg x \wedge y \wedge \neg z) \wedge$
	0 1 1	1	$(\neg x \wedge y \wedge z) \vee$	
	1 0 0	1	$(x \wedge \neg y \wedge \neg z) \vee$	
	1 0 1	0		$\neg(x \wedge \neg y \wedge z) \wedge$
	1 1 0	1	$(x \wedge y \wedge \neg z) \vee$	
	1 1 1	1	$(x \wedge y \wedge z)$	

$= \beta$

pro každý řádek, ve kterém je 1, konstruuje se
minterm, který tento řádek popisuje
 β je disjunktce těchto získaných mintermů
- jestliže neexistuje řádek s hodnotou 1, je $\beta = x \wedge \neg x$
(nejatá kontradikce)

de Morgan

- každý řádek, ve kterém je 0 popíšeme
mintermem. Utvoříme formuli,
která je konjunktací negací těchto
mintermů. Použitím de Morganova
zákonu dostaneme ~~formuli~~ $\neg$ mintermů maxtermů,
 α tautologie $\gamma = x \vee \neg x$ formuli γ

$(x \vee y \vee z) \wedge$

$(x \vee \neg y \vee z) \wedge$

$(\neg x \vee y \vee \neg z) \dots \gamma$

Sémantický důsledek

(konsekvence, tautologický důsledek)

Pr. $\{a, a \Rightarrow b\}$ znamená, že b je pravdivé

$$\frac{a \quad a \Rightarrow b}{b}$$

Def. Máme množinu formulí S a formuli α . Řekneme, že α je sémantický důsledek množiny S , píšeme $S \models \alpha$, iff pro každé pravdivostní ohodnocení u takové, že v u je pravdivá ~~každá~~ $\varphi \in S$, je $u(\alpha) = 1$. (tj. α je také pravdivá v u)

"Kdykoliv je S pravdivá v u , je v u pravdivá i α ."

$S \not\models \alpha$ (α není sém. důsledek S) znamená, existuje ohodnocení u , ve kterém je pravdivá S a α nepravdivá.

S není pravdivá v u znamená, že existuje $\varphi \in S$, která je v u nepravdivá.

Píšeme $\emptyset \models \alpha$ místo $\{\emptyset\} \models \alpha$,
 $\models \alpha$ místo $\emptyset \models \alpha$

Plati 1) $\alpha \models \beta$ iff $\alpha \models \beta$ a $\beta \models \alpha$

2) $\alpha \models \beta$ iff $\alpha \Rightarrow \beta$ je tautologie

Věta o dedukci: Pro každou množinu formulí S
a formule α, β platí

$$S \models (\alpha \Rightarrow \beta) \text{ iff } S \cup \{\alpha\} \models \beta$$

Plati: 1) Je-li α tautologie, pak $S \models \alpha$ pro každou S .

2) Jestliže $\models \alpha$, pak α je tautologie
(neboť $\emptyset$ je pravdivá v každém ohodnocení)

3) Pro každou $\varphi \in S$ platí $S \models \varphi$.

4) Jestliže $S \models \beta_i, i=1, \dots, n$ a $\{\beta_1, \dots, \beta_n\} \models \alpha$,
pak $S \models \alpha$

5) Je-li $M \models S$ a $M \models \alpha$, pak $S \models \alpha$

6) $\{\beta, \neg \beta\} \models \alpha$ ^{pro} každou formuli α .

($\{\beta, \neg \beta\} \models \alpha$ znamená, že existuje μ tak, že $\{\beta, \neg \beta\}$
je pravdivé v μ a α je nepravdivé v μ
- nemůže nastat)

Def: Řekneme, že množina formulí S je nesplnitelná iff
pro každé ohodnocení μ existuje $\varphi \in S$ nepravdivá v μ .

6) Je-li S nesplnitelná, pak $S \models \alpha$ pro každou α

Př. $S = \{ \alpha, \beta \Rightarrow \alpha \} \not\models \beta$

Věta: Máme množinu formulí S a formuli α .

Pak $S \models \alpha$ iff $S \cup \{ \neg \alpha \}$ je nesplnitelná

Resoluční metoda

Př. $\varphi = a \vee \neg b \vee c$, $\psi = a \vee b \vee d \vee e$

Pak $\{ \varphi, \psi \} \models (a \vee c \vee d \vee e) = \alpha$

μ , ve kterém je pravdivá φ i ψ .

$\mu(b) < 1$, pak $\mu(\neg b) = 0$ pak $\mu(a \vee c) = 1$, tedy $(a \vee c \vee d \vee e) = 1$
 0 , pak $\mu(a \vee d \vee e) = 1$, tedy $(a \vee c \vee d \vee e) = 1$

využití v logickém programování

$a \Rightarrow b \models \neg a \vee b$

$(a \wedge b) \Rightarrow c \models \neg(a \wedge b) \vee c \models \neg a \vee \neg b \vee c$

(3)

Platí: $\{ \beta_1, \dots, \beta_n \} \models \alpha$ iff $(\beta_1 \wedge \beta_2 \wedge \dots \wedge \beta_n) \Rightarrow \alpha$ je tautologie

Př. Každý sportovec je vydrvalý.

Tomáš je sportovec

Tudíž Tomáš je vydrvalý

$a \Rightarrow b$

$\frac{c}{d}$

není správné
 důkaz se
 vydrvalý

potřebujeme k popisu - Predikátová logika (logika 1. řádu)

Každý, kdo je sportovec, má vlastnost být vydrvalý.

vlastnosti: být sportovec S
 být vydrvalý

Každý, kdo má S , má V

Každý, když má S, má V.

$$\forall x (S(x) \Rightarrow V(x))$$

proměnná individuální

t ... konstanta Tomáš

$$S(t)$$

$$V(t)$$

$$\forall x (S(x) \Rightarrow V(x))$$

$$S(t)$$

$$V(t)$$

S, V ... vlastnosti - predikáty

t ... konstanty

Domain = soubor, o kterém výroky vyprávějí
(Universum)

$\forall$... univerzální (velký) kvantifikátor

Př. Tomáš je sportovec

Tomáš je vytrvalý

Tedy někdo je sportovec a vytrvalý $\exists x (S(x) \wedge V(x))$

$$S(t)$$

$$V(t)$$

$$\exists x (S(x) \wedge V(x))$$

$\exists$... existenciální (malý) kvantifikátor

Pr Následník libovolného sudého čísla je liché číslo.
 Číslo 2 je sudé.
 Následník čísla 2 je lichý.

$D = \mathbb{N}$ (přirozená čísla) Duvce, jako x
 predikáty (vlastnosti) $S(x)$... x je sudé
 $L(x)$... x je liché

funkční symbol $f: x \mapsto x+1$
 konstanta $a/2$

$$\forall x (S(x) \Rightarrow L(f(x)))$$

$$S(a)$$

$$L(f(a))$$

Pr 1. Pro každé reálné číslo existuje větší číslo.
 2. Existuje největší reálné číslo.

$$D = \mathbb{R}$$

predikát $Q\left(\overset{x}{-}, \overset{y}{-}\right)$ — je větší než min.

$$1. \quad \forall x \exists y Q(y, x)$$

($y > x$)

$$2. \quad \exists y \forall x Q(y, x)$$

$y > x$

Jazyk predikátové logiky se skládá z

- speciálních symbolů:

- predikátové symboly: $P, Q, R, S, \dots$, spolu s aritou (četností)
pred. symb.

- funkční symboly: $f, g, h, \dots$, ----- " ----- "
funkčního symbolu

- konstantní symboly: $a, b, c, \dots$

- logické symboly

- množinové proměnných: $x, y, z, x_1, x_2, \dots$

- logické spojky: $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$

- kvantifikátory: $\forall, \exists$

- pomocné symboly: $, [] () \{ \}$

Term: 1. Každá proměnná a každá konstanta je term.

2. Je-li f funkční symbol arity n a $t_1, \dots, t_n$ jsou
termy, pak $f(t_1, \dots, t_n)$ je term.

Atomická formule: Je-li P predikátový symbol arity n
a $t_1, \dots, t_n$ jsou termy, pak $P(t_1, \dots, t_n)$ je atomická formule.

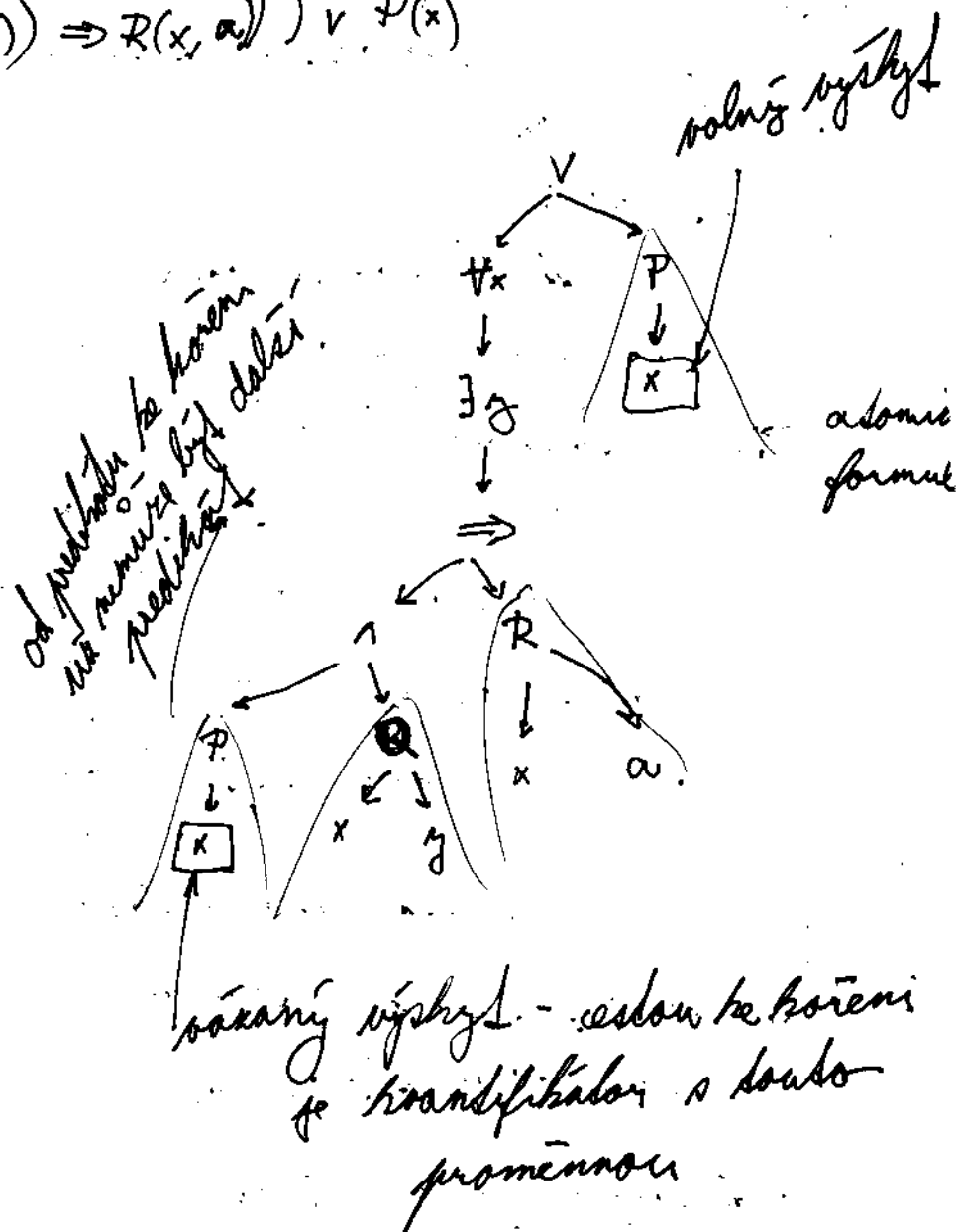
Formule: 1. Každá atomická formule je formule.

2. Když α, β jsou formule, pak $\neg \alpha, (\alpha \wedge \beta), (\alpha \vee \beta),$
 $(\alpha \Rightarrow \beta), (\alpha \Leftrightarrow \beta)$ jsou formule.

3. Když α je formule, x je proměnná, pak
 $(\forall x \alpha), (\exists x \alpha)$ jsou formule.

Derivační strom formule

$$(\forall x \exists y ((P(x) \wedge Q(x, y)) \Rightarrow R(x, a))) \vee P(x)$$



Sentence (uzavřená formule) je formule, která nemá volné výskyty proměnné.

Dvě formule jsou stejně, liší-li se pouze ve jménu vázané proměnné
např. $\forall x P(x) = \forall y P(y)$

$$\mathcal{P}_A \quad \forall x (S(x) \Rightarrow S(f(f(x))))$$

(I) D lidé

predikát $S(x)$ | x je naživu

funkční symbol $f(x)$ | otec x

- každý, kdo je naživu, je jeho dědeček
z obou strany naživu

(II) $D = \mathbb{N}$

$S(x)$ | x je sudé

$f(x)$ | je následník $x+1$

následník následníka sudého č. je sudé č.

existuje tato interpretace

Interpretace se skládá z:

- neprázdné množiny D
- pro každý predikátový symbol P je dána relace na P podle arity P ; je-li P unární, pak podmnožina D
 P binární, pak podmnožina D^2
- pro každý funkční symbol dána f z $D^n \rightarrow D$, kde n je arity
- pro každý konst. symbol prvek D

Káždá sentence je v interpretaci pravdivá, nebo nepravdivá.

