

<http://moth.feld.cvut.cz/velebie> - text přednášek, skripta
 Matematická logika - (predikátová logika)

MATEMATICKÁ INDUKCE

Standardní model přirozených čísel

1. 0 nula je přirozené číslo
2. Když n je přirozené číslo, pak $n+1$ je přirozené číslo
3. Každé přirozené číslo vzniklo konečným použitím těchto pravidel.

Na těchto přiroz. číslech je dáno uspořádání $n < n+1$ (ostře uspořádání)

- (1) Uspořádání je lineární - tj. pro lib. $a, b \in \mathbb{N}$ platí buď $a < b$ nebo $b < a$ nebo $a = b$.
 - (2) Každá neprázdná podmnožina $A \subseteq \mathbb{N}$ má v tomto uspořádání nejmenší prvek, tj. $a \in A$ takové, že $a < b$ pro všechna $b \in A$, $a \neq b$.
- U dobrého uspořádání platí (1) a (2).

Princip slabé indukce

V - vlastnost pro přirozená čísla

- Jestliže
1. $n_0 \in \mathbb{N}$ má vlastnost V (základní krok - vlastnost V má určitě n_0)
 2. kdyby nějaké $m \geq n_0$ mělo vlastnost V, pak by také $m+1$ mělo vlastnost V. (indukční krok - přenos vlastnosti z m na $m+1$)
- pak platí: všechna $n \geq n_0$ mají vlastnost V.

Použití: Dokažte $(1+x)^n \geq 1+nx$, $x \geq 0$, $x \in \mathbb{R}$, pro všechna $n \geq 1$

Důkaz slabou indukcí: 1. $n=1$, $(1+x)^1 \geq 1+1x$... platí rovnost

2. indukční předpoklad - pro nějaké $m \geq 1$ je $(1+x)^m \geq 1+mx$,
 chci dokázat $(1+x)^{m+1} \geq 1+(m+1)x$,

DEKOMPOZICE - rozložením výrazu pro $m+1$ na výraz pro m a zbytek,
 abych mohl použít indukční předpoklady.

$$(1+x)^{m+1} = (1+x)^m \cdot (1+x) \underset{(i.p.)}{\geq} (1+mx)(1+x) = 1+mx+x+mx^2 = 1+(m+1)x + mx^2 \geq 1+(m+1)x$$

princip slabé indukce:

pro všechny $n \geq 1$ platí daná nerovnost

Princip silné indukce

2

Jestliže platí: 1. n_0 má danou vlastnost V

2. kdyby platilo pro nějaké $n \geq n_0$ měly všechny k :

$n_0 \leq k \leq n$ vlastnost V , pak by také $n+1$ mělo vlastnost V .

potom vš. $n \geq n_0$ mají vlastnost V .

Použití: Každé $n \geq 2$ má prvočíselný rozklad, tj. $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$,
kde $p_1 < p_2 < \dots < p_r$ jsou prvočísla, $k_i \in \mathbb{N}$, $r \geq 1$, $r \in \mathbb{N}$

Důkaz silnou indukcí:

1. $n=2$ $2=2^1$ triviální rozklad

2. indukční předp. - všedna $k: 2 \leq k \leq m$ mají prvočíselný rozklad, abychom našli rozklad pro $m+1$

rozklad $\left\{ \begin{array}{l} \text{buď } m+1 = p \rightarrow \text{je prvočíslo (triv. rozklad)} \\ \text{nebo } m+1 = a \cdot b, \text{ kde } a, b \in \{1, m+1\} \text{ jsou vlastní} \\ \text{dělitele } m+1, 2 \leq a \leq b \leq m \\ \text{i. p. } a = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}, b = p_1^{k_1} \cdot \dots \cdot p_r^{k_r} \end{array} \right.$

Zde by nestačil předpoklad pro sloboou indukci v dekompozici nemí m , ale čísla $a, b \leq m$.

$m+1 = \left(\prod_1^r p_i^{k_i} \right) \cdot \left(\prod_1^s q_i^{k_i} \right)$, dáme dohromady stejná prvočísla a získáme rozklad pro $m+1$

Princip silné indukce zaručuje všedna $n \geq 2$ mají prvorozklad

Tvzení: Z principu silné indukce plyne vlastnost slobe' indukce.

Důkaz: Předpokládáme - silná indukce funguje

Chci dokázat platnost slobe' ind. - implikace (1. a 2.) \Rightarrow všedna $n_0 \geq n_0$ mají V .

Dokazují implikaci = vyjde z $\alpha \Rightarrow \Rightarrow \Rightarrow \beta$

$\alpha \Rightarrow \beta$

Tedy platí α : 1. n_0 má V

2. když m má V , pak $m+1$ má V

Použijeme pro dokázání β silnou indukci, takže musíme odvodit, zda platí 1. a 2. pro silnou indukci.

1. silné - stejné jako 1. slobe' \rightarrow platí

2. Když vš. $k: n_0 \leq k \leq m$ měla $V \stackrel{?}{\rightarrow}$ pak by $m+1$ mělo V

Z předp. slobe' ind. lze odvodit platnost předpokladu 1., 2. pro silnou indukci a o ní vím, že funguje, tedy z předp. 1., 2. odvodí $\forall n \geq n_0$ platí V_0 .

Tvrzení: Ze slabé indukce plyne platnost silné indukce

Důkaz: Vezmu předpis 1., 2. pro silnou indukci, tj.

1. n_0 má vlastnost V
2. přenosnost V ze všech $k: n_0 \leq k \leq m$, na $m+1$

Odvodíme, že platí předpoklady pro slabou ind. a použijeme je

1. n_0 má V - stejně jako u silné
2. přenosnost V z m na $m+1$

Sporem: Necht' exist m , které má V , ale $m+1$ nemá V

Vezmu $A \subseteq \{n_0, \dots, m+1\}$

$$A = \{k; n_0 \leq k \leq m+1; k \text{ nemá } V\} \neq \emptyset$$

A - konečná, neprázdná množina přiroz. čísel \rightarrow má nejmenší prvek - označíme ho s .

platí: všechna $k: n_0 \leq k \leq (s-1)$ mají $V \xrightarrow{\text{dle 2.}} s$ má V - spor!

Platí předpis 1., 2. pro slabou indukci $\xrightarrow[\text{funguje}]{\text{silné ind.}}$ vš. $n \geq n_0$ n má V

Princip dobrého uspořádání

Každá (konečná i nekonečná) neprázdná podmnožina přiroz. čísel má nejmenší prvek.

Tvrzení: Z principu dobrého uspořádání plyne princip silné indukce.

Důkaz: 1. n_0 má V

2. Když všechna $k, n_0 \leq k \leq m$ mají V , pak $m+1$ má V .

Chci dokázat, že všechna $n \geq n_0$ mají V .

Sporem: existuje n , které nemá vlastnost V

$$A = \{n \geq n_0, n \text{ nemá } V\} \neq \emptyset \xrightarrow[\text{uspořád}]{\text{dobře}} A \text{ má nejmenší}$$

prvek, označím s , vš. $k: n_0 \leq k \leq (s-1)$ mají $V \rightarrow$

$\rightarrow s$ má V ... spor! Tedy $A = \emptyset$

Tvrzení: Ze silné indukce plyne princip dobrého uspořádání.

Důkaz: Ukážeme, že A , která nemá nejmenší prvek, je prázdná, aneb $N \setminus A = N$

V ... n není v množině A

Silnou indukci: 1. $0 \notin A$... kdyby $0 \in A$, byla by 0 nejmenší prvek

2. Když vš. $k, 0 \leq k \leq m, k \notin A \rightarrow m+1 \notin A$

jinak by $m+1$ bylo nejmenší

Věta: Následující principy jsou ekvivalentní

1. Sloba indukce.
2. Silná indukce.
3. Dobré uspořádání na \mathbb{N} .

11.10.

Rekurzivní algoritmy a principy indukce

variant - velikost úlohy; rekurzivní algoritmus - pro min. velikost řeší úlohu přímo a pro větší velikost rozdělí úlohu na úlohy menší velikosti a volá rekurzi; totální korektnost - vždy skončí (= terminace) a když skončí tak dá správné řešení (= parciální korektnost)

Ověření totální korektnosti

- terminace - variant se při volání rekurze zmenšuje až na minimální velikost, která se řeší bez rekurze.
- parciální korektnost - slobou či silnou indukcí dle variantu

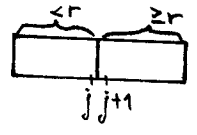
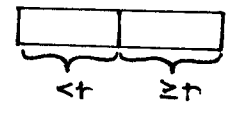
Př.: function FAC (n: integer) : integer

```
begin
  if n=0 then FAC := 1
  else FAC(n) := n * FAC(n-1)
end
```

1. Skončí - při volání rekurze se snižuje n → po n krocích pracuje nerekurzivně
 2. Spočte n! - slobou indukcí dle n
 1. n=0, FAC(0) = 1 = 0!
 2. I.p. pro n-1 spočte FAC(n-1) = (n-1)!
pro n > 0 else větev FAC(n) = n * FAC(n-1) = n * (n-1)! = n!
- $\forall n \geq 0, FAC(n) = n!$

Př.: procedure QUICKSORT (x1, ..., xk: real) - setřídí posl. čísel vzestupně (neklešajících)

```
begin
  if k=1 or x1 = x2 = ... = xk then STOP
  else urči median r = (xn + xm) / 2 pro xn ≠ xm
  rozdělí posloupnost na dvě části
    i:=1, j:=k
  repeat while xi < r do i:=i+1
    while xj >= r do j:=j-1
    zaměň xi a xj
    z:=xi; xi:=xj; xj:=z
  until j < i
  NYNÍ
  QUICKSORT (x1, ..., xj)
  QUICKSORT (xj+1, ..., xk)
end;
```



Ověření tot. korektnosti

1. terminace - rekurze je volaná na kratší posloupnosti, protože žádná ze dvou částí není prázdná - porovnáváme $r = \frac{x_n + x_m}{2}$, BÚNO $x_n < x_m$

2. parciální korektnost - alg. QUICKSORT setřídí čísla vzestupně

Důkaz silnou indukcí dle počtu čísel k

1. $k=1, \{x_1\}$ to je setříděná posloupnost

2. i.p. - pro vs. $l; 1 \leq l \leq k-1$ algoritmus setřídí vzestupně x_1, \dots, x_l

Pro k čísel, $k > 1$ - buď then větev, když $x_1 = x_2 = \dots = x_k \rightarrow$ SKONČÍ, $\{x_1, \dots, x_k\}$ je setříděná

nebo else větev \rightarrow rozdělí posl., obě posl. kratší než k, lze použít i.p.

i.p.: QUICKSORT (x_1, \dots, x_j) setřídí vzestupně

QUICKSORT (x_{j+1}, \dots, x_k) setřídí vzestupně

$[\bar{x}_1 \leq \bar{x}_2 \leq \dots \leq \bar{x}_j] < r \leq [\bar{x}_{j+1} \leq \dots \leq \bar{x}_k]$

\hookrightarrow zde je správná < nerovnost \rightarrow celá posloupnost je setříděná vzestupně

Silná indukce: $\forall k \geq 1$ alg. QUICK SORT setřídí x_1, \dots, x_k vzestupně

Induktivně zadané množiny, strukturální indukce

Př.: Backus - Naurova forma pro definování typu

typ - kladná přirozená čísla

$\langle \text{číslo} \rangle = 1 | 2 | 3 | \dots | 9 | \langle \text{číslo} \rangle 0 | \langle \text{číslo} \rangle 1 | \dots | \langle \text{číslo} \rangle 9 | \dots$

- 1. Nejmenší objekty typu $\langle \text{číslo} \rangle$ jsou 1, 2, ..., 9
- 2. Když už mám řetězec, který je číslem, tak za něj mohu připsat 0 (nebo 1, ..., 9) a znovu vytvořím číslo
- 3. Pravidla mohou být použita jenom konečněkrát.

Množiny dané induktivně

$\Sigma = \{a, b\}$ abeceda, Σ^* = množina všech slov (konečně dlouhých) nad abecedou Σ , včetně mezery = prázdného slova ϵ .

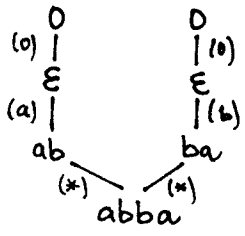
G gramatika - systém odvozovacích pravidel
pravidla $\left\{ \begin{array}{l} \text{axiomatická } \frac{}{\epsilon}^{(0)} \\ \text{deduktivní } \frac{w(a)}{awb}, \frac{w(b)}{bwa}, \frac{u, v}{uv}^{(*)} \end{array} \right.$

Jazyk L nad Σ je zadán induktivně pomocí gramatiky G, když každé slovo jazyka L vzniklo konečným počtem použití odvozovacích pravidel.

Př.: $abba \in L$?

$\frac{\frac{\epsilon^{(0)}}{ab}^{(a)} \quad \frac{\epsilon^{(0)}}{ba}^{(b)}}{abba}^{(*)}$

ODVOZOVACÍ STROM



graf je strom

Graf je strom - listy neobsazene; hrany od listu - ax. pravidla; ostatni hrany dedukt. pravidla; kořen - slovo které odvozujeme

Plati $w \in L \leftrightarrow$ ma odvozovací strom T_w

Zajima nas, zda by se množina slov L dala definovat neinduktivně - pomoci testovací vlastnosti.