Atomická formule $P(t_1, \dots, t_n)$ je pravdivá v interpretaci, jestliže $(a_1, \dots, a_n) \in D^n$, kde a_i je význam ~~termu~~ termu t_i , má vlastnost odpovídající P .

Platí $\neg x$ je pravdivá iff x je nepravdivá.

$\forall x \alpha(x)$ je pravdivé (v interpretaci) iff pro každé dosazení
za x prvku D dostaneme pravdivou formuli.

$\exists x \alpha(x)$ je pravdivá (v interp.) iff existuje aspoň jedno
dosazení za x prvku D takové, že dostaneme
pravdivou formuli.

Def: Interpretace, ve které je sentence φ pravdivá,
se nazývá model φ

Tautologie je sentence pravdivá v každé interpretaci.

Kontradikce je sentence, která nemá model.

Splnitelná sentence je sentence, která má model.

Model množiny sentencí S je každá interpretace,
ve které je pravdivá každá sentence $s \in S$.

Př. 1) $S = \{ \forall x (P(x) \vee Q(x)), \neg P(a), \exists x \neg Q(x) \}$
ano, má model.

$D = N$

predikáty

$P(x)$

x je sudé

$Q(x)$

x je ~~liché~~ liché

$a = 3$

$$2) \quad T = \{ \forall x (P(x) \vee Q(x)), \neg P(a), \neg \exists x Q(x) \}$$

nená model

Def: Řekneme, že dvě sentence φ a ψ jsou tautologicky ekvivalentní, píšeme $\varphi \models \psi$, iff mají stejné modely.

Pr. 1) $\forall x \forall y Q(x, y) \models \forall y \forall x Q(x, y)$

2) $\exists x \exists y Q(x, y) \models \exists y \exists x Q(x, y)$

3) $\neg \forall x P(x) \models \exists x \neg P(x)$

4) $\neg \exists x P(x) \models \forall x \neg P(x)$

5) $(\forall x P(x)) \wedge (\forall x Q(x)) \models \forall x (P(x) \wedge Q(x))$

6) $(\exists x P(x)) \vee (\exists x Q(x)) \models \exists x (P(x) \vee Q(x))$

Ala! $(\forall x P(x)) \vee (\forall x Q(x)) \not\models \forall x (P(x) \vee Q(x))$

$(\forall x P(x)) \vee (\forall x \neg P(x)) \not\models \forall x (P(x) \vee \neg P(x))$

není tautologie

tautologie

7) $(\forall x P(x)) \vee (\forall y Q(y)) \models \forall x \forall y (P(x) \vee Q(y))$

ještě pravda!

8) $(\exists x P(x)) \wedge (\exists y Q(y)) \models \exists x \exists y (P(x) \wedge Q(y))$

Def: Māme mnozīmu sentenci S a sentenci φ . Ņemam, ka φ ir konsekvents S , ņemam $S \models \varphi$, patērē šādi, ka S ir modelem φ .

Plati: $\varphi \models \psi$ iff $\varphi \models \psi$, $\psi \models \varphi$

Pā: 1) $(\forall x P(x)) \vee (\forall x Q(x)) \models \forall x (P(x) \vee Q(x))$

2) $\exists x \forall y Q(x, y) \models \forall y \exists x Q(x, y)$

Vēl: $S \models \varphi$ iff $S \cup \{\neg \varphi\}$ nēma model

Matemātiskā indukcija

Pā: Bubble sort

Vstus: $s[1], s[2], \dots, s[n]$

Vstus: sērašenē neklerajām xpiroben

$i := 1$

while $i \leq n$ do $j := 1$

while $j \leq n-1$ do

if $s[j] > s[j+1]$ then prohod $s[j]$

$j := j+1$

end

end

* Indukcí dokážeme následující tvrzení:

Jestliže byl vnitřní cyklus proveden k -krát,
pak posledních k členů je největších a
správně uspořádaných, tj. $s[m-k+1], \dots, s[m-1], s[m]$
je větší nebo rovno $s[i]$, $i \leq m-k$
a $s[m-k+1] \leq s[m-k+2] \leq \dots \leq s[m-1] \leq s[m]$

1) $k=0$ není co dokazovat

2) předpokládáme, že tvrzení platí pro k

Pak po přechodu vnitřním cyklem $s[m-k] \geq s[i]$
pro vs. $i \leq m-k-1$

a křejně $s[m-k] \leq s[m-k+1] \leq \dots \leq s[m]$

Pr. Odvodě vzorec pro $\sum_{i=1}^n i^2 = \frac{\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n}{= \frac{1}{6}n(2n^2 + 3n + 1)}$

Předpoklad $\sum_{i=1}^n i^2 = an^3 + bn^2 + cn + d$

1) $n=1$ $1^2 = a + b + c + d$

2) indukční krok

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^n i^2 + (n+1)^2$$

$$a(n+1)^3 + b(n+1)^2 + c(n+1) + d = an^3 + bn^2 + cn + d + (n+1)^2$$

$$3an^2 + 3an + a + 2bn + b + c = n^2 + 2n + 1$$

$$n^2: \quad 3a = 1, \quad a = \frac{1}{3}$$

$$n^1: \quad 3a + 2b = 2 \quad 2b = 1 \quad b = \frac{1}{2}$$

$$n^0: \quad a + b + c = 1 \quad c = \frac{1}{6} \quad d = 0$$

Princip (slabé) matematické indukce

Máme vlastnost V přirozených čísel.

Jestliže platí následující podmínky:

1) n_0 má vlastnost V

2) jestliže $n, n \geq n_0$ má vlastnost V ,
pak V má i $n+1$

Pak každé $n \geq n_0$ má vlastnost V .

Př. Každé přiroz. číslo větší než 1 lze napsat
ve tvaru součinu prvočísel.

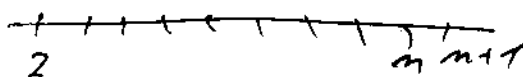
Indukcí:

1) $n=2$

$$2 = 2^1$$

2) $n+1$ — je buď prvočíslo $(n+1) = (n+1)^1$

nebo je složené $n+1 = p \cdot q, p \cdot q < n+1$



2*, jestliže každé $h, n_0 \leq h < n+1$ má V ,
má ji i $n+1$.

Princíp silnej mat. indukcie.

→

2*) jestliže všechna k , $m_0 \leq k < m+1$ mají vlastnost V , pak V má i $m+1$

Princíp dobrého usporiadání:

Každá neprázdna podmnožina N má nejmenší prvok.

Princíp dobrého usporiadání je ekvivalentný s oboma princípy matematickej indukcie.

Pr Ukážte, že $11^n - 6$ je deliteľné 5 pre každé $n \geq 1$

Res: 1) $n=1$ $11-6=5$ je deliteľné 5.

2) predpokladáme, že $11^n - 6 = 5 \cdot k \rightarrow 11^n = 5k + 6$

$$\begin{aligned} 11^{n+1} - 6 &= 11(5k + 6) - 6 = 55k + 66 - 6 = \\ &= 55k + 60 = 5(11k + 12) \end{aligned}$$

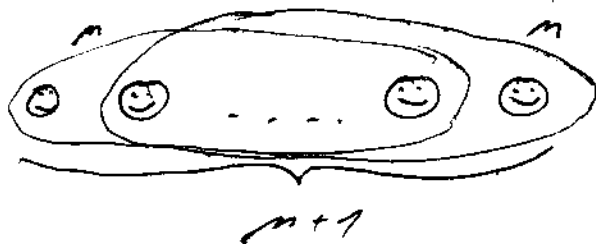
Př

Kšichni máme stejnou barvu očí.

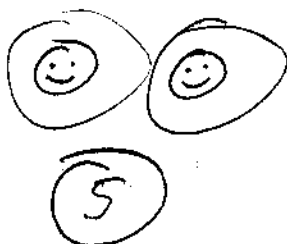
1) $n=1$

ano

2)



nežde při přechodu od $n=1$ k $n=2$
- příkaz je prádný



Množiny radané indukčně

Př Množina S binárních slov je dána následovně:

1) prádné slovo ϵ patří do S

2) a) jestliže slovo w patří do S , pak $0w1$, $1w0$ patří do S

b) jsou-li $u, v \in S$, pak $uv \in S$

$$\begin{array}{cc} \epsilon & \\ \hline 0w1 & 1w0 \\ \hline u & v \\ \hline uv & \end{array}$$

S leží např.: $1010, \dots$

S neleží např.: $1, 11, \dots$

Ukážeme, že každé slovo $w \in S$ splňuje:
obsahuje stejný počet 0 a 1.

označme $w_{(0)}$: počet výskytů 0 ve slově w

$w_{(1)}$ — 11 — 1 — 11 —

Pro každé $w \in S$ je $w_{(0)} = w_{(1)}$

D.: 1) $\epsilon_{(0)} = 0$ $\epsilon_{(1)} = 0$ tedy $\epsilon_{(0)} = \epsilon_{(1)}$

2) a) jestliže $w_{(0)} = w_{(1)}$, pak $(0w1)_{(0)} = 1 + w_{(0)}$, $(0w1)_{(1)} = 1 + w_{(1)}$

Tedy $(0w1)_{(0)} = (0w1)_{(1)}$

b) jestliže $\mu_{(0)} = \mu_{(1)}$, $\nu_{(0)} = \nu_{(1)}$, pak

$$(\mu\nu)_{(0)} = \underline{\mu_{(0)}} + \underline{\nu_{(0)}}, \quad (\mu\nu)_{(1)} = \underline{\mu_{(1)}} + \underline{\nu_{(1)}}$$

$$\text{tj. } (\mu\nu)_{(0)} = (\mu\nu)_{(1)}$$

Strukturní indukce:

Množina S je dána indukčně

Ukážeme-li, že

- 1) každý prvek $x \in S$ základního pravidla má vlastnost V
- 2) Pro každé indukční pravidlo platí:
jestliže předpoklad pravidla má V ,
pak i závěr pravidla má V .

Pak každý prvek S má V .

Př. $\{0,1\}^*$ je množina všech binárních slov

$$1) \varepsilon \in \{0,1\}^*$$

$$2) \text{ jestliže } w \in \{0,1\}^*, \text{ pak } w1, w0 \in \{0,1\}^*$$

$$\text{reverse } (011100)^R = 001110$$

$$1) \varepsilon^R = \varepsilon$$

$$2) (w0)^R = 0w^R \quad (w1)^R = 1w^R$$

Binární relace

- Pr
- 1) rovnost objektů
 - 2) být dělitelem
 - 3) být podmnožinou
 - 4) menší nebo rovno
 - 5) student si kapsal předmět
 - 6) funkce sinus
- (x, y) je v relaci iff $y = \sin x$

Def: Binární relace R z množiny A do množiny B
je $R \subseteq A \times B$

napíšeme $(x, y) \in R$, ale píšeme $x R y$

Definice obor relace $R \subseteq A \times B$

$$\{x; x \in A, x R y \text{ pro nějaké } y \in B\}$$

obor hodnot R $\{y; y \in B, x R y \text{ pro nějaké } x \in A\}$

operace s relacemi:

- 1) Inverzní relace: Máme $R \subseteq A \times B$, pak
inverzní relace R^{-1} je relace z B do A .
definována: $b R^{-1} a$ iff $a R b$.

- 2) Skládaní relací:

Máme danou relaci R z A do B , relaci S z B do C , pak
složená relace $R \circ S$ je relace definována:

$R \circ S$ je relace z A do C

$a (R \circ S) c$ iff existuje $b \in B$ tak, že $a R b, b S c$.

Sklaotānā relāci ņ asociatīvi: $\text{if } (R \circ S) \circ T = R \circ (S \circ T)$
 kadkolio $R \# A \text{ do } B$, $S \# B \text{ do } C$, $T \# C \text{ do } D$

Ano, prolē

$a(R \circ S) \circ Td$ if $\text{ex. } c \in C, \bar{a} R \circ S c, cTd$

if $\text{ex. } b \in B, \bar{a} Rb, bSc, cTd$

$aRb \quad bScTd$

$aR \circ (S \circ T) d$

Sklaotānā relāci nenī komutatīvi

$R \circ S \neq S \circ R$ i kadz oke relāce evadujis

Px: A: māxina, lido

aSb iff a je sūrozenees b

cRd iff c je rodiē d

$aS \circ Rc$ if $\text{ex. } b \quad aSb, bRc$ - a sūjē, c je sūroee

ale dwojē sūjē a , sūroee c nenī o relāci $R \circ S$

$aR \circ Sc$ by znamēnālo a je rodiē b , b je sūrozenees c ,
 znamēnā a rodiē c

Relace na množině A , tj. $R \subseteq A \times A$

Překontrolujeme, že R je

- a) reflexivní iff aRa pro každé $a \in A$
- b) symetrická iff pro každé a, b platí: je-li aRb , pak bRa .
- c) antisymetrická iff pro každé a, b platí:
je-li aRb a bRa , pak $a=b$
- d) transitivní iff pro každé $a, b, c \in A$ platí:
je-li aRb a bRc , pak aRc

Def: Máme relaci R na množině A . R se nazývá ekvivalence iff je reflexivní, symetrická a transitivní.

- Př:
- 1) rovnost je ekvivalence
 - 2) relace "podobnosti" na trojúhelnících
 - 3) R na $\mathbb{Z}$ (celá čísla) je definována
 aRb iff $(a-b)$ je sudé číslo

4) $A = \{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{N} \setminus \{0\}\}$

$$(m, n) S (p, q) \text{ iff } m \cdot q = n \cdot p$$

$$\frac{m}{n} S \frac{p}{q}$$

✓ domrem představují stejné číslo

reflexivita: $\exists (p, q) S (p, q) \quad p \cdot q = q \cdot p \quad \checkmark$

symetrie: když $(p, q) S (r, s)$, tj. $ps = qr$, $rs = qp = ps = qr$,
tj. $(r, s) S (p, q)$

(6)

transitivita:

$$(p, q)S(x, y), (r, s)S(x, y), \quad \left(\begin{array}{l} ? (p, q)S(x, y) \\ py = qx \end{array} \right)$$

tg. $ps = qx, rx = sy$

$y = \frac{sx}{r}$ pro $r \neq 0$

$$\underline{py} = p \cdot \frac{sx}{r} = ps \cdot \frac{x}{r} = qx \cdot \frac{x}{r} = qx \quad r \neq 0$$

$r = 0$ $ps = 0, s \neq 0$, tg. $\underline{p = 0}$, tg. $py = 0$, navíc $r = 0$,
tg. $sx = 0$, tg. $\underline{x = 0}$

$$0 = py = qx = 0$$

tg. $(p, q)S(x, y)$

S je vlastně rovnost čísel jakéhožto racionálního č.

Třída ekvivalence R obsahující prvky $a \in A$ je

$$R[a] = \{ b \mid a R b \}$$

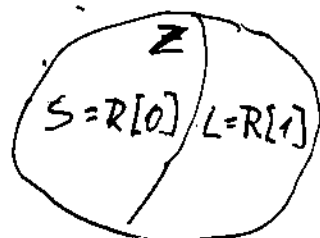
Př. 1) $\mathbb{Z}$, $i R j$ iff $i - j$ je sudé

$$R[0] = \{ i \mid 0 R i \}$$

$-i = 0 - i$ je sudé, tg. i je sudé.

$$R[0] = \{ 2k \mid k \in \mathbb{Z} \}$$

$$R[1] = \{ j \mid 1 R j \} = \{ 2k+1 \mid k \in \mathbb{Z} \}$$



$$p \sim 2) \quad (p, q) S (r, s) \quad \nexists \quad p s = q r$$

$$\frac{p}{q} S \frac{r}{s} \quad \text{---} \quad \text{---}$$

$$S[(1,2)] = \left\{ (x, y) \mid y = 2x \right\} \quad - \text{ všechny rovnice}$$

odpovídající racionální čísla $\frac{1}{2}$

Věta: Jestliže R je ekvivalence na množině A , pak $\{R[a] \mid a \in A\}$ splňuje následující vlastnosti:

- 1) $\{R[a]\} \neq \emptyset$ pro každé $a \in A$, $\bigcup_{a \in A} R[a] = A$
- 2) Když $R[a] \cap R[b] \neq \emptyset$, tak $R[a] = R[b]$

D: 1) $a \in R[a]$, neboť aRa pro každé $a \in A$ (reflexivita)
 $\nexists R[a] \neq \emptyset$

$$\bigcup_{a \in A} R[a] = A$$

$$R[a] \cap R[b] = \{b \mid aRb\} \subseteq A$$

- 2) Když $R[a] \cap R[b] \neq \emptyset$, tj. existuje c , $\exists c \in R[a]$
 $c \in R[b]$

$$\text{tj. } \underline{aRc}, \underline{bRc}, \underline{cRb} \quad \text{tj. } aRb, bRa$$

symetrie tranzitivita symetrie

$$R[a] \overset{c}{\cap} R[b]$$

$$\underline{d \in R[a]}, \text{ tj. } \underline{aRd}, \underline{bRa}, \text{ tj. } \underline{bRd}, \text{ tj. } \underline{d \in R[b]}$$

tranzitivita

$$\underline{e \in R[b]}, \text{ tj. } \underline{bRe}, \underline{aRb}, \text{ tj. } \underline{aRe}, \text{ tj. } \underline{e \in R[a]}$$

$$\hookrightarrow \text{tj. } R[a] = R[b]$$

Množina $\mathcal{Y}$ neprázdnejch podmnožín množiny A sa nazýva
rozklad A iff

$$1) \bigcup \{X \mid X \in \mathcal{Y}\} = A$$

$$2) \text{ Když } X \cap Y \neq \emptyset, \text{ tak } X = Y$$

Keta úloha: Každá ekvivalencia na A určuje rozklad na A .

Tvrzení: Je-li $\mathcal{Y}$ rozklad množiny A a definujeme-li

$R_{\mathcal{Y}}$ takto:

$a R_{\mathcal{Y}} b$ iff existuje $X \in \mathcal{Y}$ tak, že $a, b \in X$

pak $R_{\mathcal{Y}}$ je ekvivalence.

$R_{\mathcal{Y}}$ je reflexivní, ano každé $a \in A$ leží v nějaké $X \in \mathcal{Y}$

$R_{\mathcal{Y}}$ je symetrická - zřejmé

$R_{\mathcal{Y}}$ je transitivní: $\left. \begin{array}{l} a R_{\mathcal{Y}} b \\ b R_{\mathcal{Y}} c \end{array} \right\} \begin{array}{l} a, b \in X \\ b, c \in Y \end{array} \left. \vphantom{\begin{array}{l} a R_{\mathcal{Y}} b \\ b R_{\mathcal{Y}} c \end{array}} \right\} \begin{array}{l} b \in X \cap Y \neq \emptyset \\ \text{if } X = Y, \\ \text{if } a, b, c \in X \end{array}$

$$\underline{R_{\mathcal{Y}}} \text{ ekvivalence } \rightsquigarrow \mathcal{Y} = \{R[a] \mid a \in A\} \rightsquigarrow \underline{R_{\mathcal{Y}}}$$

$$\text{pak } R = R_{\mathcal{Y}}$$

$$\underline{\mathcal{Y}} \text{ je rozklad } \rightsquigarrow R_{\mathcal{Y}} \rightsquigarrow \underline{\{R_{\mathcal{Y}}[a] \mid a \in A\}}$$

$$\text{pak } \mathcal{Y} = \{R_{\mathcal{Y}}[a] \mid a \in A\}$$

je-li R ekvivalence na A , pak

$\{R[a] \mid a \in A\}$ se nazývá faktorová množina podle R
značení A/R

PM 1) $\mathbb{Z}/R = \{S, L\}$ $S = R[0], L = R[1]$

2) $A/S = \mathbb{Q}$

Uspořádání (částečné uspořádání)

značí $\subseteq$

Relace R se nazývá uspořádání (částečné uspořádání, partial order) iff je reflexivní, antisymetrická a tranzitivní

PM. 1) $A = P$, relace $\subseteq$

2) $A = \{X \mid X \subseteq U\} = P(U)$, $\subseteq$

$X \subseteq X$; když $X \subseteq Y, Y \subseteq X$, pak $X = Y$;

kdýž $X \subseteq Y, Y \subseteq Z$, pak $X \subseteq Z$

3) $A = \mathbb{N}$, relace je dělitelnost $|$, tj $m|m$ iff
 $m = k \cdot n$ pro nějaké $k \in \mathbb{N}$

tedy $m|m$ $n = 1 \cdot m$

2) když $m|m, m|n$, tak $m = k \cdot n, n = l \cdot m$

tj $m = (k \cdot l) \cdot m$ $k \cdot l = 1, k = 1 = l$

3) $m|m, m|p$, tak $m = k \cdot n, p = l \cdot m$, tj $p = (l \cdot k) \cdot n$
tj $m|p$

Hasseho diagram uspořádaní

$$P\mathbb{N} \cdot A = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

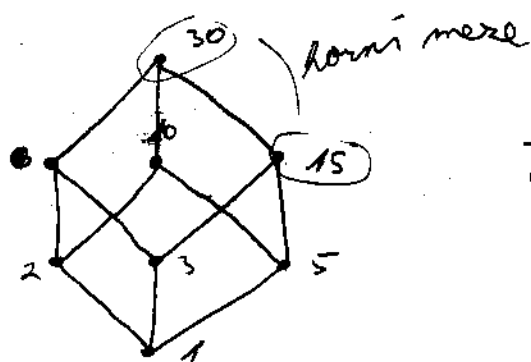
relace pokrývání:

co je menší, je na diagramu níže

$a < b$ iff $a \in b$ a neexistuje

$$c \neq a, c \neq b$$

$$a \in c, c \in b$$



$$B = \{3, 5\}$$

$$\sup \{3, 5\} = 15$$

$$\inf \{3, 5\} = 1$$

Máme množinu A a na ní uspořádaní $\in$.

Pro $a, b \in A$ je pokrývání nesrovnatelné iff
neplatí $a \in b$ ani neplatí $b \in a$

Pro $B \subseteq A$ platí: supremum množiny B ($\in A$) je
takový prvek c , který splňuje:

1) $x \in c$ pro každé $x \in B$ (c je horní mez)

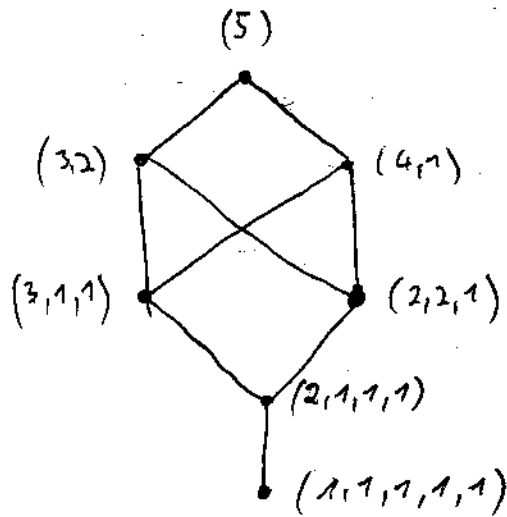
2) kdykoliv $x \in d$ pro každé $x \in B$, tak $c \in d$.
(c je nejmenší horní mez)

Pro $e \in A$ je pokrývání infimum množiny B iff

1) $e \in x$ pro každé $x \in B$ (e je dolní mez)

2) kdykoliv $f \in x$ pro každé $x \in B$, tak $f \in e$.
(e je největší dolní mez)

P2 (A, E) , jehož Hasse diagram



$$\sup \{ (3,1,1), (2,2,1) \}$$

$$\text{horní mez } \{ (3,1,1), (2,2,1) \}$$

$$(3,2), (4,1), (5)$$

neexistuje nejmenší

horní mez, tj. neexistuje

$$\inf \{ (4,1), (3,2) \} \text{ neexistuje}$$

$$\sup \{ (3,2), (4,1) \} = (5)$$

$$\inf \{ (2,2,1), (3,1,1) \} = (2,1,1,1)$$

Tvrzení: Máme uspořádání E na A a $B \subseteq A$.

Jestliže existuje $\sup(B)$, pak je políné.

Obdobně pro $\inf(B)$

D: Kdyby c_1, c_2 byla suprema B , pak $c_1 \equiv c_2$

(c_1 je nejmenší horní mez, c_2 je horní mez)

$$c_2 \equiv c_1$$

(c_2 je nejmenší horní mez, c_1 je horní mez)

tedy z antisymetrie $c_1 = c_2$

Máme uspořádanou množinu $(A, \subseteq)$

Prvek $a \in A$ je největší prvek iff $x \subseteq a$ pro každé $x \in A$

Prvek $b \in A$ je maximální prvek iff neexistuje $x \in A, x \neq b$ a $b \subseteq x$
 $\neg \exists x (b \subseteq x \wedge b \neq x) \quad \forall x (b \subseteq x \Rightarrow x = b)$

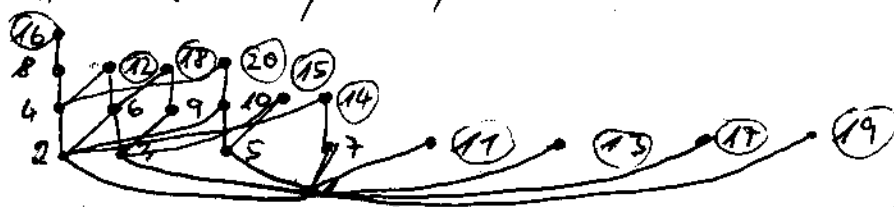
Když a je největší, tak je i maximální

Př. $A = \{1, \dots, 20\}$ | dělitelnost

není největší prvek

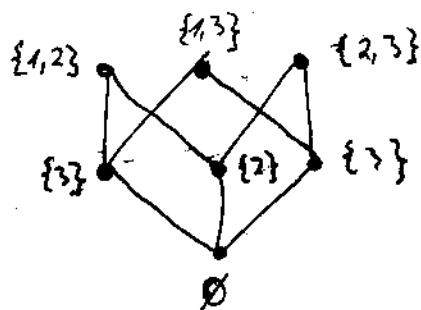
maximální prvky 20, 19, 18, ..., 11

10 není max. prvek, dělí 20



jiný př.