Pro dokazování, že vs. slova generovaná gramatikou G mají nějakou vlastnost se používá strukturalní indukce.

Princip strukturalní indukce

Máme abecedu Σ a gramatiku G , L induktivně zadána množina slov pomocí G , V - vlastnost slov v Σ^* .

- Jestliže 1. slova z axiom. pravidel gramatiky G mají vlastnost V
 - 2. Všechna deduktivní pravidla splňují implikaci:
 Jestliže slova v předpoklodech splňují V , pak i to co lze odvodit splňuje V . (aneb deduktivní pravidla vlastnost V přenašejí)
- Potom všechna slova z L mají vlastnost V .

Důkaz: silnou indukci - dle výšky h odvozeného stromu (= max. počet hran mezi kořenem a listem)

- 1. $h=1$ $\frac{w}{w} \leftarrow w$ je odvozeno axiom. pravidlem \rightarrow dle předpokladu 1. strukt. ind. w má vlastnost V
- 2. i.p. - všechna slova w s indukčním stromem výšky $l: 1 \leq l \leq h-1$; w mají vlastnost V .

Vezmu libovolné w s odvozovacím stromem T_w výšky h .

$\frac{\{ \frac{w_i}{w_i} \dots \frac{w_k}{w_k} \}}{w}$ (poslední deduktivní pravidlo); slova w_1, \dots, w_k mají deduktivní strom maximálně výšky $h-1$

\rightarrow w_1, \dots, w_k mají vlastnost V i.p.

\rightarrow předpoklad 2. strukt. indukce - dedukt. prav. V zachovají $\rightarrow w$ má V

Silná indukce

$\forall h \geq 1$ w s odvozovacím stromem T_w výšky h má vlastnost V (A to jsou všechna slova z L).

Př.: $\Sigma = \{a, b\}$ $G: 1. \frac{}{\epsilon}$

2. $\frac{w}{awb}, \frac{w}{bwa}, \frac{u, v}{uv}$

Plati: $L = \{w, w \text{ odvozené gramatikou } G\} = T = \{w, \text{ stejně a-ček jako b-ček}\}$ $w_a = w_b$

- 1. $L \subseteq T$ strukturalní indukci
 - 1. $\epsilon, \epsilon_a = 0 = \epsilon_b$
 - 2. Když $w_a = w_b$, pak $(awb)_a = w_a + 1 = w_b + 1 = (awb)_b$ i.p.
 - Když $u_a = u_b, v_a = v_b$, pak $(uv)_a = u_a + v_a = u_b + v_b = (uv)_b$ i.p.
- 2. $T \subseteq L$ silnou indukci dle délky slova s V (nebo zde přes $u = w_a = w_b$)

Dělitelnost v \mathbb{N} a \mathbb{Z}

Věta: r dělní se zbytkem v \mathbb{Z}

Nechť $a, b \in \mathbb{Z}, b \neq 0$. Pak existuje jednoznačně $q, n \in \mathbb{Z}$, tak že

$$a = q \cdot b + n, 0 \leq n < |b|$$

Důkaz: existence (pro $a \geq b$) - indukcí dle a :

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

2. pro $a = k, a = q \cdot b + n, 0 \leq n < b,$

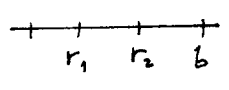
pak pro $a = k+1 \dots a+1 = q \cdot b + (n+1)$ $\left\{ \begin{array}{l} n+1 < b \rightarrow \text{hotovo } \bar{q} = q, \bar{n} = n+1 \\ n+1 = b \rightarrow a = qb + b = (q+1)b \end{array} \right.$

Jednoznačnost - sporem:

Nechť exist $(q_1, r_1) \neq (q_2, r_2), 0 \leq r_1, r_2 < b$

$$a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$$

BÚNO $r_2 \geq r_1, (q_1 - q_2) \cdot b = r_2 - r_1$



$$|(q_1 - q_2) \cdot b| = |r_2 - r_1| < b$$

↑ celočíselný násobek čísla b mezi $(0, b) \rightarrow 0$

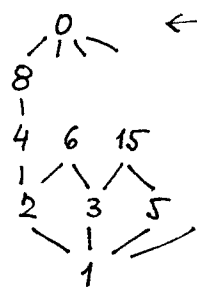
$$|(q_1 - q_2) \cdot b| = |r_2 - r_1| = 0 \rightarrow r_1 = r_2, q_1 = q_2, \text{ SPOR!}$$

Def.: Řekneme, že b dělí $a, b, a \in \mathbb{Z}$, když exist. $k \in \mathbb{Z}, a = k \cdot b$.

Značíme $b|a$.

Pozn.: Číselce $|$ je uspořádána na \mathbb{N} ,
a b nemí uspořádána na \mathbb{Z} .

(neplatí antisymetrie: $2|(-2), (-2)|2,$
ale $2 \neq (-2)$)



← 0 je největší prvek,
pozor, dle def. $0|0$

p prvočíslo

Def.: $a, b \in \mathbb{Z}$. Řekneme, že $d \in \mathbb{N}$ je největší společný dělitel pro a, b ,
jestliže 1. d je společný dělitel, tj. $d|a, d|b$
2. d je největší v uspořádání "děli", tj. když $c \equiv c|a, c|b$, pak $c|d$.

Např.: $24 = 2^3 \cdot 3; 42 = 2 \cdot 3 \cdot 7$

$$\text{gcd}(24, 42) = 2 \cdot 3 = 6 - \text{společná}$$

prvočíslo v maximální společné množině.

Značíme $\text{gcd}(a, b) = d$
greatest common divisor

Eukleidův algoritmus - pro $a, b (a \geq b \geq 0)$ najde $\text{gcd}(a, b)$

Př.: $\text{gcd}(198, 144)$

$$198 = 1 \cdot 144 + 54$$

$$144 = 2 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + \boxed{18}$$

$$36 = 2 \cdot 18 + 0$$

1. kdyby $a = b \cdot k + 0$, pak by $b = \text{gcd}(a, b)$

2. Platí: $a = q \cdot b + r, r > 0$. Dvojice a, b má stejné dělitele
jako dvojice $b, r \rightarrow$ když $c|a, c|b$ pak $r = a - q \cdot b =$
 $= c \cdot a_1 - q \cdot c \cdot b_1 = c(a_1 - q \cdot b_1) \rightarrow c|r$
když $c|b, c|r$ pak $a = q \cdot b + r, c$ dělí oba sčítance \rightarrow
 $c|a$

Jsou $(x, y) = (x_p, y_p) + t(x_0, y_0)$, kde $t \in \mathbb{Z}$ všechna celočíselná řešení?

Kdyby $t \in \mathbb{R}$ - získám všechna řešení v \mathbb{R}

Nemůže pro $t \in \mathbb{R} \setminus \mathbb{Z}$ ještě vzniknout $(x, y) \in \mathbb{Z}^2$?

ANO - $t = \frac{p}{q}$, kde q by dělil x_0, y_0

↑ Tomuto se lze vyhnout, když volím x_0, y_0 nesoudělné $x_0 = \frac{b}{\gcd(a, b)}$, $y_0 = \frac{-a}{\gcd(a, b)}$

Př.: Řešte v \mathbb{Z} : $198x + 144y = 54$

1. Euklidův algoritmus na 198, 144

$$\gcd(198, 144) = 18, \quad 18 \mid 54 \rightarrow \text{má to řešení v } \mathbb{Z}$$

2. (x_p, y_p)

$$\begin{aligned} \text{Bezoutova věta: } 18 &= 3 \cdot 198 - 4 \cdot 144 \rightarrow 54 = 3 \cdot 18 \cdot 3 = 3 \cdot (3 \cdot 198 - 4 \cdot 144) = \\ &= 9 \cdot 198 - 12 \cdot 144 \end{aligned}$$

$$x_p = 9, \quad y_p = -12$$

3. Nesoudělné řešení homog. rovnice

$$198x + 144y = 0 \quad | : \gcd = 18$$

$$11x + 8y = 0, \quad x_0 = 8, \quad y_0 = -11$$

$$4. (x, y) = (9 + t \cdot 8, -12 - t \cdot 11), \quad t \in \mathbb{Z}$$

Prvočísla

Def.: Číslo $p > 1$ je prvočíslo, je-li dělitelné jen p a 1 . Když n není prvočíslo nazývá se složené číslo.

Tvrzení: Každé $n \geq 2$ má jednoznačný prvočíselný rozklad $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_n^{k_n}$, kde $p_1 < p_2 < \dots < p_n$ jsou prvočísla.

Důkaz: existence - silnou indukcí (viz dříve), jednoznačnost

Pomocné lemma: Když $c \mid a \cdot b$, c, a jsou nesoudělná, pak $c \mid b$.

Důkaz: Z Bezoutovy věty

$$\gcd(c, a) = 1 \rightarrow 1 = k \cdot c + l \cdot a, \quad k, l \in \mathbb{Z} \quad | \cdot b$$

$$b = k \cdot c \cdot b + l \cdot a \cdot b = c(n) \rightarrow c \mid b$$

$$n \in \mathbb{Z}$$

Důsledek: Když $c = p$ prvočís $p \mid a \cdot b$, pak $p \mid a$ nebo $p \mid b$.

Důkaz: Buď $p \mid a$ nebo $p \nmid a \rightarrow p, a$ nesoudělná $\rightarrow p \mid b$.

Indukcí - když prvočíslo p dělí součin k čísel, pak dělí jedno z nich.

Důkaz: Jednoznačnost prvočíselného rozkladu

Sporem: Necht' $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r} = q_1^{l_1} \cdot q_2^{l_2} \cdot \dots \cdot q_s^{l_s}$ - různé prvočís. rozklady

• buď existuje $p_i \neq q_i$ pro všechna $j = 1, \dots, s$.

$p_i \mid n \rightarrow p_i \mid (q_1^{l_1} \cdot \dots \cdot q_s^{l_s}) \xrightarrow{\text{lemma}} p_i \mid q_j$ dělí jedno z prvočísel, ale

q_i je prvočíslo \rightarrow dělí ho jen 1 a $q_i \rightarrow p_i = q_i$ (neboť $p_i \neq 1$) - spor!

• nebo stejná prvočísla v různých mocninách: $n = p_1^{k_1} \dots p_r^{k_r} = p_1^{l_1} \dots p_r^{l_r}$
 BÚNO: exist $k_i < l_i \rightarrow$ vydělíme rovnost $p_i^{k_i}$, $m = p_1^{k_1} \dots p_r^{k_r} = p_1^{l_1} \cdot p_1^{k_1 - l_1} \dots p_r^{l_r}$ -
 v jednom není p_i , ve druhém ano - převedeno na předchozí případ.
 SPOR!

Tvrzení: Existuje nekonečně mnoho prvočísel

Důkaz: Sporem - necht' je jich konečně: $P = \{p_1, \dots, p_k\}$ všechna prvočísla

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$$

$$\frac{n}{p_i} = p_1 \cdot \dots \cdot p_{i-1} \cdot p_{i+1} \cdot \dots \cdot p_k + \frac{1}{p_i} \notin \mathbb{Z} \rightarrow p_i \text{ není dělitelne' žádným}$$

prvočíslem, $p_i \rightarrow$ ani žádným jiným číslem a (to by mělo prvočís. rozklad \rightarrow prvočíslo z něj by dělilo n)

$\rightarrow n$ je dělitelne' jen 1 a n

$\rightarrow n$ je prvočíslo \rightarrow SPOR! ($n \in P$)

Tvrzení: $\sum_{p \in P} \frac{1}{p} = +\infty$ (řada diverguje), P -množina všech prvočísel.

($\sum \frac{1}{n}$ diverg., $\sum \frac{1}{n^2}$ konverg. \rightarrow prvočísel je hustěji než druhých mocnin.)

Tvrzení: (Bertrand): Pro každé $n \geq 2$ existuje prvočíslo p : $n \leq p < 2n$.

Důsledek: Pro každé $s \geq 1$ existují alespoň 3 s -ciferná prvočísla.

Důkaz: $1 \cdot 10^s \leq p_1 < 2 \cdot 10^s \leq p_2 < 4 \cdot 10^s \leq p_3 < 8 \cdot 10^s$ (Bertrand).

Tvrzení: Pro každé $d \geq 1$ existuje $n \in \mathbb{N}$ takové, že $n, n+1, \dots, n+(d-1)$ jsou složená čísla.

Důkaz: $(d+1)! + 2, \dots, (d+1)! + k, \dots, (d+1)! + (d+1)$ - d po sobě jdoucích složených čísel $k \mid [(d+1)! + k], 2 \leq k \leq d+1$

Počítání modulo n

Def.: $a, b \in \mathbb{Z}$. Řekneme, že a je KONGRUENTNÍ s b modulo n , jestliže $(a-b)$ je dělitelne' n . Píšeme $a \equiv b \pmod{n}$.

Tvrzení: ~~Relace~~ Následující věty jsou ekvivalentní:

1. $n \mid (a-b) \leftrightarrow$
2. $a = b + k \cdot n, k \in \mathbb{Z} \leftrightarrow$
3. a, b mají stejný zbytek po dělení n .

Tvrzení: Relace $\equiv \pmod{n}$ rozděluje množinu \mathbb{Z} na systém disjunktních podmnožin - tzv. třídy ekvivalence.

Tvrzení: Relace $\equiv \pmod{n}$ je relou' ekvivalence na \mathbb{Z} .