$A = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\} \} \subseteq$



není největší prvek

maximální prvky $\{1,2\}, \{1,3\}, \{2,3\}$

celá čísla

Lemma o dělení: Pro každá celá čísla a, b , $a \neq 0$, existují
jednoznačně celá čísla q, r tak, že $b = a \cdot q + r$, $0 \leq r < |a|$
 $\downarrow$ $\downarrow$
cel. podíl zbytek

Pro $a > 0, b \geq 0$ známé

Pro $b < 0$ $-b = q_1 a + r_1$

$$b = (-q_1)a - r_1 =$$

$$= \underbrace{-(q_1 + 1)}_q a + \underbrace{(a - r_1)}_r$$

$$0 \leq r_1 < a$$

$$0 \leq a - r_1 < a$$

Def: 1) Číslo a dělí b iff $r = 0$, tj. $b = q \cdot a$.

2) Číslo c je společný dělitel a, b iff $c|a, c|b$

3) Číslo c je největší společný dělitel a, b ($c = \gcd(a, b)$) i)

a) $c|a, c|b$

b) if $d|a, d|b$, then $d|c$

Euklidov algoritmus

Vstup: $a, b \in \mathbb{Z}, a, b > 0$

Výstup: $c = \text{gcd}(a, b)$

1. if $a \geq b$, then $x := a, t := b$ ($x_2 = 1, y_2 = 0, x_t = 0, y_t = 1$)
else $x := b, t := a$ ($x_2 = 0, y_2 = 1, x_t = 1, y_t = 0$)
2. spočítáme $r = q \cdot t + r$, kde $0 \leq r < t$
3. if $r = 0$, then $c := t$ ~~stop~~ ($x = x_t, y = y_t$) stop
else $x := t, t := r$ a goto 2
($u = x_2 - q x_t, v = y_2 - q y_t, x_2 = x_t, y_2 = y_t, x = t, y = u, t = v$)

Správnost algoritmu:

Platí: Dvojice z, t má stejné dělitele, jako dvojice t, r

a) if $d | x, d | t$, tj. $x = k \cdot d, t = l \cdot d$

$$\begin{aligned} x &= q \cdot t + r & r &= x - q \cdot t = k \cdot d - q \cdot l \cdot d = \\ & & &= (k - q \cdot l) \cdot d, \text{ tj. } d | r \end{aligned}$$

b) if $e | t, e | r$, $t = l \cdot e, r = p \cdot e$

$$\begin{aligned} x &= q \cdot t + r = q \cdot l \cdot e + p \cdot e = (q \cdot l + p) \cdot e, \\ & \text{tj. } e | x \end{aligned}$$

Bézoutova věta: Máme celá nesoporná čísla a, b , pak

existují celá čísla x, y tak, že

$$ax + by = c, \text{ kde } c = \text{gcd}(a, b)$$

$$k = a \quad t = b$$

albo

$$k = b \quad t = a$$

$$a = 1 \cdot a + 0 \cdot b$$

$$b = 0 \cdot a + 1 \cdot b$$

$$k = k - q \cdot t$$

Když

$$k = a x_k + b y_k \quad t = a x_t + b y_t$$

$$k = k - q \cdot t = a x_k + b y_k - q (a x_t + b y_t) =$$

$$= a (x_k - q x_t) + b (y_k - q y_t)$$

$\underbrace{\hspace{1cm}}_{x_k} \quad \underbrace{\hspace{1cm}}_{y_k}$

Pr: ... $a = 127, b = 36$

1. $k = 127, t = 36$

$$127 = 3 \cdot 36 + 19$$

2. $k = 36, t = 19$

$$36 = 1 \cdot 19 + 17$$

3. $k = 19, t = 17$

$$19 = 1 \cdot 17 + 2$$

4. $k = 17, t = 2$

$$17 = 8 \cdot 2 + 1$$

$$1 = -17 \cdot 127 + 60 \cdot 36$$

$$x = -17 \quad y = 60$$

	127	36	
127	1	0	
36	0	1	
127	1	0	
-3 \cdot 36	0	-3	
19	1	-3	
36	0	1	
-19	-1	3	
17	-1	4	
19	1	-3	
-17	1	-4	
2	2	-7	
17	-1	4	
-8 \cdot 2	-16	56	
1	-17	60	

Důsledky:

Twicken: Rovnice $ax + by = c$ má celočíselné řešení x, y
iff c je násobkem $\gcd(a, b)$

D.: a) p-li $c = k \cdot \gcd(a, b)$, pak existují x_1, y_1 tak,
že $ax_1 + by_1 = \gcd(a, b)$

$$a \cdot \underbrace{(kx_1)}_x + b \cdot \underbrace{(ky_1)}_y = k \cdot \gcd(a, b) = c$$

b) jestliže $ax + by = c$ pro $x, y \in \mathbb{Z}$ a $d = \gcd(a, b)$
dělí a, b

$$a = kd, b = ld$$

$$kdx + ldy = c, \text{ tj. } c = d(kx + ly) \text{ a } d | c$$

ovšem p-li a, b nesoudělná a číslo a dělí $b \cdot c$,
pak a dělí c .

D. a, b nesoudělná $\gcd(a, b) = 1$

$$x, y \in \mathbb{Z} \quad ax + by = 1 \quad | \cdot c$$

$$acx + bcy = c$$

a dělí acx , a dělí bcy , tedy a dělí $c = acx + bcy$

Důsledek: jestliže prvočíslo p dělí $b \cdot c$, pak
dělí b nebo c nebo obojí.

(8)

Ekvivalence modulo n

$$j^{927} = j^3 = -j$$

$$927 : 4 = 231$$

$$927 = 4 \cdot 231 + 3$$

Def.: Na množině $\mathbb{Z}$ je definovaná relace $\equiv (\text{mod } n)^{(n>1)}$ takto:
 $a \equiv b (\text{mod } n)$ iff $a - b = k \cdot n$ pro nějaké $k \in \mathbb{Z}$
 iff a i b mají stejný zbytek při dělení n

Ukážeme: $a - b = k \cdot n$ iff a i b mají stejný zbytek při dělení n

$$\text{když } a = q_a \cdot n + r$$

$$b = q_b \cdot n + r$$

$$0 \leq r < n,$$

$$\text{pak } a - b = q_a \cdot n + r - (q_b \cdot n + r) = \underbrace{(q_a - q_b)}_k \cdot n$$

$$\text{když } a = q_a \cdot n + r_a$$

$$b = q_b \cdot n + r_b$$

$$r_a \neq r_b, \quad r_a > r_b$$

$$a - b = (q_a - q_b) \cdot n + (r_a - r_b) \quad 0 < r_a - r_b < n$$

$a - b$ není dělitelné n

Ukážeme: 1) Relace $\equiv (\text{mod } n)$ na $\mathbb{Z}$ je ekvivalence na $\mathbb{Z}$
 a navíc platí:

$$2) \text{ když } a \equiv b (\text{mod } n) \quad \text{pak} \quad (a+c) \equiv (b+d) (\text{mod } n)$$

$$c \equiv d (\text{mod } n), \quad a \cdot c \equiv b \cdot d (\text{mod } n)$$

D: $a \equiv b \pmod{n}$ je reflexivní

$$a - a = 0 = 0 \cdot n$$

$$a \equiv a \pmod{n}$$

je symetrická if $a - b = k \cdot n$, pak $b - a = (-k) \cdot n$
 $a \equiv b \pmod{n}$

je tranzitivní if $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$

$$a - b = k \cdot n$$

$$b - c = l \cdot n$$

$$\hline a - c = (k + l) \cdot n$$

$$a \equiv c \pmod{n}$$

$$2) \quad \begin{aligned} a - b &= k \cdot n \\ c - d &= l \cdot n \end{aligned}$$

$$(a + c) - (b + d) = (k + l) \cdot n$$

$$(a + c) \equiv (b + d) \pmod{n}$$

$$\begin{aligned} a &= b + k \cdot n \\ c &= d + l \cdot n \end{aligned}$$

$$\text{pak } \underline{a \cdot c} = (b + k \cdot n) \cdot (d + l \cdot n) =$$
$$= bd + b \cdot l \cdot n + d \cdot k \cdot n + k \cdot l \cdot n^2 =$$
$$= \underline{bd} + \underbrace{(bl + dk + kl \cdot n)}_p \cdot n$$

$$ac - bd = p \cdot n$$

$$p = bl + dk + kl \cdot n$$

$$ac \equiv bd \pmod{n}$$

Speciálně: Když $a \equiv b \pmod{n}$, pak

$$1) \quad x \cdot a \equiv x \cdot b \pmod{n} \text{ pro každé } x \in \mathbb{Z}$$

neboť $x \equiv x \pmod{n}$

$$a \equiv b \pmod{n} \text{ tudíž } x \cdot a \equiv x \cdot b \pmod{n}$$

$$2) \quad a^x \equiv b^x \pmod{n} \quad x > 1$$

neboť pro $x=2$

$$a \equiv b \pmod{n}$$

$$a \equiv b \pmod{n} \text{ tudíž } a^2 \equiv b^2 \pmod{n}$$

dale indukcí

Věta dělitelnosti: 9 (3) $a_0 \dots a_n$ cifra na místě n

$$1 \equiv 1 \pmod{9}$$

$$10 \equiv 1 \pmod{9}$$

$$100 \equiv 1 \pmod{9}$$

$$10^k \equiv 1 \pmod{9}$$

$$a_0 \equiv a_0 \pmod{9}$$

$$a_1 \cdot 10 \equiv a_1 \pmod{9}$$

$$\vdots$$
$$a_i \cdot 10^i \equiv a_i \pmod{9}$$

víceciferné číslo

$$a_n a_{n-1} \dots a_1 a_0 \Rightarrow a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$$

$$(a_n \cdot 10^n + \dots + a_1 \cdot 10 + a_0) \equiv (a_n + a_{n-1} + \dots + a_1 + 10) \pmod{9}$$

Ukážeme, že číslo $a_n \dots a_1 a_0$ má stejný zbytek
při dělení 9(3) jako jeho ciferný součet

Problém: ① Řešte $(a+x) \equiv b \pmod{n}$

hledajte x tak, aby

$$x \equiv (b-a) \pmod{n}$$

② Řešte $a \cdot x \equiv b \pmod{n}$

$$ax - b = k \cdot n$$

$$ax - nk = b \quad -k=y \quad ax + ny = b$$

$$x, y \in \mathbb{Z}$$

má řešení iff b je dělitelné $\gcd(n, a)$

$ax \equiv b \pmod{n}$ má řešení pro každé b
iff a, n nesoudělná

Eulerova funkce
 $n \geq 1$

$\phi(n)$ je počet všech i , $0 \leq i < n$,
které jsou nesoudělné s n .

$$\phi(p) = p-1 \quad (p \text{ prvočíslo})$$

$$\phi(p^k) = p^k - p^{k-1}$$

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n) \quad m, n \text{ nesoudělná}$$

Malá Fermatova věta: p -li p prvočíslo a číslo a

je nesoudělné s p , pak $a^{p-1} \equiv 1 \pmod{p}$

Lemma: p -li p prvočíslo, pak $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ je dělitelné p
pro každé i , $0 < i < p$

$$i!(p-i)! \cdot \binom{p}{i} = p!$$

$i!(p-i)!$ není dělitelný p pro $i < p$
nesoudělný s p , tudíž p dělí $\binom{p}{i}$

$(p-i)!$ — " — $i > 0$

Lemma: je-li p prvočíslo, pak $a^p \equiv a \pmod{p}$

indukcí podle $a \geq 0$

$$a=0 \quad 0^p = 0 \equiv 0 \pmod{p}$$

$$a=1 \quad 1^p = 1 \equiv 1 \pmod{p}$$

indukční krok

je-li $a^p \equiv a \pmod{p}$, tj. $a^p - a = k \cdot p$, pak

$$\begin{aligned} (a+1)^p - (a+1) &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a + 1 - a - 1 \\ &= \underbrace{a^p - a}_{\text{děl } p} + \underbrace{\binom{p}{1}a^{p-1}}_{\text{děl } p} + \underbrace{\binom{p}{2}a^{p-2}}_{\text{děl } p} + \dots + \underbrace{\binom{p}{p-1}a}_{\text{děl } p} \quad \text{je dělitelné} \end{aligned}$$

Malá Fermatova věta

Když $a^p \equiv a \pmod{p}$

$$a^p - a = k \cdot p$$

$$a(a^{p-1} - 1) = k \cdot p$$

a, p nesoudělná
tj. a dělí k , tj. $k = l \cdot a$

$$a(a^{p-1} - 1) = a \cdot l \cdot p$$

$$a^{p-1} - 1 = l \cdot p$$

$$\underline{a^{p-1} \equiv 1 \pmod{p}}$$

Euler-Fermatova věta:

jestli a, n nesoudělná, pak

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

RSA: Alice, Bob posílají zprávy x

Zvolí p, q jsou prvočísla, každé ≈ 10 ciferné

$$N = p \cdot q$$

Věřejný klíč $\boxed{N}$
 e_A, e_B

$$\phi(N) = (p-1)(q-1)$$

Alice: zvolí e_A nesoudělné s $\phi(N)$

k tomu spočítá d_A tak, že

$$e_A \cdot d_A \equiv 1 \pmod{\phi(N)} \quad (e_A \cdot x \equiv 1 \pmod{\phi(N)})$$

jako bylo obecně

Bob: Zvolí e_B nesoudělné s $\phi(N)$

spočítá d_B , že $e_B \cdot d_B \equiv 1 \pmod{\phi(N)}$

to sdělají jednou

(e -encryption, d -decryption)

Bob chce poslat zprávu x

$$z \equiv x^{e_A} \pmod{N}$$

pošle z .

Alice přijme z a spočítá $u \equiv z^{d_A} \pmod{N}$

Platí $u = x$

Elektronický podpis:

$$\cancel{x} \quad S \equiv x^{d_B} \pmod{N}$$

|
podpis Boba

Alice

$$v \equiv S^{e_B} \pmod{N}$$

a musí $x = u = v$

Ukážeme, že $x = u$

$$u \equiv x^{d_A} \pmod{N} \equiv (x^{e_A})^{d_A} \pmod{N} \equiv x^{e_A \cdot d_A} \pmod{N}$$

$$e_A \cdot d_A \equiv 1 \pmod{\phi(N)}$$

$$e_A d_A = 1 + k \cdot \phi(N)$$

$$u = x^{1+k\phi(N)} \pmod{N} \equiv x \pmod{N} \quad | \quad x \text{ nesoudělné s } p, q$$

Zbytkové třídy mod n :

$$\begin{aligned} [i]_n &= \{j \mid j \equiv i \pmod{n}\} = \{j \mid j - i = k \cdot n, k \in \mathbb{Z}\} = \\ &= \{i + k \cdot n \mid k \in \mathbb{Z}\} \end{aligned}$$

$$[0]_n = \{kn \mid k \in \mathbb{Z}\}, [1]_n = \{1 + kn \mid k \in \mathbb{Z}\}, \dots, [n-1]_n = \{n-1 + kn \mid k \in \mathbb{Z}\}$$

Máme n různých zbytkových tříd $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$

$\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\}$... množina zbytkových tříd

na $\mathbb{Z}_n$ definujeme operace

$$[i]_n \oplus [j]_n = [i+j]_n \quad [i]_n \ominus [j]_n = [i-j]_n$$

9

$\oplus, \odot$ potu dobiti definovane

$k \in [i]_m \quad l \in [j]_m$

$k \equiv i \pmod{m} \quad l \equiv j \pmod{m}, \text{ tj. } k+l \equiv i+j \pmod{m}$
 $k \cdot l \equiv i \cdot j \pmod{m}$

$k+l \in [i+j]_m$

$k \cdot l \in [i \cdot j]_m$

ex: ① $(\mathbb{Z}_2, \oplus, \odot)$

$\odot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

$\oplus$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

② $\mathbb{Z}_4, \oplus, \odot$

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$
$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Vlastnosti $(\mathbb{Z}_n, \oplus, \odot)$

1) $[i]_n \oplus [j]_n = [j]_n \oplus [i]_n$ komutativní

2) $[i]_n \oplus ([j]_n \oplus [k]_n) = ([i]_n \oplus [j]_n) \oplus [k]_n$ asociativní

3) $[i]_n \oplus [0]_n = [i]_n$ $[0]_n$ je neutrální

4) $[i]_n \oplus [-i]_n = [0]_n$ neboli $[-i]_n = -[i]_n$
je opačný (inverzní) prvek k $[i]_n$

5) $[i]_n \odot [j]_n = [j]_n \odot [i]_n$ komutativní

6) $[i]_n \odot ([j]_n \odot [k]_n) = ([i]_n \odot [j]_n) \odot [k]_n$

7) $[i]_n \odot [1]_n = [i]_n$ $[1]_n$ je jednotkový prvek $\odot$

Kdy existují $[x]_n$ tak, aby $[i]_n \odot [x]_n = [1]_n$

$$[i \cdot x]_n = [1]_n$$

$$ix \in [1]_n$$

$$ix \equiv 1 \pmod{n}$$

$$ix - 1 = kn \quad x, y \in \mathbb{Z}$$

$$-k = y \quad ix - kn = 1$$

$$ix + my = 1$$

má řešení iff i, n jsou nesoudělné

Je-li p prvočíslo, $\text{v } \mathbb{Z}_p = \{[0]_p, [1]_p, \dots, [p-1]_p\}$

pro každé $[i]_p \neq [0]_p$ existuje $[x]_p$ tak, že

$$[i]_p \odot [x]_p = [1]_p$$

Je-li n složené, tj. $n = k \cdot l$, $k \neq 1$, $l \neq 1$

pro $[i]_n$ existuje $[x]_n$, že $[x]_n \odot [i]_n$ iff
jsou nesoudělné, tj. jich $\phi(n)$

Číselné nuly jsou takové regulární prvky $[i]_n, [j]_n$,

že $[i]_n \odot [j]_n = [0]_n$, tj. když $n = k \cdot l$,

$$\text{pak } [k]_n \odot [l]_n = [0]_n$$

8) že právě $[i]_n$ existuje $[x]_n$ tak, že $[i]_n \odot [x]_n = [1]_n$
iff i, n jsou nesoudělné.

pak $[i]_n$ je násobná prvky ~~$[1]_n$~~ inverzní prvky
k $[i]_n$ a značí $[i]_n^{-1}$

9) jestliže n není prvočíslo, pak existují číselné nuly
pro $\odot$.

10) $[i]_n \odot ([j]_n \oplus [k]_n) = [i]_n \odot [j]_n \oplus [i]_n \odot [k]_n$
distributivní $\times$.

$(\mathbb{Z}_p, \oplus, \odot)$ má podobné vlastnosti $(\mathbb{R}, +, \cdot)$

Aplikace v kódování (Hammingovy kódy)

informační znaky + kontrolní znaky

Hammingův binární kód

<u>a b c d</u>	<u>x y z</u>
inf. zn.	kontrolní zn.

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$abcdxyz$ bude kódovým slovem iff $H \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

$\mathbb{Z}_2$

$[x]_2$

$\oplus \begin{array}{c|c} [0]_2 & [1]_2 \\ \hline [0]_2 & [1]_2 \end{array}$

$[0]_2 \mid [0]_2 \mid [1]_2$

$[1]_2 \mid [1]_2 \mid [0]_2$

$$[x]_2 \oplus [x]_2 = 0$$

$$\begin{array}{rcll} a + b + d + x & = & 0 & | + x \\ a + c + d + y & = & 0 & | + y \\ b + c + d + z & = & 0 & | + z \end{array}$$

$$\begin{aligned} x &= a + b + d \\ y &= a + c + d \\ z &= b + c + d \end{aligned}$$

vysláno x

přijati jsme y

když došlo k jedné chybě na místě i

$$\underline{y} = \underline{x} + \underline{e}_i$$

$$\underline{e}_1 = 1000000$$

$$\underline{e}_i = 0 \dots 1 \dots 0$$

i -té místo

$$H \cdot y = H(\underline{x}^T + \underline{e}_i^T) = H \cdot \underline{x}^T + H \cdot \underline{e}_i^T = H \cdot \underline{e}_i^T = i\text{-tý sloupec}$$

matice H

→ mine, kde chyba, kde je opraven

umí opravit 1 chybu, rozpozná 2 chyby

Rozšířený Hammingův binární kód

abcdxyzw

$$\bar{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

abcdxyzw posílám iff $\bar{H} \begin{pmatrix} a \\ b \\ c \\ d \\ x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$$a + b + d + x = 0$$

$$x = a + b + d$$

$$a + c + d + y = 0$$

$$y = a + c + d$$

$$b + c + d + z = 0$$

$$z = b + c + d$$

$$a + b + c + d + x + y + z + w = 0$$

$$w = a + b + c$$

$$a + b + c + w = 0$$

Dostal 4 jednotné chyby - stejné

$$\bar{H} \cdot \bar{y}^T \dots$$

opraví 1 chybu

Dostal 2 chyby $y = x + \underline{e}_i + \underline{e}_j$

$$\bar{H} \cdot \bar{y}^T = \bar{H}(\underline{x}^T + \underline{e}_i^T + \underline{e}_j^T) = \bar{H} \cdot \underline{x}^T + \bar{H} \cdot \underline{e}_i^T + \bar{H} \cdot \underline{e}_j^T = i\text{-tý} + j\text{-tý sl.}$$

2 chyby pozná

Pologrupy, monoidy, grupy

Máme množinu S . Binární operace na S je zobrazení, které každé dvojici prvků $x, y \in S$ přiřadí výsledek operace prvek $x \in S$

$$* : x, y \mapsto x * y$$

Pr. 1) $(\mathbb{Z}, +)$, $(\mathbb{R}, \cdot)$, $(M_n, \cdot)$ M_n jsou číselové matice.

2) $S = \langle 0, 1 \rangle$ $a * b = \min(a, 1-b)$

3) S je množina všech slov nad A , $\cdot$ je křesření dvou slov
 $u = x_1 \dots x_m$ $v = y_1 \dots y_n$ pak $u \cdot v = x_1 \dots x_m y_1 \dots y_n$
 $x_i \in A$ $y_i \in A$

4) S je množina zobrazení $x \mapsto x$
 $\circ$ složitání zobrazení

grupoid je množina s binární operací.

grupoid $(S, *)$ je pologrupa iff pro každé $x, y, z \in S$ platí

$$x * (y * z) = (x * y) * z,$$

tj. platí asociativní zákon

Není pologrupa $(\mathbb{N}, \div)$ $3 \div (2 \div 1) = 2$, $(3 \div 2) \div 1 = 0$

$$(\mathbb{N}, \div) \quad m \div n = \begin{cases} m-n & \text{if } m \geq n \\ 0 & \text{jinak} \end{cases}$$

$$\langle 0, 1 \rangle \quad a * b = \min(a, 1-b)$$

$$(a * b) * c = \min(a, 1-b) * c = \min(\min(a, 1-b), 1-c)$$

$$a * (b * c) = a * \min(b, 1-c) = \min(a, 1-\min(b, 1-c))$$

$$\text{např. } a = \frac{3}{4}, b = \frac{1}{2}, c = \frac{3}{4}$$

$$\frac{3}{4}, 1 - \min(\frac{1}{2}, 1 - \frac{3}{4})$$

$$(\frac{3}{4} * \frac{1}{2}) * \frac{3}{4} = \frac{1}{4}$$

$$\frac{3}{4} * (\frac{1}{2} * \frac{3}{4}) = \frac{3}{4}$$

není pologrupa

Pologrupa $(S, *)$ je monoid iff. existuje $e \in S$ takový,

že $e * x = x * e = x$ pro každý $x \in S$

e je neutrální nebo jednotkový prvek

Př. $(\mathbb{Z}, +)$ je monoid $e = 0$

$(\mathbb{R}, \cdot)$ je monoid, $e = 1$

$(M_n, \cdot)$ je monoid, $e = E$

$(A^*, \cdot)$ slova, je monoid, $e = \varepsilon$ prázdné slovo

S je mn. všech zobrazení X do X , o je identické
zobrazení $x \mapsto x$

$$f \circ e = e \circ f = f$$

$(\mathbb{Z}_n, +)$ je monoid, $e = [0]_n$

$(\mathbb{Z}_n, \cdot)$ je monoid, $e = [1]_n$

Máme monoid $(S, *)$ s neutrálním, resp. jednotkovým prvkem e .

Řekneme, že k prvku $x \in S$ existuje opačný, resp. inverzní prvek

iff existuje $y \in S$ tak, že $x * y = e = y * x$

Prvky, ke kterým existuje opačný, inverzní se nazývají invertibilní prvky

Lemma: Jestliže existují prvky y, z tak, že

$$x * y = e = x * z$$

pak $y = z$ a y je inverzní prvek k x

$$D: y = e * y = (x * x) * y = x * (x * y) = x * e = x$$

Inverzní prvek k prvku x značíme x^{-1}

Opačný — " — x — " — $-x$

Monoid je grupa iff každý prvek je invertibilní.