Důkaz: reflexivní, tranzitivní, symetrická...

Def.: Třídou ekvivalence říkáme zbytkové třídy modulo n

$[a]_n = \{b \in \mathbb{Z}, b \equiv a \pmod{n}\}$ - třída reprezentovaná prvkem $a \in \mathbb{Z}$

Množina všech zbytkových tříd se značí $\mathbb{Z}_n = \{[a]_n, a \in \mathbb{Z}\}$

Platí $|\mathbb{Z}_n| = n$.

Např.: $\mathbb{Z}_4 : [0]_4 = \{0, 4, 8, (-4), \dots\}$, $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
 $[1]_4 = \{1, 5, 9, \dots, -3, -7, \dots\} = \{4k+1, k \in \mathbb{Z}\}$

Tvrzení: Relace $\equiv \pmod{n}$ je zachována při sčítání a násobení.

Když $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$, pak $a+b \equiv c+d \pmod{n}$ & $a \cdot b \equiv c \cdot d \pmod{n}$

Důkaz: Předpoklad: $a-c = k \cdot n$, $k \in \mathbb{Z}$, $b-d = l \cdot n$, $l \in \mathbb{Z}$, pak

$$(a+b) - (c+d) = (a-c) + (b-d) = k \cdot n + l \cdot n = (k+l) \cdot n \rightarrow (a+b) \equiv (c+d) \pmod{n}$$

$$a \cdot b - c \cdot d = ab - cb + cb - cd = (a-c) \cdot b + c(b-d) = k \cdot n \cdot b + c \cdot l \cdot n = (kb+cl) \cdot n \rightarrow$$

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

Důsledek: 1. Když $a \equiv b \pmod{n}$, pak $r \cdot a \equiv r \cdot b \pmod{n}$

2. Když $a_i \equiv b_i \pmod{n}$ pro $i=1, \dots, k$ pak $\sum_{i=1}^k r_i \cdot a_i \equiv \sum_{i=1}^k r_i \cdot b_i \pmod{n}$.

Použití - testovací kritéria pro dělitelnost.

Např.: Číslo je dělitelné 3, je-li jeho ciferný součet dělitelný 3.

$$1 \equiv 1 \pmod{3}, 10 \equiv 10 \pmod{3}, 1^k \equiv 10^k \pmod{3}$$

$$c = \sum_{i=0}^r c_i \cdot 10^i \equiv \sum_{i=0}^r c_i \cdot 1^i \pmod{3} = \text{ciferný součet}, c = c_0 \dots c_r = \text{cifry}$$

Důsledek: Mohu definovat sčítání a násobení na zbytkových třídách.

Def.: Na \mathbb{Z}_n definujeme $\oplus, \odot : [a]_n \oplus [b]_n = [a+b]_n, [a]_n \odot [b]_n = [a \cdot b]_n$

To je korektní definice, neboť výsledek vyjde stejně nezávisle na volbě reprezentantu.

$$[a] = [a_1] \rightarrow a \equiv a_1 \pmod{n} \rightarrow a+b \equiv a_1+b_1 \pmod{n} \rightarrow$$

$$[b] = [b_1] \rightarrow b \equiv b_1 \pmod{n} \rightarrow [a_1+b_1]$$

Např.: $\mathbb{Z}_4 : [2]_4 = [6]_4, [3]_4 = [7]_4$

$$\left. \begin{aligned} [2] \odot [3] &= [6] = [2] \\ [6] \odot [7] &= [42] = [2] \end{aligned} \right\} \begin{array}{l} \text{standardní} \\ \text{traz} \end{array}$$

Úmluva: Místo $[2]_4 \oplus [3]_4 = [1]_4$ budu psát $2+3=1$ v $\mathbb{Z}_4 \rightarrow$ počítáme mod 4.

$$\mathbb{Z}_4 : \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 2 & 3 \\ \hline 2 & 0 & 2 & 0 & 2 \\ \hline 3 & 0 & 3 & 2 & 1 \end{array}$$

Tvrzení: (Vlastnosti \oplus, \odot na \mathbb{Z}_n)

\oplus komutativní: $[a] \oplus [b] = [b] \oplus [a]$

asociativní: $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$

ma' nulový prvek - $[0]: \dots [a] + [0] = [a]$

ma' všechny opačné prvky: pro $[a]$ je opačný $[-a] = [n-a]$
 $[a] \oplus [-a] = [0]$

\odot komutativní, asociativní

ma' jednotkový prvek $[1]: [a] \odot [1] = [a]$

\oplus, \odot distributivní: $[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$

Def.: Množina K se dvěma binárními operacemi $+, \cdot : K \times K \rightarrow K$ jež mají

vlastnosti: $+$ - komut., asoc., ma' \emptyset prvek a všechny opačné prvky

\cdot - asoc.

$+, \cdot$ - distribut.

se nazývá OKRUH.

Je-li \odot komutativní s jednotkovým prvkem tak se to nazývá komutativní okruh s jednotkou.

Definice: Komutativní okruh s 1 , $(K, +, \cdot, 0, 1)$ ve kterém každý nenulový prvek $a \neq 0$ má inverzní prvek se nazývá těleso.

Kdy je $(\mathbb{Z}_n, +, \cdot)$ těleso?

Př.: $(\mathbb{Z}_4, +, \cdot)$ 2^{-1} neek.
 $1^{-1} = 1, 3^{-1} = 3 \rightarrow$ není to těleso

$(\mathbb{Z}_3, +, \cdot)$ $\mathbb{Z}_3 = \{[0], [1], [2]\} = \{0, 1, 2\}$
 $1^{-1} = 1$ $2 \cdot x = 1 \text{ v } \mathbb{Z}_3 \quad x = 2^{-1}$
 $2^{-1} = 2$ $2 \cdot 2 = 4 = 1 \text{ v } \mathbb{Z}_3$
 \rightarrow všechny nenulové mají inverz.
 \rightarrow je to těleso

Řešení rovnic $a \cdot x = b \text{ v } \mathbb{Z}_n$

\geq def. $[a]_n \odot [x]_n = [b]_n$
 \circ
 \geq def. $[a \cdot x]_n = [b]_n$
 rovnosti tříd $\rightarrow a \cdot x \equiv b \pmod{n}$
 \geq def. $\equiv \pmod{n}$ $\rightarrow ax - b = k \cdot n, k \in \mathbb{Z}$

Označím: $y = (-k) - ax + ny = b$, řešíme v $\mathbb{Z} \rightarrow$ Diofant. rovnice

Má řešení v \mathbb{Z} právě když $d = \gcd(a, n) \mid b$ a pak jsou všechna řešení tvaru $x = x_p + k \cdot x_0, y = y_p + k \cdot y_0, k \in \mathbb{Z}$, kde $x_0 = n/d, y_0 = -a/d$ je nesoudělné řešení homog. rovnice $ax + ny = 0$.

V \mathbb{Z}_n určí x třídy $[x]_n = [x_p + k \cdot \frac{n}{d}]$ a ty jsou různé pro $k = 0, 1, \dots, d-1$, neboť $k=d: [x] = [x_p + d \cdot \frac{n}{d}] = [x_p + n] = [x_p]$ totéž jako pro $k=0$.

Tvrzení: Rovnice $ax = b \text{ v } \mathbb{Z}_n$ má řešení právě když $\gcd(a, n)$ dělí b .
 A když $d = \gcd(a, n) \mid b$, pak existuje právě d různých řešení v \mathbb{Z}_n .

Důsledek: $a \in \mathbb{Z}_n$, a má inverz (tj. existuje a^{-1}) právě když a je nesoudělné s n .

Důkaz: $a^{-1} = x$ je takové x , že řeší rov. $a \cdot x = 1 \text{ v } \mathbb{Z}_n$
 A to má řešení právě když $\gcd(a, n) \mid 1$, ale 1 je dělitelné pouze $1 \rightarrow \gcd(a, n) = 1$, tj. a nesoudělné s n .

Důsledek: Okruh $(\mathbb{Z}_n, +, \cdot)$ je těleso právě když $n = p$ je prvočíslo.

Důkaz: vš. $a \neq 0$ mají inverz $a^{-1} \leftrightarrow$ vš. $a = 1, 2, \dots, n-1$ jsou nesoudělné $n \leftrightarrow n = p$ je prvočíslo.

Pozn.: Pokud a soudělné s n , pak 1. $a \cdot x = 0$ má nenulové řešení (neboť má ≥ 2 řešení). 2. $a \cdot x = a \cdot y$ z toho rovnice $x=y$! nelze krátit
 Pokud a nesoudělné s n , pak $ax = ay$ implikuje $x=y$ (= to jediné řešení)
 \rightarrow lze krátit - krácení odpovídá násobení rovnice prvkem a^{-1} :
 $a^{-1} a x = a^{-1} \cdot a \cdot y, 1 \cdot x = 1 \cdot y, x = y$

Čínská věta o zbytcích

Problém - farmáři pěstovali rýži - rozdělili na 3 stejné díly - každý prodává jinde.

1. Základní váha (pytel) = 87 liber - prodal vše a zbylo 18 liber.
2. 170 38
3. 143 40

Kolik rýže vypěstovali.

Věta: Čínská o zbytcích

Nechť m_1, \dots, m_n jsou navzájem nesoudělná čísla.

Pak soustava rovnic $x = a_1 \pmod{m_1}$
 $x = a_2 \pmod{m_2}$
 \vdots
 $x = a_n \pmod{m_n}$

má řešení a to je dané jednoznačně v \mathbb{Z}_M , kde $M = m_1 \cdot m_2 \cdot \dots \cdot m_n = \prod_{i=1}^n m_i$

Důkaz existence řešení:

Najdu q_1, \dots, q_n tak, že $q_i = 1 \pmod{m_i}, q_i = 0 \pmod{m_j}, j \neq i$

$q_i = s \cdot \left(\prod_{j \neq i} m_j \right)$, kde $s = N_i^{-1} \pmod{m_i}, N_i^{-1}$ existuje, protože $N_i = \prod_{j \neq i} m_j$
 nesoudělné s m_i (neboť vs. $m_j \neq m_i$ byly m_j nesoudělné s m_i)

$q_i = k \cdot m_j, j \neq i \rightarrow q_i \equiv 0 \pmod{m_j} \rightarrow q_i = 0 \pmod{m_j}$

$q_i = s \cdot N_i = N_i^{-1} \cdot N_i = 1 \pmod{m_i}$

Potom $x = a_1 \cdot q_1 + a_2 \cdot q_2 + \dots + a_n \cdot q_n \equiv a_1 \cdot 0 + \dots + a_i \cdot 1 + \dots + a_n \cdot 0 \pmod{m_i} \equiv a_i \pmod{m_i}$
 jednoznačnost v \mathbb{Z}_M

Sporem: Nechtě $x \neq y$ jsou řešení soustavy \pmod{M} , pak $z = x - y$ řeší soustavu
 $z = 0 \pmod{m_1}, \dots, z = 0 \pmod{m_n}$ aneb

$z = k_1 \cdot m_1 = k_2 \cdot m_2 = \dots = k_n \cdot m_n$

$m_1 \mid k_2 \cdot m_2$ a m_1, m_2 nesoudělná $\xrightarrow{\text{lemma}} m_1 \mid k_2$, tj. $k_2 = l_1 \cdot m_1$

$\rightarrow z = k_2 \cdot m_2 = l_1 \cdot m_1 \cdot m_2 = k_3 \cdot m_3 \rightarrow (m_1 \cdot m_2) \mid k_3 \cdot m_3$

$(m_1 \cdot m_2)$ nesouděl s $m_3 \rightarrow m_1 \cdot m_2 \mid k_3 \rightarrow z = (l_2 \cdot m_1 \cdot m_2) \cdot m_3 \rightarrow$

ATD - konečnou indukci, $z = l \cdot m_1 \cdot \dots \cdot m_n = l \cdot M, z = x - y = 0 \pmod{M}$,
 $x = y \pmod{M} \rightarrow$ SPOR!

Vypěstovali $X = 3 \cdot x$, kde $x = 18 \pmod{87}$
 $x = 38 \pmod{170}$
 $x = 40 \pmod{143}$

$m_1 = 87 = 3 \cdot 29$
 $m_2 = 170 = 2 \cdot 5 \cdot 17$
 $m_3 = 143 = 11 \cdot 13$
 $\left. \begin{matrix} \text{po dvou nesoudělná} \\ \text{existuje jediné řešení v } \mathbb{Z}_M \end{matrix} \right\}$

$M = 87 \cdot 170 \cdot 143 = 2114970$

$q_1 = s \cdot 170 \cdot 143$, kde $s = (143 \cdot 170)^{-1} \in \mathbb{Z}_{87}$

$143 \cdot 170 \stackrel{!}{=} 56 \cdot (-4) = (-224) = -50 = 37 \pmod{87} \rightarrow s = 37^{-1} \in \mathbb{Z}_{87}$

$37 \cdot s = 1 \pmod{87}$

$37s + 87n = 1$

Eukleid: $87 = 2 \cdot 37 + 13$

$37 = 2 \cdot 13 + 11$

$13 = 1 \cdot 11 + 2$

$11 = 2 \cdot 5 + 1$

$q_1 = 40 \cdot 170 \cdot 143 = 972\ 400$

Bezout: $1 = 11 - 5 \cdot 2 = 11 - 5(13 - 1 \cdot 11) = (-5) \cdot 13 + 6 \cdot 11 = \dots$
 $\dots \text{ATO} \dots = (-17) \cdot 87 + 40 \cdot 37$

Diofant rov. $s = 40 + k \cdot 87, y = (-17) + k \cdot (-37)$

$\forall \mathbb{Z}_{87} \quad s = 40 + k \cdot 87 = 40$

q_2, q_3 - obdobně

$x = 18 \cdot q_1 + 58 \cdot q_2 + 40 \cdot q_3 \in \mathbb{Z}_M$
 $= 65\ 669\ 358 = 105\ 288 \pmod{M}$

Víme-li, že výnos po $X = 3 \cdot x < 3 \cdot M$, pak můžeme říci, že výtěžili:
 $X = 3 \cdot x = 315\ 864$ liber rýže.

Použití - reziduální násobení

m_1, \dots, m_n - navzájem nesoudělné $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$

A, B - velká čísla, čím $A \cdot B < M$ nebo chci jen zbytek z $A \cdot B$ po dělení M

$A \rightsquigarrow (A_1, \dots, A_n) \quad A \equiv A_i \pmod{m_i}$

$B \rightsquigarrow (B_1, \dots, B_n)$

Protože $A \cdot B \equiv A_i \cdot B_i \pmod{m_j}$, tak mohu vynásobit zbytky modulo m_i
 $A_i \cdot B_i \equiv Z_i \pmod{m_i}$

(Z_1, \dots, Z_n) - zbytky pro $A \cdot B$

Z číselné řady α zbytků lze jednoznačně určit $A \cdot B \pmod{M}$, $A \cdot B = Z_1 \cdot q_1 + \dots + Z_n \cdot q_n$
 q_1, \dots, q_n jsou už známé

Př.: $m_1 = 3, m_2 = 5, m_3 = 7 \dots M = 3 \cdot 5 \cdot 7 = 105$

$25 \cdot 4 \quad 25 \rightarrow \begin{matrix} z_3 & z_5 & z_7 \\ (1, 0, 4) \end{matrix}$

$4 \rightarrow (1, 4, 4)$

$25 \cdot 4 \rightsquigarrow (1 \cdot 1, 0 \cdot 4, 4 \cdot 4) = (1, 0, 2)$ zde $q_1 = 70, q_2 = 21, q_3 = 15$
 $25 \cdot 4 \rightsquigarrow 1 \cdot 70 + 2 \cdot 95 = 100$

V praxi se používá $m_1 = 5, m_2 = 7, m_3 = 11, m_4 = 13, m_5 = 17, m_6 = 19, m_7 = 23, m_8 = 29$
 $M > 10^9$
 $> 2^{30}$

Zpracovávají se tak součiny v rozmezí -2^{29} až 2^{29} , kde pro $Y < 0$ se bere $M + Y \in (2^{29}, 2^{30})$.

Fermatova a Eulerova věta

Věta (malá Fermatova): At' p je prvočíslo $\gcd(a, p) = 1$. Pak $a^{p-1} = 1$ v \mathbb{Z}_p .

Důkaz: $\{1, 2, \dots, p-1\}$ jsou všemi invertibilní prvky v \mathbb{Z}_p

$$\{1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a\} \stackrel{\subseteq}{=} \{1, 2, \dots, p-1\}, \quad (2 \cdot a)^{-1} = a^{-1} \cdot 2^{-1}$$

$$1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot a \cdot \dots \cdot (p-1) \cdot a = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \quad \text{v } \mathbb{Z}_p$$

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

$$a^{p-1} = 1 \quad \text{v } \mathbb{Z}_p$$

Poznámky: 1. Malá Fermatova věta necharakterizuje prvočísla: existují přirozená složená čísla n s vlastností $\gcd(a, n) = 1$, pak $a^{n-1} = 1$ v \mathbb{Z}_n . Je jich nekonečně mnoho, říká se jim Carmichaelova.

Př.: $3 \cdot 11 \cdot 17 = 561$ je nejmenší Carmichaelovo číslo.

Rabin-Miller's Primality test.

2. Malá Fermat. věta:

$$8^{103} = 2 \quad \text{v } \mathbb{Z}_{13}, \quad 13 \text{ je prvočíslo: } 8^{12} = 1 \quad \text{v } \mathbb{Z}_{13}$$

$$8^{103} = 8^{12 \cdot 8 + 7} = (8^{12})^8 \cdot 8^7 = 8^7$$

$\{1, \dots, p-1\}$ jsou všechny inverzní prvky v \mathbb{Z}_p , p je prvočíslo.

$\{b_1, \dots, b_{\varphi(m)}\}$ jsou všechny inverzní prvky v \mathbb{Z}_m , $m \geq 2$

Definice: $\varphi(1) = 1$, $\varphi(m)$ je počet inverzních prvků v \mathbb{Z}_m (φ říkáme Eulerova funkce).

Vlastnosti funkce φ :

1. p prvočíslo $\varphi(p) = p-1$, obecně $\varphi(p^n) = p^n - p^{n-1}$, počet čísel $z \in 0 \dots p^n-1$ dělitelných p^n

2. $\gcd(m_1, m_2) = 1$ pak $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$

3. $\varphi(p_1^{n_1} \dots p_s^{n_s}) = (p_1^{n_1} - p_1^{n_1-1}) (p_2^{n_2} - p_2^{n_2-1}) \dots (p_s^{n_s} - p_s^{n_s-1})$

$$\text{Např.: } \varphi(40) = \varphi(2^3 \cdot 5) = (2^3 - 2^2) \cdot (5 - 1) = 16$$

Věta: Eulerova. At' $m \geq 2$ je přiroz. číslo, $\gcd(a, m) = 1$. Pak $a^{\varphi(m)} = 1$ v \mathbb{Z}_m

Důkaz: $\{b_1, \dots, b_{\varphi(m)}\} = \{b_1 \cdot a, b_2 \cdot a, \dots, b_{\varphi(m)} \cdot a\}$ (iše invertibilní v \mathbb{Z}_m)

$$b_1 \cdot b_2 \cdot \dots \cdot b_{\varphi(m)} = b_1 \cdot a \cdot b_2 \cdot a \cdot \dots \cdot b_{\varphi(m)} \cdot a \quad \text{v } \mathbb{Z}_m$$

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

$$1 = a^{\varphi(m)} \quad \text{v } \mathbb{Z}_m$$

Věta: Platí $(z^{e_A})^{d_A} = z \quad \forall z \in \mathbb{Z}_{n_A}$

Důkaz: $e_A \cdot d_A = 1 \quad \forall \mathbb{Z}_{\varphi(n_A)}$, $e_A \cdot d_A = 1 + k \cdot \varphi(n_A) \quad \forall \mathbb{Z}$ (pro nějaké k)

$$(z^{e_A})^{d_A} = z^{1+k \cdot \varphi(n_A)} = z \cdot z^{k \cdot \varphi(n_A)} \quad \forall \mathbb{Z}_{n_A}, \text{ kdeť bych } z^{\varphi(n_A)} = 1 \quad \forall \mathbb{Z}_{n_A}$$

(i) $\gcd(z, n_A) = 1$, pak $z^{\varphi(n_A)} = 1$ (Euler)

(ii) $\gcd(z, n_A) \neq 1$ ať třeba z je dělitel p_A , pak $p_A \mid z^{\varphi(n_A)}$,

$$z^{\varphi(n_A)} \pmod{q_A} = z^{\varphi(n_A)} \pmod{n_A}, \quad \gcd(z, q_A) = 1, \quad \underbrace{(z^{\varphi(q_A)})^{\varphi(p_A)}}_{z^{\varphi(n_A)}} = 1 \quad \forall \mathbb{Z}_{q_A}$$

Poznámky:

1. Prvočísla p_A, q_A se musí volit „rozumně“
2. Protokol lze modifikovat s $\lambda(n)$ namísto $\varphi(n)$.
3. RSA lze použít i k autorizaci zpráv (podpis)

Bob píše Alici: $z \mapsto z^{d_B} \in \mathbb{Z}_{n_B} \mapsto (x)^{e_A} \in \mathbb{Z}_{n_A}$
 \uparrow zpráva \uparrow x

Jiné kryptosystémy:

1. k-Threshold System for sharing a secret (3.6.9 - Čínská věta o zbytcích)
2. Public Key Agreement (Diffie + Hellman) (3.6.18)

Počítání zbytků velkých mocnin

1. Eulerova věta $8^{103} = 8^{12 \cdot 8 + 7} = 8^7$ (zmenšení exponentu)

2. Repeated Squares Algorithm (alg. opakování čtverců)

$$8^7 = 2 \quad \forall \mathbb{Z}_{13}, \quad (7)_2 = (1, 1, 1)$$

$X S X S X$ - za jedničkou
 \rightarrow oddělovací

$X S X S X$	\rightarrow
$X \dots 1 \cdot 8 = 8$	
$S \dots 8^2 = 64 = 12 = -1$	
$X \dots (-1) \cdot 8 = -8 = 5$	
$S \dots 5^2 = 25 = -1$	
$X \dots (-1) \cdot 8 = -8 = 5$	

Př.: $3^{19} \in \mathbb{Z}_5$

$$(19)_2 = (1, 0, 0, 1, 1) \dots \quad X S S S X X$$

$$X \dots 1 \cdot 3 = 3; \quad S \dots 3^2 = 9 = -1; \quad S \dots (-1)^2 = 1;$$

$$S \dots 1^2 = 1; \quad X \dots 1 \cdot 3 = 3; \quad S \dots 3^2 = 9 = -1; \quad X \dots (-1) \cdot 3 = 2$$

Rychlost - málo násobení

korektnost - Hornerovo schéma

$$p(x) = \left\langle \begin{matrix} a \\ p'(x) \cdot x + a \end{matrix} \right.$$

Lineární algebra (nad \mathbb{R}) ... \mathbb{R} - těleso

Př.: v \mathbb{R}^3 , podprostor dim 2 v \mathbb{R}^3 = rovina procházející počátkem

- 1. Rovinu lze popsat bází - generování kódového slova
- 2. Rovinu lze popsat normálovým vektorem - kontrola kódového slova
 - 1. fundamentální systém lineární soustavy
 - 2. rovnice roviny

Lineární algebra nad \mathbb{Z}_m

- Známe:
1. $ax = b$ v \mathbb{Z}_m má řešení iff $d | b$, kde $d = \gcd(a, m)$. Pak $ax = b$ má přesně d různých řešení v \mathbb{Z}_m .
 2. a invertibilní v \mathbb{Z}_m iff $\gcd(a, m) = 1$
 3. \mathbb{Z}_m je těleso iff m je prvočíslo.

Slogan: Nad \mathbb{Z}_p (p prvočíslo) vypadá lin. alg. stejně jako nad \mathbb{R} .

Gaussova Eliminační Metoda - udržet horní trojúhelníkový tvar matice

Elementární úpravy řádků: 1. prohodit řádky; 2. vynásobit řádek nenulovým skalárem (v \mathbb{Z}_p); 3. k danému řádku lze přičíst lineární kombinaci ostatních.

GEM se používá například na:

1. ke zjištění hodnosti (počet nenulových řádků po skončení GEM)
2. řešení $Ax = b$
3. $(A | E) \sim \dots \sim (E | A^{-1})$ inverzní matice

Algoritmy založené na GEM používáme v \mathbb{Z}_p pouze, když p je prvočíslo.

Příklad:

Nad \mathbb{Z}_5 vyřešte:

$$\begin{aligned} x + 2y - z + 3w &= 3 \\ 4x + z + w &= 2 \\ 4x + 4y + z + 2w &= 2 \end{aligned}$$

→ pro přehlednost zapisujeme operace

$$\left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 3 \\ 4 & 0 & 1 & 1 & 2 \\ 4 & 4 & 1 & 2 & 2 \end{array} \right) \sim \left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 3 \\ 0 & 2 & 0 & 3 & 0 \\ 0 & 1 & 0 & 4 & 0 \end{array} \right) \begin{matrix} R_1 \\ R_2 + R_1 \\ R_3 + R_1 \end{matrix} \sim \left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 3 \\ 0 & 2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \begin{matrix} R_1 \\ R_2 \\ R_3 + 2R_2 \end{matrix}$$

$2 = \text{hod}(A) = \text{hod}(A|b)$
 ↳ řešení existuje

Frobeniova věta: $Ax = b$ má řeš. iff $h = \text{hod}(A) = \text{hod}(A|b)$

V tomto případě řešení je tvaru $x = x_p + (\alpha_1 \cdot x_1 + \dots + \alpha_k \cdot x_k)$, kde $k = \text{počet sloupců } A - h$
 jakékoliv řešení $Ax = b$ ↑ x_1, \dots, x_k - fund. systém $\alpha_1, \dots, \alpha_k \in \mathbb{Z}_p$
 (báze řešení $Ax = 0$)

Řešení příkl: $(3, 0, 0, 0) + \alpha_1 (1, 1, 0, 1) + \alpha_2 (1, 0, 1, 0)$

$\alpha_1, \alpha_2 \in \mathbb{Z}_5$

$$\begin{aligned} 1 \cdot x_1 + 2 \cdot 1 + 0 \cdot (-1) + 2 \cdot 1 &= 0 & \rightarrow 2x_2 + 0 \cdot 0 + 3 \cdot 1 &= 0 & \rightarrow 2x_2 + 0 \cdot 1 + 0 \cdot 3 &= 0, 2x_2 = 0 \\ x_1 + 4 &= 0 & 2x_2 + 3 &= 0, 2x_2 = 2, x_2 = 1 & 1x_1 + 2 \cdot 0 - 1 \cdot 1 + 0 \cdot 0 &= 0 \end{aligned}$$