Př. $(\mathbb{Z}, +)$ $e = 0$ pro každý $a \in \mathbb{Z}$ je $-a$ prvek
 $a + (-a) = 0 = (-a) + a$

$(\mathbb{R}, \cdot)$ $e = 1$ není grupa 0^{-1} neexistuje

$(\mathbb{R} \setminus \{0\}, \cdot)$ $e = 1$ je grupa

$(M_n, \cdot)$ $e = E$ není grupa, pro singulární matice neexistuje A^{-1}

Máme monoid $(S, *)$, e je jednotkový prvek

1) $e^{-1} = e$ neboť $e * e = e$

2) jestliže existuje a^{-1} , pak $(a^{-1})^{-1} = a$

$$a * a^{-1} = e = a^{-1} * a$$

3) jestliže existují a^{-1} i b^{-1} , pak

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$$

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e$$

Věta: Pologrupa $(S, *)$ je grupou iff pro každé $a, b \in S$ existují $x, y \in S$ tak, že

$$a * x = b, y * a = b$$

Jinými slovy: pologrupa je grupa iff můžeme řešit všechny rovnice tvaru $a * x = b, y * a = b$.

1) Když $(S, *)$ je grupa, pak

$$a^{-1} * a * x = a^{-1} * b \text{ znamená } x = a * b^{-1}$$

$$y * a = b \text{ znamená } y = b * a^{-1}$$

2) Předpokládejme, že pro každé $a, b \in S$ existují $x, y \in S$ tak, že $a * x = b, y * a = b$

Vezmeme

$$a * x = a$$

$$x = e$$

$$y * a = a$$

$$y = f$$

Vezmeme $c \in S$

$$c * e = (f * a) * e = f * (a * e) = f * a = c$$

$$c = f * a$$

$$f * c = f * (a * x) = (f * a) * x = a * x = c$$

$$a * x = c$$

$$f = f * e = e$$

$f = e$ je jednotkový prvek

$T_0(S, *)$ je monoid s jednotkovým prvkem e .

$a * x = e \quad y * a = e$. Taková $x, y \in S$ existují,

$$\text{pak } x = y = a^{-1}$$

Lemma: Je-li $(S, *)$ grupa, pak každá rovnice

$a * x = b, \quad y * a = b$ má jednoznačně určené řešení.

$$\text{Kdyby } a * x_1 = b \quad a * x_2 = b \quad \text{pak } a * x_1 = a * x_2 \\ x_1 = x_2$$

$$\text{Obdobně } y_1 * a = y_2 * a \quad y_1 = y_2$$

$(\mathbb{R}, \cdot)$ $0 \cdot x = 1$ nemá řešení, $0 \cdot x = 0$ má nekonečně řešení

$(\mathbb{Z}_m, \cdot)$ existuje-li $[i]_m^{-1}$ (tj. $\gcd(i, m) = 1$), pak je $[i]_m$ jediné.

Pologrupa, monoid, grupa je komutativní
iff $a * b = b * a$ pro každé a, b

Euler-Fermatova věta: Je-li a nesoudělné s m ,
pak $a^{\phi(m)} \equiv 1 \pmod{m}$

kde $\phi(m)$ je počet i takových, že $0 \leq i < m$ a $\gcd(i, m) = 1$

D.: $(\mathbb{Z}_m, \cdot)$ označme $\mathbb{Z}_m^* = \{[i]_m \mid [i]_m \text{ existuje}\}$
iff $\gcd(i, m) = 1$

$(\mathbb{Z}_m^*, \cdot)$ je grupa, $e = [1]_m$

$(\mathbb{Z}_m^*, \cdot)$ je komutativní grupa

$\mathbb{Z}_m^* = \{b_1, \dots, b_{\phi(m)}\}$, a nesoudělné s m
 $0 < a < m$

$\{a \cdot b_1, a \cdot b_2, \dots, a \cdot b_{\phi(m)}\} \subseteq \mathbb{Z}_m^*$ $a \cdot b_i \in \mathbb{Z}_m^*$

Když $a \cdot b_i = a \cdot b_j$, pak $b_i = b_j$

$\{b_1, b_2, \dots, b_{\phi(m)}\} = \{a b_1, a b_2, \dots, a b_{\phi(m)}\}$

$b_1 \cdot b_2 \cdot \dots \cdot b_{\phi(m)} = a b_1 \cdot a b_2 \cdot \dots \cdot a b_{\phi(m)}$

$$\underbrace{(b_1, b_2, \dots, b_{\phi(m)})}_c = a^{\phi(m)} \underbrace{(b_1, b_2, \dots, b_{\phi(m)})}_c$$

$$c = a^{\phi(m)} \cdot c$$

$$a^{\phi(m)} \equiv 1 \pmod{m} \text{ iff } 1 = a^{\phi(m)} \text{ in } (\mathbb{Z}_m^*, \cdot), \text{ tedy i v } (\mathbb{Z}_m, +)$$

(11)

Def Máme danou pologrupu $(S, *)$, pak $N \subseteq S$ je podpologrupa iff pro každé $a, b \in S$ platí
if $a, b \in N$ then $a * b \in N$

Je-li $(S, *)$ monoid s jednotkovým prvkem e , pak podpologrupa N je podmonoidem iff $e \in N$

Je-li $(S, *)$ grupa s jednotkovým prvkem e , kde každý $a \in S$ má $a^{-1} \in S$, pak podmonoid N je podgrupa iff je-li $a \in N$, je $a^{-1} \in N$

Pr $S = \{1, 2, 3, 4, 5\}$

$\oplus$	1	2	3	4	5
1	2	3	4	5	3
2	3	4	5	3	4
3	4	5	3	4	5
4	5	3	4	5	3
5	3	4	5	3	4

$$a \oplus b \begin{cases} a+b & \text{if } a+b \leq 5 \\ a+b-3 & \text{if } 6 \leq a+b \\ a+b-6 & \text{if } 9 \leq a+b \end{cases}$$

$$(a \oplus b) \oplus c$$

$$a \oplus (b \oplus c)$$

$$\begin{aligned}
 &= \begin{cases} a+b+c & \text{iff } a+b+c \leq 5 \\ a+b+c-3 & \text{iff } 6 \leq a+b+c \leq 8 \\ a+b+c-6 & \text{iff } 9 \leq a+b+c \leq 11 \\ a+b+c-9 & \text{iff } 12 \leq a+b+c \leq 14 \\ a+b+c-12 & \text{iff } a+b+c = 15 \end{cases}
 \end{aligned}$$

je podgrupa

$$a \oplus e = a \oplus a = a \quad ? \quad \text{neni monoid}$$

$\oplus$	3	4	5
3	3	4	5
4	4	5	3
5	5	3	4

je podpodgrupa

$$3 \oplus a = a = a \oplus 3$$

$$3 = e$$

je monoid

$$3 \oplus 3 = 3 \quad 4 \oplus 5 = 3 \quad 5 \oplus 4 = 3$$

je grupa

$$T = \{0, 1, 2, 3, 4, 5\}$$

$(T, \oplus)$ je monoid

Úloha 1: Máme monoid $(S, *)$ s jednotkovým prvkem e .

Uvažujeme $N = \{a \mid a \in S, \text{ existuje } a^{-1}\}$

Paž $(N, *)$ je podmonoid $(S, *)$, který je navíc grupou.

D: Máme $e^{-1} = e$, tj. $e \in N$

Když $a, b \in N$, tj. existují a^{-1}, b^{-1} . Paž $(a * b)^{-1} = b^{-1} * a^{-1}$,

tj. existuje $(a * b)^{-1}$ a tedy $a * b \in N$

Tj. $(N, *)$ je podmonoid.

$a \in N$, a^{-1} existuje, $(a^{-1})^{-1} = a$, tj. $a^{-1} \in N$

Tj. každý prvek $a \in N$ má v N inverzi a^{-1}

Úloha 2: $(\mathbb{Z}_n, \cdot)$ $e = [1]_n$ ($[a]_n \cdot [1]_n = [a]_n$)

$\mathbb{Z}_n^* = \{ [a]_n \mid [a]_n^{-1} \text{ existuje} \}$ je podmonoid,

který je grupou

$$a \mid \mathbb{Z}_n^* = \phi(n)$$

$S = \{ f; f: X \rightarrow X \}$, o složeném násobení

$e =$ identické zobrazení $id(x) = x$ pro každý $x \in X$

$N = \{ f \mid \text{existuje } f^{-1} \} = \{ f \mid f \text{ je prosté a na} \}$

je podmonoid, který je grupou

Isomorfismus, homomorfismus

Př. 1.
$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

$T = \{id, f\}$ $id: \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \end{array}$ $f: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \end{array}$

$(S, +)$ $S = \{0, 1\}$ +

$$\begin{array}{c|cc} & id & f \\ \hline id & id & f \\ f & f & id \end{array} \quad (T, \circ)$$

Př. $(\mathbb{R}^+, \cdot)$ $\xrightarrow{\log_{10}}$ $(\mathbb{R}, +, 0)$
 $\mathbb{R}^+ = \{x \mid x > 0\}$

$\log_{10}(x \cdot y) = \log x + \log y$

$\log_{10} 1 = 0$

$\log_{10} \frac{1}{x} = -\log x$

$x \cdot y = \log_{10}^{-1}(\log_{10} x + \log_{10} y)$

Def. Máme dvě pologrupy $(S, *)$, $(T, \square)$. Zobrazení $\varphi: S \rightarrow T$ se nazývá isomorfismus $(S, *)$ na $(T, \square)$ iff

1) φ je prostě a na

2) $\varphi(x * y) = \varphi(x) \square \varphi(y)$ pro každé $x, y \in S$

je-li $(S, *, e_s)$ a $(T, \square, e_t)$ monoidy, pak
 izomorfismus pologrup $\Leftrightarrow$ izomorfismus monoidů
 iff $\varphi(e_s) = e_t$

je-li $(S, *, e_s)$ a $(T, \square, e_t)$ grupy, pak φ $\Leftrightarrow$ grupový
 izomorfismus iff navíc $\varphi(x^{-1}) = (\varphi(x))^{-1}$

Twzení: Je-li φ izomorfismus pologrupy $(S, *)$ na $(T, \square)$
 (monoidu $(S, *, e_s)$ na $(T, \square, e_t)$, grupy
 $(S, *, e_s)$ na grupu $(T, \square, e_t)$), pak
 $\varphi: T \rightarrow S$ $\Leftrightarrow$ izomorfismus pologrup (monoidů,
 grup)

$$\varphi^{-1}(a \square b) \stackrel{?}{=} \varphi^{-1}(a) * \varphi^{-1}(b)$$

$$\begin{aligned} \varphi^{-1}(a) = x & \quad \text{iff} \quad a = \varphi(x) \\ \varphi^{-1}(b) = y & \quad \text{iff} \quad b = \varphi(y) \end{aligned}$$

$$\varphi \text{ $\Leftrightarrow$ izomorfismus} \quad \varphi(x * y) = \varphi(x) \square \varphi(y) =$$

$$= a \square b$$

$$\text{iff} \quad x * y = \varphi^{-1}(a \square b) = \varphi^{-1}(a) * \varphi^{-1}(b)$$

$$\varphi(e_s) = e_t \quad \varphi^{-1}(e_t) = e_s$$

Máme dvě pologrupy $(S, *)$ a $(T, \square)$. Zobrazení

$\varphi: S \rightarrow T$ je homomorfismus pologrup iff

$$\forall x, y \in S \quad \varphi(x * y) = \varphi(x) \square \varphi(y)$$

je-li navíc $\varphi(e_S) = e_T$, mluvíme o homomorfismu monoidů

Průběh je-li $\varphi: S \rightarrow T$ homomorfismus monoidů

$$\varphi(S, *, e_S) \rightarrow (T, \square, e_T)$$

pak $\varphi(x^{-1}) = (\varphi(x))^{-1}$ pro každé $x \in S$, kde x^{-1} existuje

$$\text{D.} \quad x * x^{-1} = e_S = x^{-1} * x$$

$$\varphi(x * x^{-1}) = \varphi(e_S) = \varphi(x^{-1} * x)$$

$$\varphi(x) \square \varphi(x^{-1}) = e_T = \varphi(x^{-1}) \square \varphi(x)$$

$$\text{iff } \varphi(x^{-1}) = (\varphi(x))^{-1}$$

Pr $(A^*, \cdot)$ A^* je množina všech slov nad A je křesleni

$(A^+, \cdot)$ A^+ je $\text{---} \parallel \text{---}$ sepradnyj $\text{---} \parallel \text{---}$

$$A = \{0, 1\} \quad (\mathbb{Z}, +)$$

$$f: \{0, 1\} \rightarrow \mathbb{Z} \quad f(0) = i \quad f(1) = j$$

$$\varphi(0) = f(0) = i \quad \varphi(1) = f(1) = j$$

$$\varphi(01) = \varphi(0) + \varphi(1) = i + j$$

$$\varphi(010) = \varphi(01) + \varphi(0) = \varphi(0) + \varphi(1) + \varphi(0) = 2 \cdot i + j$$

$$\varphi(011010) = 3 \cdot \varphi(0) + 4 \cdot \varphi(1) = 3i + 4j$$

μ μ_0 - počet 0 ve slově μ μ_1

1

$$\varphi(\mu) = \mu_0 i + \mu_1 j$$

Twicken: Je-li $(S, \otimes)$ pologrupa ($(S, \otimes, \varepsilon)$ monoid),
 pak pro každé zobrazení $f: A \rightarrow S$ existuje
 právě jeden homomorfismus $\varphi: (A^+, \cdot) \rightarrow (S, \otimes)$
 ($\varphi: (A^*, \cdot, \varepsilon) \rightarrow (S, \otimes, \varepsilon)$) takové, že
 $\varphi(a) = f(a)$ pro každé $a \in A$