Př.: nad \mathbb{Z}_7 $\left(\begin{array}{cccc|c} 1 & 3 & 1 & 1 & 2 \\ 0 & 2 & 3 & 1 & 5 \\ 0 & 0 & 0 & 1 & 4 \end{array} \right)$ hod $A = \text{hod}(A|b) = 3 \rightsquigarrow$ řešení existuje

řeš.: $(3, 0, 0, 4, 4) + \alpha_1(0, 2, 1, 0, 0) + \alpha_2(6, 6, 0, 0, 1)$ $\alpha_1, \alpha_2 \in \mathbb{Z}_7$

$x_1 + 3 \cdot 0 + 1 \cdot 0 + 1 \cdot 4 + 4 \cdot 4 = 2$
 $x_1 + 6 = 2$
 $x_1 + 3 \cdot 2 + 1 \cdot 1 + 1 \cdot 0 + 4 \cdot 0 = 0$
 $2x_2 + 3 \cdot 1 + 1 \cdot 0 + 2 \cdot 0 = 0$
 $2x_2 + 3 = 0$
 $2x_2 = 4$
 $x_2 = 2$

$x_1 + 3 \cdot 6 + 1 \cdot 0 + 1 \cdot 0 + 4 \cdot 1 = 0, x_1 = -22 \equiv -1 = 6$
 $2x_2 + 3 \cdot 0 + 1 \cdot 0 + 2 \cdot 1 = 0$
 $2x_2 = -2$
 $x_2 = -1$

$G = \begin{pmatrix} 1 & 3 & 1 & 1 & 4 \\ 0 & 2 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$... matice soustavy, $H = \begin{pmatrix} 0 & 2 & 1 & 0 & 0 \\ 6 & 6 & 0 & 0 & 1 \end{pmatrix}$

H má vlastnost ... $G \cdot H^T = 0$ & H má maximální možnou hodnotu s touto vlastností!
 (H je ortogonální doplněk G)

Lineární algebra nad \mathbb{Z}_m (m složené číslo)

- aritmetika matic stejná (sčítání, násobení)
- výpočet determinantu

Věta: A je $n \times n$ nad \mathbb{Z}_m . A^{-1} existuje iff existuje $(\det A)^{-1} \in \mathbb{Z}_m$.

V tomto případě $A^{-1} = (\det A)^{-1} \cdot D^T$, kde D je matice algebraických doplňků A .

Příklad: Nad \mathbb{Z}_{26} najděte A^{-1} , pokud existuje k $A = \begin{pmatrix} 2 & 3 & 5 \\ 5 & 11 & 2 \\ 1 & 2 & 2 \end{pmatrix}$

$\det A = 2 \cdot 11 \cdot 2 + 1 \cdot 3 \cdot 2 + 5 \cdot 2 \cdot 5 - 1 \cdot 11 \cdot 5 - 5 \cdot 3 \cdot 2 - 2 \cdot 2 \cdot 2 = 7 \pmod{26}$

$\gcd(26, 7) = 1 \rightsquigarrow 7^{-1}$ existuje v $\mathbb{Z}_{26} \rightsquigarrow A^{-1}$ existuje. $A^{-1} = (7)^{-1} \cdot D^T = 15 \cdot D^T$

$D = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$ $\underbrace{(-1)^{3+2} \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix}}_{\text{alg. doplněk}} = (-1) \cdot (4 - 3) = -1 = 25$

2 v A na 2ř., 3 sl.

Lineární kódy

vysílání $\xrightarrow{\text{korupce}}$ příjem

p prvočíslo, \mathbb{Z}_p těleso

$V \leftrightarrow (\mathbb{Z}_p)^n \leftarrow$ vektorový prostor dim n nad \mathbb{Z}_p

\uparrow lineární podprostor

$0 \leq \dim V = k \leq n$

$v \in V$... kódové slovo (to se bude posílat)

V ... lineární p -kód délky n a dimenze k

g_1, \dots, g_k báze V , $G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$ matice k LN řádků, n sloupců
 ($\text{hod } G = k$)
 \uparrow generující matice

$(\alpha_1, \dots, \alpha_k) \cdot G = v \in V$
 $\underbrace{\hspace{2cm}}_{\text{souřadnice = info}} \uparrow$ kódové slovo s redundantními bity, které info chrání

Existuje matice H (kontrolní, Hemingova matice) s vlastností:

$$v \in V \text{ iff } H \cdot v^T = 0 \quad (H \text{ je ortogonální doplněk } G)$$

Příklad: Nad \mathbb{Z}_2

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \dots \text{generující matice 2-kódu délky 7 a dimenze 4}$$

$$\underbrace{(\alpha_1, \alpha_2, \alpha_3, \alpha_4)}_{\text{info}} \cdot G = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_2 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_3 + \alpha_4, \alpha_1 + \alpha_2 + \alpha_4)$$

$$\underbrace{(1, 1, 0, 1)}_{\text{info}} = (1, 1, 0, 1, 0, 0, 1) = w \dots \text{kódové slovo, které pošleme}$$

$$w \in V \text{ iff } H w^T = 0, \quad \text{systématický kód } (E | \dots) = G, \quad H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

At při přenosu dojde k maximálně 1 chybě:

1. k 0 chybám došlo iff $H \cdot w^T = 0$ (w je vyslané slovo v)

2. k 1 chybě došlo iff $H \cdot w^T \neq 0$ (syndrom $w = H \cdot w^T$)

$$w = v + e^i$$

↑ error pattern, všude 0 a na jediném místě je 1

$$H w^T = H(v + e^i) = H v^T + H e^{iT} = H \cdot e^{iT} = i\text{-tý sloupec } H$$

5 CHYBOU

$$w = (1, 1, 0, 1, 0, 0, 1); \quad w = (1, 1, 1, 1, 0, 0, 1)$$

$$H w^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \dots \text{5. sloupec } H \Rightarrow \text{k chybě došlo ve 3. bitu}$$

Znám H a potřebuji zjistit G

$$G \cdot H^T = 0 \text{ iff } (G \cdot H^T)^T = 0^T \text{ iff } H \cdot G^T = 0$$

\mathbb{K} - komutativní okruh s 1

Def: Polynom v neurčité x nad \mathbb{K} je výraz:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

kde $n \geq 0$, $a_i \in \mathbb{K}$, $a_n \neq 0$ nebo $0 \in \mathbb{K}$ ($n = \deg(p(x))$, definujeme $\deg(0) := -\infty$, $a_n x^n \dots$ vedoucí člen, $a_n \dots$ vedoucí koeficient).

Množina všech... $\mathbb{K}[x]$

Poznámka:

1. Polynom je výraz nitoli funkce.

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \leftrightarrow (a_n, a_{n-1}, \dots, a_0) \in \mathbb{K}^{n+1}$$

Například rovnost $p(x) = q(x)$ je rovnost příslušných vektorů

2. $-\infty$ je symbol. Konvence $(-\infty) + (-\infty) := -\infty$,
 $(-\infty) + n = n + (-\infty) = -\infty$

3. $p(x) = x+1$
 $q(x) = x^3+1$ } v \mathbb{Z}_2 různé polynomy $(1, 1)$
 $(1, 0, 0, 1)$

STEJNĚ FUNKCE $p: x \mapsto p(x)$ $q: x \mapsto q(x)$
 $0 \mapsto 1$ $0 \mapsto 1$
 $1 \mapsto 0$ $1 \mapsto 0$

Def: Sčítání a násobení vektorů

Př: $p(x) = x+1$
 $q(x) = x^2+2x+2$ } nad \mathbb{Z}_5

$p(x) + q(x) = x^2 + 3x + 3$ (počítáme v \mathbb{Z}_5)

$p(x) \cdot q(x) = (x+1) \cdot (x^2+2x+1) = x^3 + 2x^2 + 2x + x^2 + 2x + 2 = x^3 + 3x^2 + 4x + 2$

Věta: $\langle \mathbb{K}[x], +, \cdot, 0, 1 \rangle$ tvoří komutativní okruh s jednotkou

Důkaz: $p(x) + q(x) = q(x) + p(x)$... atd.

Dále \mathbb{K} těleso!

Tvrzení: $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$

Důkaz: $p(x) = \begin{cases} 0 \\ a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \end{cases}$

$p(x) = 0 = q(x) \dots -\infty = (-\infty) + (-\infty)$

$q(x) = \begin{cases} 0 \\ b_m x^m + b_{m-1} x^{m-1} + \dots + b_0 \end{cases}$

$p(x) = 0, q(x) \neq 0 \dots -\infty = (-\infty) + m$

$p(x) \neq 0, q(x) \neq 0 \dots p(x) \cdot q(x) = a_n \cdot b_m \cdot x^{n+m} + \dots$

$a_n \cdot b_m \neq 0$, protože \mathbb{K} je těleso; $a_n \neq 0$ iff ex. a_n^{-1} ;

$b_m \neq 0$ iff ex. b_m^{-1} ; $a_n \cdot b_m \neq 0$ iff ex. $(a_n \cdot b_m)^{-1}$

Věta: o dělení polynomů

At' $a(x), b(x)$ jsou nenulové polynomy nad \mathbb{K} . Pak existují jedinečně určené polynomy $q(x)$ (kvocient) a $r(x)$ (zbytek) v $\mathbb{K}[x]$ tak, že $\deg(r(x)) < \deg(b(x))$

a $a(x) = q(x) \cdot b(x) + r(x)$.

Důkaz: indukci

Př: $a(x) = 2x^3 - 4x + 1$, $b(x) = 3x + 2$

1. nad \mathbb{R} : $(2x^3 - 4x + 1) : 3x + 2 = \frac{2}{3}x^2 - \frac{4}{9}x - \frac{28}{27}$

$-(2x^3 + \frac{4}{3}x^2)$

$-\frac{4}{3}x^2 - 4x + 1$

$-(-\frac{4}{3}x^2 - \frac{8}{9}x)$

$-\frac{28}{9}x + 1$

$-(\frac{28}{9}x - \frac{56}{27})$

$\frac{83}{27}$

$2x^3 - 4x + 1 = \underbrace{(\frac{2}{3}x^2 - \frac{4}{9}x - \frac{28}{27})}_{\text{kvocient}} \cdot (3x + 2) + \underbrace{\frac{83}{27}}_{\text{zbytek}}$

$$2. \text{ nad } \mathbb{Z}_7: (2x^3 - 4x + 1) : (3x + 2) = 3x^2 + 5x$$

$$-(2x^3 + 6x^2)$$

$$\hline x^2 - 4x + 1$$

$$-(x^2 + 3x)$$

$$\hline 1$$

$$\begin{array}{c} \uparrow \\ 2 \cdot 3^{-1} \\ 3^{-1} = 5 \end{array}$$

$$(2x^3 - 4x + 1) = \underbrace{(3x^2 + 5x)}_{\text{kvocient}} \cdot (3x + 2) + \underbrace{1}_{\text{zbytek}}$$

Def.: $a \in K$ je kořenem $p(x) \in K[x]$, když platí $p(a) = 0$

Tvrzení: $p(a)$ je rovna zbytku po dělení $p(x)$ polynomem $(x-a)$ v bodě a .

Čili a je kořen $p(x)$ iff $p(x)$ je dělitelem $(x-a)$.

$$\text{Důkaz: } p(x) = (x-a) \cdot q(x) + r(x)$$

Důsledek: Polynom st $n \geq 0$ má nejvýše n kořenů

Důsledek: Pro těleso K jsou následující podmínky ekvivalentní:

1. K má nekonečně mnoho prvků

2. Nad K není třeba rozlišovat mezi polynomy jako výrazy a polynomy jako funkcemi.

Poznámky:

1. polynomij v $\mathbb{R}[x]$ jako funkce

2. Fundamentální věta algebry: $p(x) \in \mathbb{C}[x]$ $\deg(p(x)) = n$ má přesně n kořenů (počítaných s násobnostmi)

3. Např.: $x^2 + 1 \in \mathbb{R}[x]$ nemá kořen v \mathbb{R}

4. Např.: $x^2 + x + 1 \in \mathbb{Z}_2[x]$ nemá kořen v \mathbb{Z}_2

Def.: $a(x) \mid b(x) \dots b(x) = k(x) \cdot a(x)$; $a(x), b(x), k(x) \in K[x]$

Pozor! $2 \mid (-2)$ & $(-2) \mid 2$ v \mathbb{Z} ; $2, -2$ jsou asociované

$$\underbrace{(2x+1) \mid (x+3)} \text{ \& \ } \underbrace{(x+3) \mid (2x+1)} \text{ nad } \mathbb{Z}_5$$

$$(x+3) = 3 \cdot (2x+1) \quad (2x+1) = 3^{-1}(x+3) = 2(x+3)$$

Tvrzení: $a(x), b(x)$ jsou asociované iff $a(x) = c \cdot b(x)$, kde $c \in \mathbb{R}$ invertibilní.

Definice: Polynom je MONICKÝ, když jeho vedoucí koeficient je 1.

Definice: $\gcd(a(x), b(x))$

Pozor! \gcd není určen jednoznačně (učen až na asociovanost).

$$\text{Př.: } \gcd(25, 19) = 1 = -3 \cdot 25 + 4 \cdot 19$$

$$25 = 1 \cdot 19 + 6 \quad \begin{array}{cccc} 1 & 0 & 0 & 1 \end{array}$$

$$19 = 3 \cdot 6 + 1 \quad \begin{array}{cccc} 0 & 2 & 1 & -1 \end{array}$$

$$6 = 6 \cdot 1 + 0 \quad \begin{array}{cccc} 2 & -3 & -1 & 4 \end{array}$$

Př.: $\gcd(x^5+1, x^2+1)$ nad \mathbb{Z}_5

$$x^5+1 = [x^3+4x](x^2+1) + (x+1)$$

$$x^2+1 = [x+4](x+1) + 2$$

$$x+1 = [3x+3] \cdot 2 + 0$$

$$\begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 4x^3+x \\ 1 & 4x+1 & 4x^3+x & x^4+4x^3+4x^2+x+1 \end{array}$$

$$\begin{array}{r} x^5+1 : x^2+1 = x^3+4x \\ -(x^5+x^2) \\ \hline 4x^3+1 \\ -(4x^3+4x) \\ \hline x+1 \end{array}$$

$$\begin{array}{r} x^2+1 : x+1 = x+4 \\ -(x^2+x) \\ \hline 4x+1 \\ -(4x+4) \\ \hline 2 \end{array}$$

$$1 - (x+4) \cdot (4x^3+x) = 1 - (4x^4 + x^2 + x^3 + 4x) = 1 - 4x^4 - x^2 - x^3 - 4x = x^4 + 4x^3 + 4x^2 + x + 1$$

Bezoutova rovnost:

$$2 = (4x+1) \cdot (x^5+1) + (x^4+4x^3+4x^2+x+1) \cdot (x^2+1) \text{ nad } \mathbb{Z}_5$$

$\mathbb{Z}_5[x]$ „modulo x^5+1 “

$$1 = (3x^4+2x^3+2x^2+3x+3)(x^2+1)$$

$$2 = (x^4+4x^3+4x^2+x+1)(x^2+1)$$

Př.: $\mathbb{Z}_2[x]$ $m(x) = x^2+x+1$

zbytky po dělení $0, 1, x, x+1$

tabulka počítání v \mathbb{Z}_2

•	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	1	x+1	1
x+1	0	x+1	1	x

$$(x \cdot x = x^2)$$

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

$$\begin{array}{r} -(x^2+x+1) \\ \hline x+1 \end{array}$$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	0	1	x

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

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

$$x^2+x+1 = 0 \text{ nemá v } \mathbb{Z}_2 \text{ řešení}$$

$$x^2+x+1 = 0 \text{ má řešení v } \mathbb{Z}_2[x]$$

Přepsání tabulek:

+	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

•	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

$$x^2+x+1 = 0 \text{ nad } \mathbb{Z}_2 \text{ nemá řešení}$$

$$x^2+x+1 = 0 \text{ nad } \mathbb{Z}_2[x]/_{x^2+x+1} \text{ má řešení: } A^2+A+1 = B+A+1 = 1+1 = 0, \\ B^2+B+1 = A+B+1 = 1+1 = 0.$$

Definice: At' K je těleso, $m(x) \in K[x]$. Pak označíme jako $K[x]/m(x)$ množinu zbytků modulo $m(x)$ a budeme ji říkat ALGEBRAICKÉ ROZŠÍŘENÍ K .

Poznámky: (1) $K[x]/m(x)$ je opět okruh. Neformálně: sčítáte a násobíte zbytky jako polynomy, v případě velkého stupně nahradíte zbytkem po dělení $m(x)$. Formálně: třídy ekvivalence $[p(x)]_{m(x)}$

(2) K je podokruh $K[x]/m(x)$. Neformálně: „tabulky“ K jsou „podtabulkami“ „tabulek“ $K[x]/m(x)$.

Pr.: $\mathbb{R}[x]/(x^2+1) = \mathbb{C}$

obsahuje $ax+b$, $a, b \in \mathbb{R}$

sčítání: $(ax+b) + (a'x+b') = (a+a')x + (b+b')$

násobení: $(ax+b) \cdot (a'x+b') = aa'x^2 + (ab'+a'b)x + bb' = (ab'+a'b)x + (bb'-aa')$

Zbytek po dělení: $aa'x^2 + (ab'+a'b)x + bb' : x^2+1 = aa'$
 $\frac{-(aa'x^2 + aa')}{(ab'+a'b)x + (bb'-aa')}$

$\mathbb{R}[x]/x^2+1$ jsou algebraickým rozšířením \mathbb{R}

$x^2+1=0$ nad \mathbb{R} nemá řešení

$x^2+1=0$ nad $\mathbb{R}[x]/(x^2+1)$

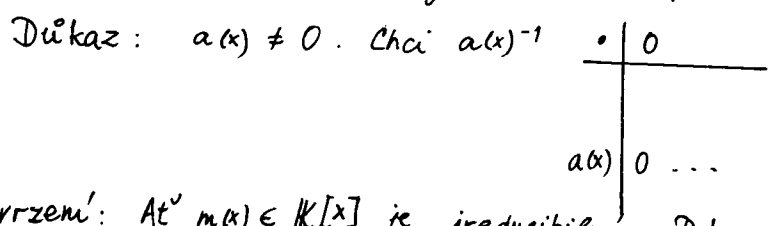
Kdy je $\mathbb{K}[x]/m(x)$ těleso?

Kdy je \mathbb{Z}_m těleso? (iff m je ireducibilní: $m = a \cdot b$, $1 < a < m$ & $1 < b < m$)

Def.: $m(x) \in \mathbb{K}[x]$ je ireducibilní, když nelze napsat: $m(x) = a(x) \cdot b(x)$, kde $1 < \deg(a(x)) < \deg(m(x))$ & $1 < \deg(b(x)) < \deg(m(x))$

- Pr.: 1. x^2+1 nad \mathbb{R} je ireducibilní
 - 2. x^2+x+1 nad \mathbb{Z}_2 je ireducibilní
 - 3. x^2+1 nad \mathbb{C} je reducibilní... $x^2+1 = (x+i)(x-i)$
- ireducibilní ~ chová se jako prvočíslo

Tvrzení: At $m(x) \in \mathbb{K}[x]$ je ireducibilní. Pak $\mathbb{K}[x]/m(x)$ je těleso.



Tvrzení: At $m(x) \in \mathbb{K}[x]$ je ireducibilní. Pak rovnice $m(x) = 0$ má kořen v $\mathbb{K}[x]/m(x)$.

Důkaz: (i) $m(x) = a_1x + a_0$, $a_1 \neq 0$
 $m(x) = 0$ má kořen $-a_0 \cdot a_1^{-1} \in \mathbb{K}$

(ii) $m(x) = a_nx^n + \dots + a_0$, $n \geq 2$, $a_n \neq 0$
prvky $\mathbb{K}[x]/m(x)$ jsou polynomy stupně $< n$. Neboť $[x]_{m(x)}$ je prvek $\mathbb{K}[x]/m(x)$.

$A \stackrel{\text{def}}{=} [x]_{m(x)}$, $m(A) = a_n \cdot A^n + a_{n-1} \cdot A^{n-1} + \dots + a_0 = a_n \cdot [x]_{m(x)}^n + \dots + a_0 =$
 $= [a_n x^n + a_{n-1} x^{n-1} + \dots + a_0]_{m(x)} = [m(x)]_{m(x)} = 0$

Věta: At $n \geq 2$. Nad \mathbb{Z}_p (p je prvočíslo) pak existuje alespoň jeden ireducibilní polynom stupně n .

Důsledek: Pro prvočíslo p a $n \geq 1$ existuje těleso o přesně p^n prvcích.

Důkaz: (i) $n=1$ těleso je \mathbb{Z}_p

(ii) $n \geq 2$ vezmu $m(x) \in \mathbb{Z}_p[x]$ ireducibilní stupně n a hledám těleso je $\mathbb{Z}_p[x]/m(x)$. Prvky $\mathbb{Z}_p[x]/m(x)$ mají stupeň $< \deg(m(x)) = n$. Každý takový \leftrightarrow vektor koef. $(\underbrace{\quad, \quad, \quad}_{\text{délky } n}, \dots)$ je jich p^n

Def.: Těleso σ p^n prvků se nazývá Galoisovo a značí se $GF(p^n)$

Př.: $\mathbb{Z}_2[x]/(x^2+x+1) = GF(4)$

Věta: Každé konečné těleso je (až na izomorfismus) nějaké $GF(p^n)$.

Poznámky:

1. kružítkem a pravítkem sestavit pravidelný sedmiúhelník - NELZE!

2. $ax^2 + bx + c = 0$ $a, b, c \in \mathbb{R}$
 $ax^3 + bx^2 + cx + d = 0$
 $ax^4 + bx^3 + cx^2 + dx + e = 0$ } jde to řešit vzorečkem

$ax^5 + bx^4 + cx^3 + \dots = 0$ Nelze! (musí se řešit numericky)

3. trisekce úhlu, kvadratura kruhu, duplikace krychle - NELZE

... Technika alg. rozšíření

Aplikace algebraických rozšíření

Lineární kódy: $V \hookrightarrow (\mathbb{Z}_p)^n$, $0 \leq \dim V = k \leq n$

Pokud navíc má V následující vlastnost $(a_{n-1}, a_{n-2}, \dots, a_0) \in V \rightarrow$

$(a_{n-2}, a_{n-1}, \dots, a_0, a_{n-1}) \in V$ říkáme, že V je cyklický kód.

Př.: $V \hookrightarrow (\mathbb{Z}_3)^5$, $0 \leq \dim V \leq 5$, $(a_4, a_3, a_2, a_1, a_0) \in V \iff a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}_3[x]$
 $a_4(a_3, a_2, a_1, a_0, a_4)$ $(a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0) \cdot x \pmod{x^5-1}$
 $\in \mathbb{Z}_3[x]/(x^5-1)$

Tvrzení: Atž V je cyklický kód. Pak

1. lineární kombinace kódových slov je kódové slovo

2. (Jde-li o kód délky n .) Součin $p(x) \cdot v(x)$ je kódové slovo, jestliže $v(x)$ bylo kódové slovo a násobení probíhá modulo x^n-1 .

Důkaz: 1. protože V je lineární kód

2. $(a_n x^n + \dots + a_0) \cdot v(x) = a_n \boxed{x^n \cdot v(x)} + a_{n-1} \boxed{x^{n-1} \cdot v(x)} + \dots + a_0 \boxed{v(x)}$
 $\in V$ $\in V$ $\in V$

Tvrzení: Atž V je cyklický kód.

vše modulo 1. Ex. polynom $g(x)$ (generující polynom) s vlastností: $v(x) \in V$ iff $v(x) = p(x) \cdot g(x)$ pro nějaké $p(x)$.

2. Ex. polynom $h(x)$ (kontrolní polynom) s vlastností: $v(x) \in V$ iff $v(x) \cdot h(x) = 0$

spec BINARY IS
 sorts: binary
 operations: -
 endspec

Definice: Binární operace $*$ na množině X je zobrazení: $*$: $X \times X \rightarrow X$
 (píšeme $x * y$). Dvojice $\langle X, * \rangle$ se nazývá GRUPOID

Poznámky + příklady:

1. Grupoid je „model“
2. Např.: $(x, y) \mapsto \frac{x}{y}$ na \mathbb{R} , $y \neq 0$ NENÍ binární operace
3. $X = \{a, b, c\}$

*	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

4. $F = \{f \mid f : \{0, 1\} \rightarrow \{0, 1\}\} = \{id, t, c_0, c_1\}$ s operací skládání

id: $0 \mapsto 0$
 $1 \mapsto 1$
 $c_0: 0 \mapsto 0$
 $1 \mapsto 0$

t: $0 \mapsto 1$
 $1 \mapsto 0$
 $c_1: 0 \mapsto 1$
 $1 \mapsto 1$

o	id	t	c_0	c_1
id	id	t	c_0	c_1
t	t	id	c_1	c_0
c_0	c_0	c_0	c_0	c_0
c_1	c_1	c_1	c_1	c_1

Def: Binární operace $*$ na X je

1. asociativní, když $x * (y * z) = (x * y) * z$ pro vš. $x, y, z \in X$.
2. komutativní, když $x * y = y * x$ pro vš. x, y .
3. má levý neutrální prvek e_l , když $e_l * x = x$ pro vš. x
4. má pravý neutrální prvek e_r , když $x * e_r = x$ pro vš. x
5. má neutrální prvek e , když $e * x = x * e = x$ pro vš. x

Tvrzení: $\langle X, * \rangle$ grupoid. At' $*$ má e_l a e_r . Potom $e_l = e_r$

Důkaz: víme $e_l * x = x$ pro vš. x
 $x * e_r = x$ pro vš. x
 $e_l * e_r = e_r$ ale $e_l * e_r = e_l$ Takže $e_l = e_r$

Důsledek: Grupoid $\langle X, * \rangle$ má max 1 neutrální prvek.

Př: $\{a, b, c\}$ $x * y := x$ NEMÁ ŽÁDNÝ neutrální prvek.