$1. \varphi(\varepsilon) = \varepsilon$ $\varphi(a) = f(a)$ $2. \varphi(\mu a) = \varphi(\mu) \otimes \varphi(a)$		$A^* \quad 1) \varepsilon \in A^*$ $a \in A^* \text{ pro } a \in A$ $2) \text{ if } \mu \in A^+, \text{ pak } \mu a \in A^* \text{ pro } a \in A$
---	--	---

To je důvod, proč $(A^+, \cdot)$ je volná pologrupa,
 $(A^*, \cdot, \varepsilon)$ volný monoid nad A

show that

1. pred. logika
2. instance
3. relace (sluč, shled)
4. syst. třídy
5. pologrupy...
6. diferenciální rovnice

12

Okruchy, tělesa

$\mathbb{R}, \mathbb{Q}, \boxed{\mathbb{Z}}, \mathbb{C}$

$(\mathbb{Z}, +, \cdot)$

- (i) $(\mathbb{Z}, +)$ je komutativní grupa, neutrální prvek 0
 $a + 0 = a$ pro každé $a \in \mathbb{Z}$
 pro každé a existuje $-a$ tak, že $a + (-a) = 0$
- (ii) $(\mathbb{Z}, \cdot)$ je komutativní monoid, jednotkový prvek 1, tj. $1 \cdot a = a \cdot 1$
- (iii) pro každé $a, b, c \in \mathbb{Z}$ platí $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
 $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

Def: Okruch s jednotkou je $(R, +, \cdot)$, $+, \cdot$ jsou binární operace, s prvky 0, 1 tak, že

- (i) $(R, +, 0)$ je komutativní grupa
- (ii) $(R, \cdot, 1)$ je monoid
- (iii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ pro každé $a, b, c \in R$

Př. ~~1.1~~ $M_{n,n}$ - číselné matice řádu n , $+, \cdot, 0, \mathbb{E}$

2) $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n, \mathbb{Q}$

není okruh: $(\mathbb{N}, +, \cdot)$ $(\mathbb{N}, +)$ není grupa

komutativní okruh je okruh, kde násobení je komutativní

2)

Def.: Těleso je komutativní okruh $(R, +, \cdot)$ s jednotkou,

kteří navíc splňuje:

(i) pro každé $a \neq 0$ existuje inverzní prvek $a^{-1} \in R$ tak, že $a^{-1}a = 1$

(ii) $0 \neq 1$

Př.: $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ p. prvočíslo, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

Platí: V každém okruhu $(R, +, \cdot)$ platí

1) $a \cdot 0 = 0$ pro každé a

$$(a(b+1) = a \cdot 1 \quad a \cdot 0 + a \cdot 1 = a \cdot 1 \quad a \cdot 0 = 0)$$

2) $a \cdot (-1) = -a$

$$\left(\begin{array}{l} 1 + (-1) = 0 \quad a \cdot 1 + a \cdot (-1) = 0 \quad a + a(-1) = 0 \\ -a = a(-1) \end{array} \right)$$

Máme konečné těleso $(F, +, \cdot, 0, 1)$ F je konečná množina

$1 \in F$, $1+1$, $1+1+1$, $1+1+1+1$, ..., $\underbrace{1+1+\dots+1}_{n\text{-krát}}$, ...

musí existovat n, k tak, že $n+k$

$$\underbrace{1+1+\dots+1}_{n\text{-krát}} = \underbrace{1+1+\dots+1}_{k\text{-krát}} \quad k < n$$

$$\underbrace{1+1+\dots+1}_{(n-k)\text{-krát}} = 0$$

Platí: Nejmenší číslo p , pro které $1+1+\dots+1=0$ je prvočíslo.

Kdyby $p = n \cdot s$

$$\underbrace{(1+\dots+1)}_{n \text{ krát}} \cdot \underbrace{(1+\dots+1)}_{s \text{ krát}} = \underbrace{1+1+\dots+1}_{n \cdot s \text{ krát}} = 0 \Rightarrow \begin{matrix} 1+1+\dots+1=0 \\ n \text{ krát} \\ \hline 1+1+\dots+1=0 \\ s \text{ krát} \end{matrix}$$

$$n=p, s=1$$

$$s=p, n=1$$

p je prvočíslo

Toto prvočíslo p se nazývá charakteristika konečného tělesa $(F, +, \cdot, 0, 1)$

Máme obecně $(R, +, \cdot, 0, 1)$. Prvky $a, b \in R$ nazýváme dělitele nuly, iff $a \neq 0, b \neq 0$ a $a \cdot b = 0$

Př. $(\mathbb{Z}_m, +, \cdot, 0, 1)$. m složené $m = n \cdot s, n < m, s < m$,
pak $n \cdot s = 0$

Žádné těleso nemá dělitele 0.

Polynomy nad $(\mathbb{Z}_p, +, \cdot, 0, 1)$ p prvočíslo

je výraz $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ $a_i \in \mathbb{Z}_p$

$\text{st}(p)$ největší n , ke $a_n \neq 0$, nulový polynom $p(x)=0$ má st. roven -1

Dva polynomy jsou stejně iff mají stejný stupeň a koeficienty u stejných mocnin se rovnají.

Polynomy umíme sčítat, odčítat, násobit.

$$\deg(p \pm q) \leq \max(\deg p, \deg q)$$

$$\deg(p \cdot q) = \deg p + \deg q$$

pro $p \neq 0, q \neq 0$

Věta o dělení

Pro každé dva polynomy $p(x)$ a $g(x)$, $g(x) \neq 0$, existují polynomy $d(x)$, $r(x)$ jednoznačně tak, že

$$p(x) = d(x) \cdot g(x) + r(x), \quad \deg r < \deg g$$

Překneme, že polynom $g(x)$ dělí $p(x)$ iff $r(x) = 0$

Číslo $a \in \mathbb{Z}_p$ je kořen polynomu $p(x)$ iff $p(a) = 0$

Věta: Číslo $a \in \mathbb{Z}_p$ je kořen polynomu $p(x)$ iff $p(x)$ je dělitelné $(x-a)$

$$D.: p(x) = d(x)(x-a) + r(x) \quad \deg r < 1, \quad r(x) = r_0$$

$$p(x) = d(x)(x-a) + r_0$$

$$p(a) = d(a) \cdot \underbrace{(a-a)}_0 + r_0$$

$$p(a) = r_0$$

Věta: Každý polynom stupně $n \geq 1$ má nejvýš n kořenů počítáno i s jejich násobností.

Def. Polynom $p(x)$ nazveme ireducibilnīm polynomem iff
 pastāv $p(x) = r(x) \cdot s(x)$, $\deg r = \deg p$ nebo $\deg s = \deg p$

Vēl. Pro katrē n eksistē ireducibilnī polynom $\text{st} p = n$ $\mathbb{Z}_p$

(13)

spoleinī delitel polynomu $p(x), q(x)$ ir kopīg polynom $d(x)$,
 $d(x) \text{ del } p(x), d(x) \text{ del } q(x)$

Nejvairāk spēkā ir kopīg delitel nejvairāk spēkā

$$d(x) \mid p(x) \quad d(x) \mid q(x) \quad \underline{k \cdot d(x)} \quad k \neq 0 \quad k \in \mathbb{Z}_p$$

$$p(x) = a(x) \cdot d(x)$$

$$q(x) = b(x) \cdot d(x)$$

$$p(x) = (k^{-1} a(x)) \cdot (k \cdot d(x))$$

$$q(x) = (k^{-1} b(x)) \cdot (k \cdot d(x))$$

Eukleidovs algoritms pro maksimālā spēkā delitelē

Kāpēc $p(x), q(x) \text{ mod } \mathbb{Z}_p$

$$1. \text{ if } \deg p \geq \deg q, \text{ then } u(x) = p(x); v(x) = q(x)$$

$$\text{else } u(x) = q(x); v(x) = p(x)$$

$$2. \text{ apdēlīme } u(x) = t(x) \cdot v(x) + z(x)$$

$$3. \text{ if } z(x) = 0 \text{ (} k \text{ ir nulavī polynom)}$$

$$\text{then } \gcd(p(x), q(x)) = v(x)$$

$$\text{else } u(x) = v(x); v(x) = z(x) \text{ a jmp 2}$$

Bézoutova věta: Pro každé dva polynomy $p(x)$ a $g(x)$ existují polynomy $a(x), b(x)$ (nad $\mathbb{Z}_p$) tak, že

$$p(x) \cdot a(x) + g(x) \cdot b(x) = d(x)$$

$$\text{kde } d(x) = \gcd(p(x), g(x)).$$

Pr. Máme daný polynom $p(x) = x^2 + x^4 + x^3 + x^2 + x + 1$,
 $g(x) = x^3 + x^2 + x + 1$ nad $\mathbb{Z}_2$

Najděte $a(x), b(x)$ tak, aby

$$p(x) \cdot a(x) + g(x) \cdot b(x) = \gcd(p(x), g(x))$$

$$\begin{array}{r} (x^2 + x^4 + x^3 + x^2 + x + 1)(x^3 + x^2 + x + 1) = x^4 + x^3 + x + 1 \\ \underline{x^2 + x^6 + x^5 + x^4} \\ x^6 + x^5 + x^3 + x^2 + x + 1 \\ \underline{x^6 + x^5 + x^4 + x^3} \\ x^4 + x^2 + x + 1 \\ \underline{x^4 + x^3 + x^2 + x} \\ x^3 + x \\ \underline{x^3 + x^2 + x + 1} \\ x^2 + x \end{array}$$

$$(1) \quad p(x) = (x^4 + x^3 + x + 1) \cdot g(x) + \underbrace{(x^2 + x)}_{h(x)}$$

$$\begin{array}{r} (x^3 + x^2 + x + 1) : (x^2 + x) = x \\ \underline{x^3 + x^2} \\ x + 1 \end{array}$$

$$(2) \quad g(x) = x \cdot h(x) + (x + 1)$$

$$(x^2 + x) : (x + 1) = x$$

$$h(x) = x(x + 1) + 0$$

$$\underline{\gcd(p, g) = (x + 1)}$$

$$(1) \quad h(x) = p(x) + (x^4 + x^3 + x + 1) \cdot g(x)$$

$$(2) \quad (x+1) = g(x) + x \cdot h(x)$$

$$(x+1) = g(x) + x \cdot (p(x) + (x^4 + x^3 + x + 1) \cdot g(x))$$

$$= \cancel{x \cdot p(x)} + (x^5 + x^4 + x^2 + x + 1) g(x)$$

$a(x) = x$ $b(x) = x^5 + x^4 + x^2 + x + 1$

Označme $\mathbb{Z}_p[x]$ množinu všech polynomů nad $\mathbb{Z}_p$

$$(\mathbb{Z}_p[x], +, \cdot, 0, 1)$$

je komutativní okruh s jednotkou, bez dělitele nuly.

Inverzní polynom existuje pouze pro polynomy stupně 0.

$$p(x) = k \neq 0 \text{ inverzní polynom } q(x) = k^{-1}$$

Není těleso

Diferenční rovnice

Př 1) Hanojské věže

$$T(n) = 2T(n-1) + 1 \quad T(1) = 1$$

$$\{T(n)\}_{n=1}^{\infty}$$

2) Strassenův algoritmus:

$$P(2^n) = 7 \cdot P(2^{n-1}) \quad P(2^0) = 1$$

$$a_n = P(2^n)$$

$$a_n = 7a_{n-1} \quad a_0 = 1$$

$$\{a_n\}_{n=0}^{\infty}$$

Kladná posloupnost, aby splňovala předpoklady

→ k vynásobení 2 matic řádu 2^n
stačí 7 násobení 2 matic řádu 2^{n-1}

Diferenční lineární rovnice řádu k
s konstantními koeficienty

$$(*) \quad a_n + d_1 a_{n-1} + d_2 a_{n-2} + \dots + d_k a_{n-k} = b_n$$

Kde $d_1, d_2, \dots, d_k \in \mathbb{R}$, $d_k \neq 0$, $\{b_n\}$ je posloupnost

Řešení je posloupnost $\{a_n\}$, tak, že po dosazení dostaneme rovnost

řidružená homogenní rovnice

$$(**) a_n + d_1 a_{n-1} + \dots + d_k a_{n-k} = 0$$

Řešení (**)

1) pokud-li $\{x_n\}, \{y_n\}$ řešení (**), pak $\{x_n\}, \{x_n + y_n\}$ jsou opět řešení (**)

$$\text{Ktme, že } x_n + d_1 x_{n-1} + \dots + d_k x_{n-k} = 0$$

$$y_n + d_1 y_{n-1} + \dots + d_k y_{n-k} = 0$$

$$\begin{aligned} (l \cdot x_n) + d_1 (l \cdot x_{n-1}) + \dots + d_k (l \cdot x_{n-k}) &= l \cdot \overbrace{(x_n + d_1 x_{n-1} + \dots + d_k x_{n-k})}^0 = \\ &= l \cdot 0 = 0 \end{aligned}$$

$$(x_n + y_n) + d_1 (x_{n-1} + y_{n-1}) + \dots + d_k (x_{n-k} + y_{n-k}) =$$

$$= (x_n + d_1 x_{n-1} + \dots + d_k x_{n-k}) + (y_n + d_1 y_{n-1} + \dots + d_k y_{n-k}) =$$

$$= 0 + 0 = 0$$

2) Předpokládáme řešení $\{L^n\}_{n=0}^{\infty}$

$$L^n + d_1 L^{n-1} + d_2 L^{n-2} + \dots + d_k L^{n-k} = 0 \quad / : L^{n-k} \quad L \neq 0$$

$$\underline{L^k + d_1 L^{k-1} + \dots + d_k = 0} \quad \text{charakteristická rovnice (**)}$$

Každý kořen charakteristické rovnice dává řešení $\{L_0^n\}$

Když L_0 je dvojnásobný kořen, $\{n \cdot L_0^n\}$ je řešení

$$\frac{d}{d\lambda}$$

$$n \cdot \lambda^{n-1} + d_1(n-1)\lambda^{n-2} + \dots + d_k(n-k)\lambda^{n-k-1} = 0 \quad | \cdot \lambda$$

$$n \lambda_0^n + d_1(n-1)\lambda_0^{n-1} + \dots + d_k(n-k)\lambda_0^{n-k} = 0$$

$\{n\lambda_0^n\}$ je řešením (**)

Je-li λ_0 kořen char. rovnice násobnosti k , má (**)

řešení $\{\lambda_0^n\}, \{n\lambda_0^{n-1}\}, \{n^2\lambda_0^{n-2}\}, \dots, \{n^{k-1}\lambda_0^{n-k+1}\}$

Abychom k obecnému řešení uřídili jedno, potřebujeme k počátečním podmínkám $a_0, a_1, a_2, \dots, a_{k-1}$

Pr. Najděte obecné řešení

$$a_n + 2a_{n-1} - 7a_{n-2} + 4a_{n-3} = 0$$

$$\lambda^3 + 2\lambda^2 - 7\lambda + 4 = 0$$

$$\begin{array}{r|rrrr} & 1 & 2 & -7 & 4 \\ (\lambda-1) & 1 & 1 & 3 & -4 \\ \hline & 1 & 3 & -4 & 0 \end{array}$$

$$(\lambda-1)(\lambda^2 + 3\lambda - 4) = 0$$

$$\lambda_{1,2} = 1$$

$$(\lambda-1)(\lambda+4)(\lambda-1) = 0$$

$$\lambda_3 = -4$$

$$\{1^n\} = \{1\}_{n=0}^\infty \quad \{n \cdot 1^{n-1}\} = \{n\} \quad \{(-4)^n\}$$

$$\{a_n\} = \alpha \{1\} + \beta \{n\} + \gamma \{(-4)^n\}$$

$$\underline{a_n = \alpha + \beta n + \gamma (-4)^n}$$

počáteční podmínky

$$a_0 = 0, a_1 = -5, a_2 = 15$$

$$\alpha + \beta = 0$$

$$\alpha + \beta + \gamma = -5$$

$$\alpha + 2\beta + 4\gamma = 15$$

$$\gamma = 1 \quad \beta = 0 \quad \alpha = -1$$

$$\underline{a_n = -1 + (-4)^n}$$

Řešení (**) má 1 komplexní kořen

Př.: $a_n = 2a_{n-1} - 2a_{n-2}$

Najděte obecné řešení

Řeš: $a_n - 2a_{n-1} + 2a_{n-2} = 0$

char. rovnice $\lambda^2 - 2\lambda + 2 = 0 \quad (\lambda - 1)^2 = -1$

$$\lambda_{1,2} = 1 \pm i$$

$$\{x_n\} = \{(1+i)^n\}_{n=0}^{\infty}$$

$$\{y_n\} = \{(1-i)^n\}_{n=0}^{\infty}$$

$$\lambda_{1,2} = 1 \pm i = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \left(\pm \frac{\pi}{4} \right) \right)$$

$$\left(\sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \left(\pm \frac{\pi}{4} \right) \right) \right)^n$$

$$= (\sqrt{2})^n \left(\cos n \frac{\pi}{4} + i \sin \left(\pm n \frac{\pi}{4} \right) \right)$$

$$\{x_n\} = \left\{ \sqrt{2}^n \left(\cos n \frac{\pi}{4} + i \sin n \frac{\pi}{4} \right) \right\}$$

$$\{y_n\} = \left\{ \sqrt{2}^n \left(\cos n \frac{\pi}{4} - i \sin n \frac{\pi}{4} \right) \right\}$$

$$x_n = \sqrt{2}^n \cdot \left(\cos n \frac{\pi}{4} + i \sin n \frac{\pi}{4} \right)$$

$$y_n = \sqrt{2}^n \cdot \left(\cos n \frac{\pi}{4} - i \sin n \frac{\pi}{4} \right)$$

$$\frac{x_n + y_n}{2} = \sqrt{2}^n \cos n \frac{\pi}{4}$$

$$\frac{x_n - y_n}{2} = \sqrt{2}^n \sin n \frac{\pi}{4}$$

$$\{\sqrt{2}^n \cos n\frac{\pi}{4}\}_{n=0}^{\infty}, \{\sqrt{2}^n \sin n\frac{\pi}{4}\}_{n=0}^{\infty}$$

$$\underline{a_n = \alpha \cdot \sqrt{2}^n \cos n\frac{\pi}{4} + \beta \sqrt{2}^n \sin n\frac{\pi}{4}} \quad \alpha, \beta \in \mathbb{R}$$

Má-li charakteristická rovnice kořen $\lambda_1 = a + ib$,
má i kořen $\lambda_2 = a - ib$,

pak $\{\lambda_1^n\}, \{\lambda_2^n\}$ jsou komplexní řešení (**)

$$a + ib = r \cdot (\cos \varphi + i \sin \varphi) \quad r = \sqrt{a^2 + b^2} \quad \text{dg } \varphi = \frac{b}{a}$$

$$\text{Tedy } \{x_n\} = \{r^n (\cos n\varphi + i \sin n\varphi)\}$$

$$\{y_n\} = \{r^n (\cos n\varphi - i \sin n\varphi)\} \text{ jsou řešení (**)}$$

$$\text{Proto } \left\{ \frac{x_n + y_n}{2} \right\} = \{r^n \cos n\varphi\}, \left\{ \frac{x_n - y_n}{2} \right\} = \{r^n \sin n\varphi\}$$

jsou řešení (**)

Rěšení nehomogenní (*)

Platí: 1) jsou-li $\{x_n\}, \{y_n\}$ řešení (*), pak $\{x_n\} - \{y_n\} =$
 $= \{x_n - y_n\}$ je řešení (**).

$$\text{Ano, } x_n - y_n + d_1(x_{n-1} - y_{n-1}) + d_2(x_{n-2} - y_{n-2}) + \dots + d_k(x_{n-k} - y_{n-k}) =$$

$$= (x_n + d_1 x_{n-1} + d_2 x_{n-2} + \dots + d_k x_{n-k}) - (y_n + d_1 y_{n-1} + \dots + d_k y_{n-k}) =$$

$$= b_n - b_n = 0$$

2) Je-li $\{x_n\}$ řešení (*) a $\{u_n\}$ řešení (**), pak
 $\{x_n\} + \{u_n\} = \{x_n + u_n\}$ je řešení (*)

$$\begin{aligned}
 a_{n0}, \quad x_n + u_n + d_1(x_{n-1} + u_{n-1}) + \dots + d_k(x_{n-k} + u_{n-k}) &= \\
 &= \underbrace{(x_n + d_1 x_{n-1} + \dots + d_k x_{n-k})}_{b_n} + \underbrace{(u_n + d_1 u_{n-1} + \dots + d_k u_{n-k})}_0 \\
 &= b_n + 0 = b_n
 \end{aligned}$$

3) Je-li $\{a_n\}$ jedno pevně zvolené řešení $(*)$,
pak pro každé řešení $\{x_n\}$ $(*)$ platí

$$\{x_n\} = \{a_n\} + \underbrace{\{x_n - a_n\}}_{\text{řes } (**)}$$

Jinými slovy: obecné řešení rovnice $(*)$ dostaneme
jako součet: jedno řešení $(*)$ + obecné řešení $(**)$.

Pro $b_n = p(n) \cdot \lambda^n$ kde $p(n)$ je polynom, je
odhad $\hat{a}_n = q(n) \cdot n^l \cdot \lambda^n$, kde q je obecný polynom
stejného stupně jako p , l je násobnost λ jako kořene
charakteristické funkce.

Pr 1: Řešte

$$a_n = 2a_{n-1} - a_{n-2} + 2 + 2^n$$

$$a_0 = 1 \quad a_1 = 4$$

$$a_n - 2a_{n-1} + a_{n-2} = 2 + 2^n$$

homogenní

$$a_n - 2a_{n-1} + a_{n-2} = 0$$

$$\lambda^2 - 2\lambda + 1 = 0$$

$$(\lambda - 1) = 0$$

$$\lambda_{1,2} = 1$$

$$\{1^n\} \quad \{n \cdot 1^n\}$$

$$\tilde{a}_n = \alpha + \beta \cdot n$$

nehomogenní

$$2 \cdot 1^n \dots \hat{a}_n^1 = A \cdot n^2 \cdot 1^n = A n^2$$

$$A n^2 - 2 \cdot A \cdot (n-1)^2 + A \cdot (n-2)^2 = 2$$

$$A n^2 - 2 A n^2 + 4 A n - 2 A + A n^2 - 4 A n + 4 A = 2$$

$$2A = 2$$

$$\underline{A = 1}$$

$$\underline{\hat{a}_n^1 = n^2}$$

$$1 \cdot 2^n \dots \hat{a}_n^2 = B \cdot 2^n$$

$$\cancel{B \cdot 2^n} - 2 \cdot \cancel{B \cdot 2^{n-1}} + B \cdot 2^{n-2} = 2^n \quad / : 2^{n-2}$$

$$\underline{B = 4}$$

$$\hat{a}_n^2 = 4 \cdot 2^n = 2^{n+2}$$

$$\hat{a}_n = n^2 + 2^{n+2}$$

$$a_n = n^2 + 2^{n+2} + \alpha + \beta n \dots \text{obecné řešení rovnice}$$

$$n=0 \quad 1 = \alpha + 4 \quad \alpha = -3$$

$$n=1 \quad 4 = 1 + 8 + \alpha + \beta \quad \beta = -2$$

$$\underline{a_n = n^2 + 2^{n+2} - 3 - 2n}$$

Pr: Reihe, $a_n + a_{n-1} - 2a_{n-2} = 6n + 2$

$$a_0 = 1$$

res. homogen

$$a_1 = 2$$

$$a_n + a_{n-1} - 2a_{n-2} = 0$$

$$\lambda^2 + \lambda - 2 = 0 \quad (\lambda + 2)(\lambda - 1) = 0 \quad \lambda_1 = 1, \lambda_2 = -2$$

$$\tilde{a}_n = \alpha + \beta(-2)^n \quad \alpha, \beta \in \mathbb{R}$$

$$(6n+2) \cdot 1^n \quad \hat{a}_n = (A_n + B) n^1 \cdot 1^n = \underline{A n^2 + B n}$$

$$A n^2 + B n + A(n-1)^2 + B(n-1) - 2(A(n-2)^2 + B(n-2)) = 6n + 2$$

$$\cancel{A n^2 + B n} + \cancel{A n^2} - \cancel{2A n} + \cancel{A} + \cancel{B n} - \cancel{B} - \cancel{2A n^2} + \cancel{4A n} - \cancel{2A} - \cancel{2B n} + \cancel{4B} = 6n + 2$$

$$6A n - 7A + 3B = 6n + 2$$

$$n^1: \quad 6A = 6$$

$$A = 1$$

$$n^0: \quad -7A + 3B = 2$$

$$B = 3$$

$$\hat{a}_n = n^2 + 3n$$

$$a_n = n^2 + 3n + \alpha + \beta(-2)^n$$

$$n=0: \quad 1 = \alpha + \beta$$

$$n=1: \quad 1 = 1 + 3 + \alpha - 2\beta$$

$$\alpha + \beta = 1$$

$$\alpha - 2\beta = -2$$

$$\alpha + \beta = 1$$

$$-3\beta = -3$$

$$\beta = 1$$

$$\alpha = 0$$

$$\underline{\underline{a_n = n^2 + 3n + (-2)^n}}$$