- Def: 1. Grupoid $\langle X, * \rangle$ s asociativní $*$ se nazývá pologrupa.
 2. Pologrupa $\langle X, * \rangle$ s neutrálním prvkem se jmenuje monoid.
 3. Monoid $\langle X, *, e \rangle$ s inversem se jmenuje GRUPA.
 $(-)^{-1} : X \rightarrow X$ s vlastností $x * x^{-1} = x^{-1} * x = e$

- Př: 1. Grupa \rightarrow monoid \rightarrow pologrupa \rightarrow grupoid
 2. Monoidy = „modely“ LIST. Σ^* — — zřetězování je asoc. E je neutr.
 $\langle F, \circ, id \rangle$ je monoid. Jak porovnat různé modely? (Homomorfismus)

3. grupoid, který není pologrupa

$$X = \mathbb{N} \quad x * y = x^y$$

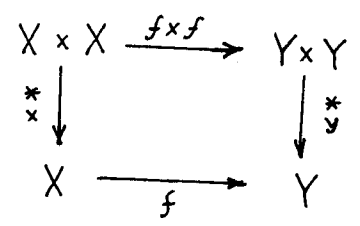
$$2^8 = 2^{(2^3)} = 2 * (2 * 3) \neq (2 * 2) * 3 = (2^2)^3 = 2^6$$

4. pologrupa, která není monoid

$$\{a, b, c\} \quad x * y := x \quad x * (y * z) = x, \quad (x * y) * z = x * z = x$$

5. Monoid, který není grupa $\langle \mathbb{Z}_4, \cdot \rangle$

! Def.: At' $\langle X, *_x \rangle$ a $\langle Y, *_y \rangle$ jsou grupoidy. Homomorfismus z $\langle X, *_x \rangle$ do $\langle Y, *_y \rangle$ je 1. $f: X \rightarrow Y$ & 2. $f(x *_x x') = f(x) *_y f(x')$ pro vš. x, x'

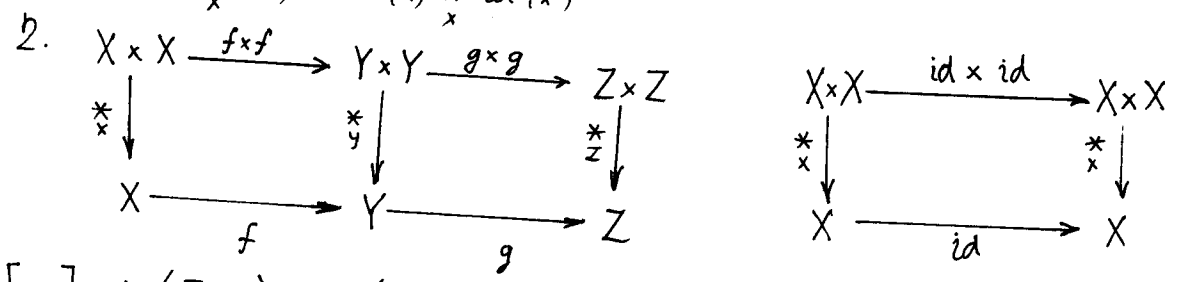


Trzení: Složení homomorfismů grupoidů je homomorfismus grupoidů. Identické zobrazení je homomorfismus grupoidů.

Důkaz: 1. $f: \langle X, *_x \rangle \rightarrow \langle Y, *_y \rangle, \quad g: \langle Y, *_y \rangle \rightarrow \langle Z, *_z \rangle$

$$g(f(x *_x x')) = g(f(x) *_y f(x')) = g(f(x)) *_z g(f(x'))$$

$$id(x *_x x') = id(x) *_x id(x')$$



Př: 1. $[-]_6: \langle \mathbb{Z}, \cdot \rangle \rightarrow \langle \mathbb{Z}_6, \odot_6 \rangle, \quad [z \cdot z']_6 = [z]_6 \odot_6 [z']_6$

2. $\langle \mathbb{R}, \cdot \rangle \rightarrow \langle \mathbb{R}, \cdot \rangle$

$$f: \mathbb{R} \rightarrow \mathbb{R} \text{ NENÍ homomorfismus}$$

$$1 \mapsto 128 \quad 128 = f(1 \cdot 1) = f(1) \cdot f(1) = 128^2$$

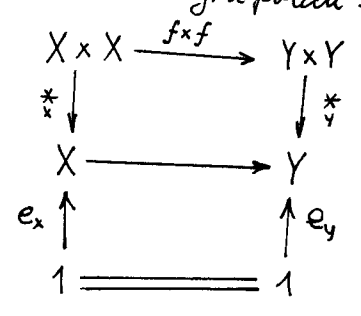
Trzení: $f: \langle X, *_x \rangle \rightarrow \langle Y, *_y \rangle$ homomorf. grupoidů a at' $\langle X, *_x \rangle$ a $\langle Y, *_y \rangle$ jsou pologrupy. Pak f „respektuje asociativitu“.

Důkaz: $x *_x (y *_x z) = (x *_x y) *_x z$

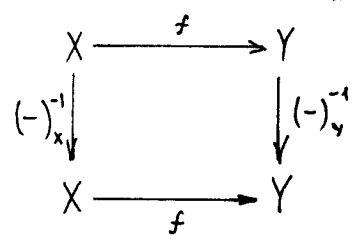
$$f(x) *_y (f(y) *_y f(z)) = (f(x) *_y f(y)) *_y f(z)$$

Definice: 1. Homomorfismus pologrup je homomorfismus grupoidů.

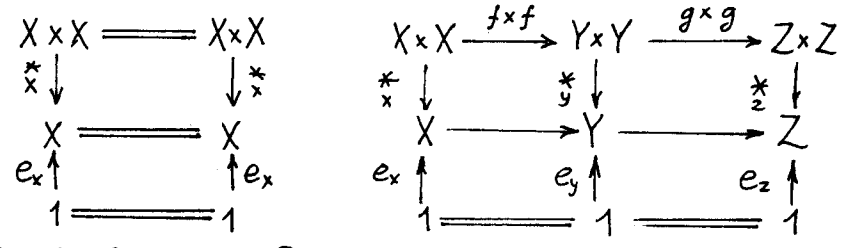
2. $f: \langle X, *_x, e_x \rangle \rightarrow \langle Y, *_y, e_y \rangle$



3. $f: \langle X, *_x, e_x, (-)_x^{-1} \rangle \rightarrow \langle Y, *_y, e_y, (-)_y^{-1} \rangle$ je hom. monoidů



Důkaz: pro monoidy:



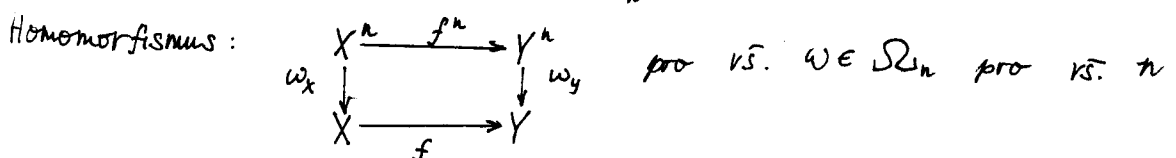
Def.: FINITÁRNÍ typ Ω je posloupnost $\Omega_0, \Omega_1, \dots$ navzájem disjunktních množin. Prvkům Ω_n říkáme formální operace arity n .

Př.: $\Omega_2 = \{*\}$, $\Omega_n = \emptyset$ pro $n \neq 2$
finitární typ, modely jsou grupy

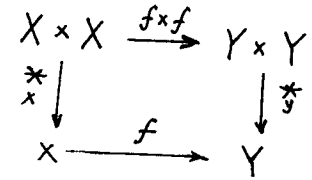
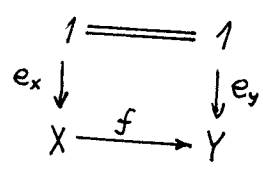
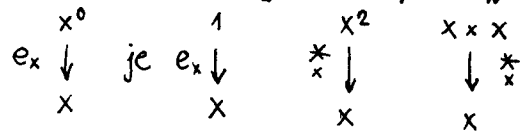
Značení: $X^0 := 1$, $X^{n+1} := X \times X^n$, $X^0 \xrightarrow{f^0} Y^0$ je $1 \xrightarrow{id} 1$
 $X^{n+1} \xrightarrow{f^{n+1}} Y^{n+1}$ je $X \times X^n \xrightarrow{f \times f^n} Y \times Y^n$

Definice: At Ω je finitární typ. Algebra typu Ω je množina X s kolekcí

$\omega_x: X^n \rightarrow X$ pro vš. $\omega \in \Omega_n$ pro vš. n



Př.: $\Omega_0 = \{e\}$, $\Omega_2 = \{*\}$, $\Omega_n = \emptyset$ $n \neq \{0, 2\}$



Př.: Modely ASSOCIATIVE = pogrupy

Pogruba $\langle \mathbb{Z}_6, + \rangle$

pro vš. $x_1, x_2, x_3 \in \mathbb{Z}_6$: $1 + (3 + 0) = (1 + 3) + 0$
 $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$

$$\begin{array}{ccccc} \uparrow & \uparrow & & \uparrow & \uparrow \\ n_1 & *(n_2 * n_3) & (n_1 * n_2) & * n_3 & \end{array}$$

$\Omega_2 = \{*\}$, $\Omega_n = \emptyset$, $n \neq 2$

Množina formálních proměnných $V = \{n_1, n_2, n_3\}$

interpretace V v \mathbb{Z}_6 : $\rho: V \rightarrow \mathbb{Z}_6$, $n_1 \mapsto 1$, $n_2 \mapsto 3$, $n_3 \mapsto 0$

Spec ASSOCIATIVE is

Sorts: S

operations: $*$: $S \times S \rightarrow S$

variables: n_1, n_2, n_3 : S

equations:

$$n_1 * (n_2 * n_3) = (n_1 * n_2) * n_3$$

end.spec

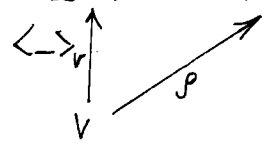
Def.: V množina formálních proměnných, Ω finitární typ. Množinu $T_\Omega(V)$ termů nad V definujeme induktivně:

$$\frac{n \in V}{n \in T_\Omega(V)} \quad \frac{\omega \in \Omega_n \quad t_1, \dots, t_n \in T_\Omega(V)}{\omega(t_1, \dots, t_n) \in T_\Omega(V)}$$

Intuitivně: $t \in T_{\Omega}(V)$ je to co smí stát jako levá nebo pravá strana formální rovnosti.

Pozorování: \mathcal{X} algebra typu Ω s nosnou množinou X a li.b. $\rho: V \rightarrow X$.

Pak $T_{\Omega}(V) \xrightarrow{\rho^*} X$ pro právě jedno ρ^*



Navíc: $T_{\Omega}(V)$ je nosná množina $T_{\Omega}(V)$ a $\rho^*: T_{\Omega}(V) \rightarrow X$

$\Omega_2 = \{*\}$ $\Omega_n = \emptyset$, $\rho^*(v_1 * v_2) = \rho(v_1) + \rho(v_2)$

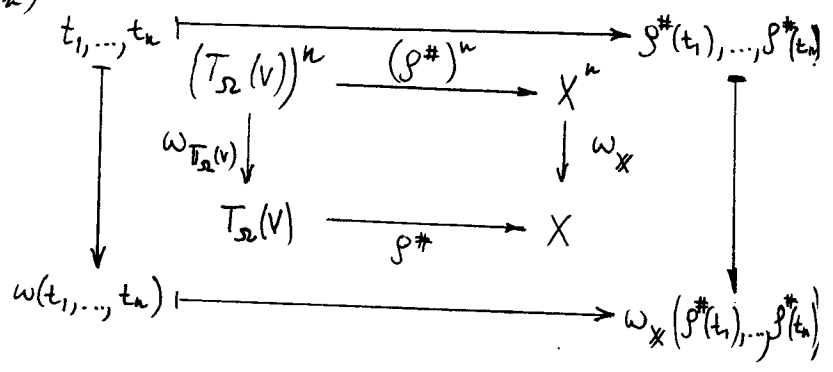
$\rho^*(v_1 * (v_2 * v_3)) = \rho(v_1) + (\rho(v_2) + \rho(v_3))$

- Obecně: 1. $\rho^*(v) = \rho(v)$
 2. $\rho^*(\omega(t_1, \dots, t_n)) = \omega_X(\rho^*(t_1), \dots, \rho^*(t_n))$ Jediné možné rozšíření!

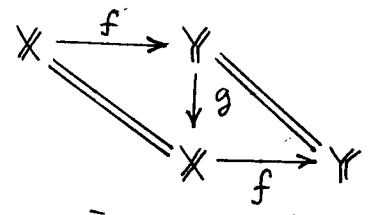
$T_{\Omega}(V)$ jako algebra $\Pi_{\Omega}(V)$

$\omega \in \Omega_n$ $\omega_{T_{\Omega}(V)}: (T_{\Omega}(V))^n \rightarrow T_{\Omega}(V)$
 $t_1, \dots, t_n \mapsto \omega(t_1, \dots, t_n)$

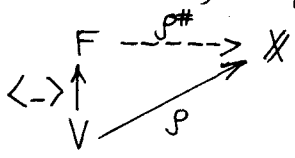
Pro všechna n , pro vš. $\omega \in \Omega_n$



Definice: $f: \mathcal{X} \rightarrow \mathcal{Y}$ je izomorfismus když ek. $g: \mathcal{Y} \rightarrow \mathcal{X}$ tak, že



Def.: Řekneme, že zobrazení $\langle - \rangle: V \rightarrow F$ předkládá algebra F jako volnou algebra nad V , když platí:



pro vš. alg. \mathcal{X} a všedna zotr $\rho: V \rightarrow X$ existuje právě jedno rozšíření na homomorfismus ρ^* .

- Poznámky: 1. $\langle - \rangle: V \rightarrow T_{\Omega}(V)$ předkládá $\Pi_{\Omega}(V)$ jako volnou algebra.
 2. konečná abeceda Σ , Σ^* tvoří monoid (= model LIST)

$\Sigma^* \xrightarrow{\rho^*} X$ $\rho^*(\epsilon) = e$
 $\rho^*(x_1 \dots x_n) = \rho(x_1) \dots \rho(x_n)$

Př.: $\mathcal{X} = (\mathbb{N}, +, 0)$
 $\rho: \Sigma \rightarrow \mathbb{N}$ "váha písmene"
 $\rho^*(\epsilon) = 0$
 $\rho^*(x_1 \dots x_n) = \rho(x_1) + \dots + \rho(x_n)$

Definice: Formální rovnice (v prom. V) je zápis $\forall V. t_1 \approx t_2$, kde $t_1, t_2 \in T_{\Omega}(V)$. Řekneme, že alg. X splňuje $\forall V. t_1 \approx t_2$ ($X \models \forall V. t_1 \approx t_2$), když platí $\rho^*(t_1) = \rho^*(t_2)$ v alg. X pro všechna $\rho: V \rightarrow X$.

Názovok: „slepování“ v $\Pi_{\Omega}(V)$ pomocí kongruencí, tj:

- 1. ekvivalence
- 2. dobrá = respektuje operace

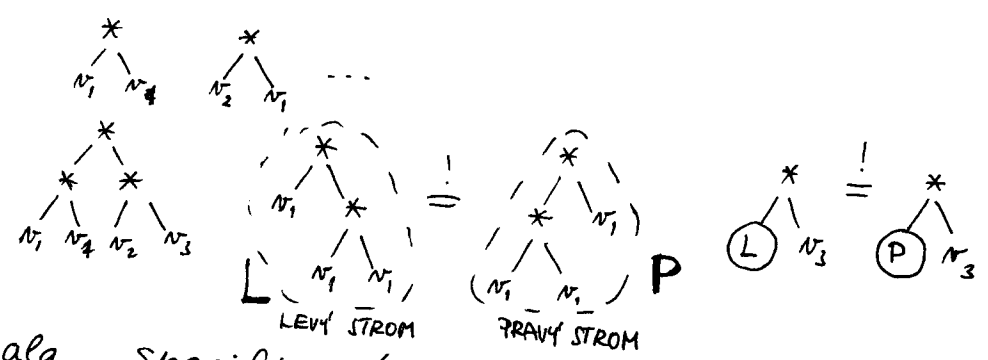
čili R je kongruence

- 1. R je ekvivalence = reflexivní, symetrická a tranzitivní
- 2. $\omega \in \Omega_n, t_1 R t_1', \dots, t_n R t_n'$ pak $\omega(t_1, \dots, t_n) R \omega(t_1', \dots, t_n')$

Trzeme: R je kongruence na $T_{\Omega}(V)$. Pak

- 1. $T_{\Omega}(V)/R$ je algebra
- 2. V případě, že R je generováno nějakou množinou E formálních rovnic, předkládá zobrazení $V \rightarrow T_{\Omega}(V)/R$ algebru $\Pi_{\Omega}(V)/R$ jako volnou algebru mezi všemi algebrymi splňujícími E .

Pr: $V = \{n_1, n_2, n_3\}, \Omega_0 = \{*\}, \Omega_2 = \emptyset$
 $T_{\Omega}(V) \dots n_1, n_2, n_3$



Iniciální sémantika alg. specifikací

alg. (rovnice) specifikace = $\langle \Omega, E \rangle$

↑ konečně mnoho formálních rovnic
 ↑ pouze konečně mnoho formálních operací
 je volná algebra nad $V = \emptyset$ splňující E .
 (=iniciální)

Iniciální sémantika $\langle \Omega, E \rangle$ je volná algebra nad $V = \emptyset$ splňující E .
 $F \xrightarrow{\rho^*} X$
 $! \uparrow$
 \emptyset

No-junk - no-confusion

Spec LIST is

sort : list
 operations : nil : \rightarrow list
 -#- : list x list \rightarrow list

$nil = nil \# nil = nil \# (nil \# nil)$

variables : x, y, z : list

equations : $x \# nil = x$
 $nil \# x = x$
 $x \# (y \# z) = (x \# y) \# z$

endspec

Definice: Modely BASIC-THRUST_VALUES se jmenují svazy.

$$\langle X, \wedge, \vee \rangle$$

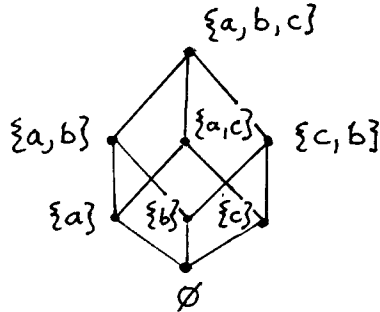
↑ spojení (join)
 ↓ průsek (meet)

Homomorfismus svazu^o = resp, \wedge, \vee

Př.: Jak poznat svaz?

$X = \{a, b, c\}$ exp X ... množina všech podmnožin X
 ↑ uspořádaná \subseteq

Hasseho diagram $\langle \text{exp } X, \subseteq \rangle$



Tvrdíme, že každá dvojice prvků má supremum a infimum

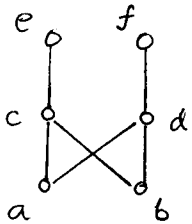
$$\sup \subseteq (\{a, b\}, \{b\}) = \{a, b\}$$

Supremum - nejmenší horní odhad; horní odhady: $\{a, b\}, \{b\} : \{a, b, c\}, \{a, b\}$

infimum - $\inf \subseteq (\{a, b\}, \{c, b\})$; (největší spodní odhad)

dolní odhady: $\emptyset, \{a\}, \{c\}$ (nejm), $\{b\}$... největší $\{b\}$

Př.: $X = \{a, b, c, d, e, f\}$



$\sup \subseteq (e, f)$ neexistuje

$\inf \subseteq (c, d)$ neexistuje (z dolních odhadů nelze vybrat největší)

$$\sup \subseteq (a, c) = c$$

Věta: (I) Ať $\langle X, \wedge, \vee \rangle$ je svaz. Pak platí: $x \wedge y = x$ iff $x \vee y = y$ (pro vš. x, y).

Definujeme-li $x \sqsubseteq y$ iff $x \wedge y = x$ pak $\langle X, \sqsubseteq \rangle$ je poset, kde každá dvojice má sup a inf a navíc $\sup \subseteq \{x, y\} = x \vee y, \inf \subseteq \{x, y\} = x \wedge y$.

(II) Ať $\langle X, \sqsubseteq \rangle$ je poset, kde každá dvojice prvků má sup a inf, pak lze definovat dvě operace $x \wedge y := \inf \subseteq \{x, y\}$ $x \vee y := \sup \subseteq \{x, y\}$. Pak $\langle X, \wedge, \vee \rangle$ je svaz.

Důkaz: (ukázka)

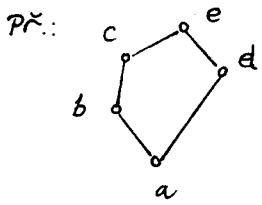
(I) tranzitivita \sqsubseteq , tj. $x \sqsubseteq y$ & $y \sqsubseteq z \rightarrow x \sqsubseteq z$, tím: $x \sqsubseteq y$ & $y \sqsubseteq z \rightarrow x \wedge y = x$ & $y \wedge z = y$, chci: $x \sqsubseteq z \leftrightarrow x \wedge z = x$
 $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$

(II) asociativita \wedge tj. $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, $\underbrace{\inf \subseteq \{x, \inf \subseteq \{y, z\}\}}_L \stackrel{?}{=} \underbrace{\inf \subseteq \{\inf \subseteq \{x, y\}, z\}}_P$

stačí $L \sqsubseteq P$ & $P \sqsubseteq L$ (\rightarrow antisymetrie $L=P$)
 $\inf \subseteq \{x, \inf \subseteq \{y, z\}\} \sqsubseteq \inf \subseteq \{\inf \subseteq \{x, y\}, z\}$ stačí $\inf \subseteq \{x, \inf \subseteq \{y, z\}\}$ je dolní odhad $\inf \subseteq \{x, y\}, z$

(i) $\inf \subseteq \{x, \inf \subseteq \{y, z\}\} \sqsubseteq \inf \subseteq \{x, y\}$, stačí $\inf \subseteq \{x, \inf \subseteq \{y, z\}\}$ je dolní odhad x, y

(ii) $\inf \subseteq \{x, \inf \subseteq \{y, z\}\} \sqsubseteq z$



svaz: ANO

$$ALE: c = c \wedge (b \vee d) \neq (c \wedge b) \vee (c \wedge d) = b \vee a = b$$

$$b = b \vee (c \wedge d) \neq (b \vee c) \wedge (b \vee d) = c \wedge e = c$$

Věta: Ve svazu $\langle X, \wedge, \vee \rangle$ je ekvivalentní:

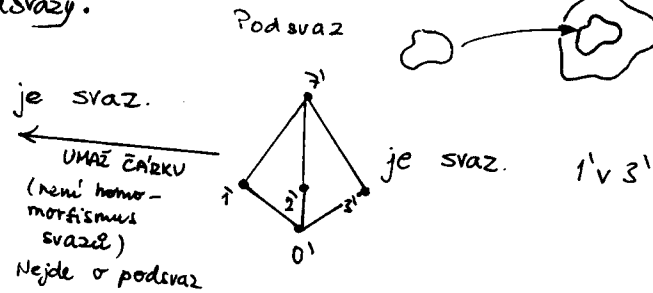
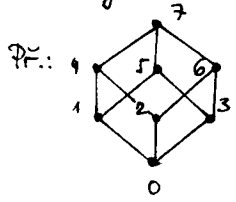
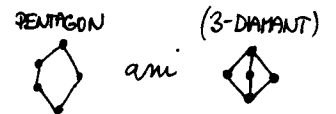
1. pro vs. x, y, z : $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
2. pro vs. x, y, z : $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Důkaz: 2. \rightarrow 1.

$$\underbrace{(x \wedge y) \vee (x \wedge z)}_{\text{ABSORBE}} \stackrel{(2)}{=} ((x \wedge z) \vee x) \wedge ((x \wedge z) \vee z) \stackrel{\text{ABSORBE}}{=} x \wedge ((x \vee z) \wedge (y \vee z)) \stackrel{\text{ASOCIATIVITA}}{=} (x \wedge (x \vee z)) \wedge (y \vee z) = x \wedge (y \vee z)$$

Def: Modely DISTR-TRUTH-VALUES jsou distributivní svazy.

Věta: At' $\langle X, \wedge, \vee \rangle$ je svaz. Pak jde o distributivní svaz iff neobsahuje pentagon ani 3-diamant.



je svaz.
UMAZ ČAROU (nemí homomorfismus svazů)
Nejde o podsvaz

$1 \vee 3 = 7$ ALE $1 \vee 3 = 5$

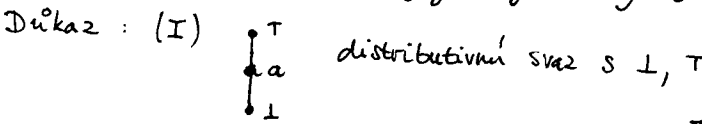
Intuitivní význam rovnosti v CLASSICAL-TRUTH-VALUES

- 9-16 jako ve svazu
- 17* and, or jako v distr. svazu
- 18 $x \in \text{true}$
- 19 false \in
- 20 true
- 21 x false negation(x)

nejmenším (bottom) a největším (top) prvkem.

Pozorování: $\langle X, \wedge, \vee, \perp, \top \rangle$

Pak pro vs. x ex. nejvýše jedno y s vlastnostmi: $x \wedge y = \perp$ & $x \vee y = \top$



hledáme pro a nějaké y :

- $y = \top$ $a \wedge \top \neq \perp$
- $y = a$ $a \wedge a \neq \perp$
- $y = \perp$ $a \vee \perp \neq \top$

(II) at'

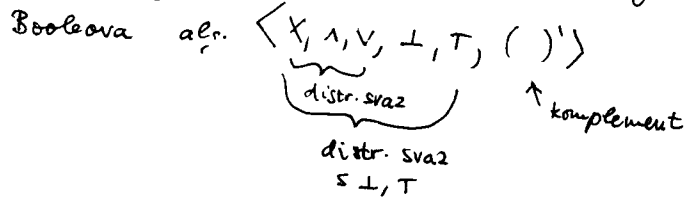
$$x \wedge y_1 = \perp \quad x \wedge y_2 = \perp$$

$$x \vee y_1 = \top \quad x \vee y_2 = \top$$

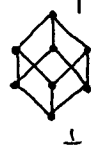
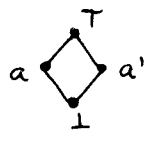
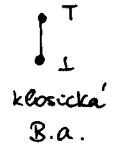
$$y_1 = y_1 \wedge \top = y_1 \wedge (x \vee y_2) = (y_1 \wedge x) \vee (y_1 \wedge y_2)$$

$$= (y_2 \wedge x) \vee (y_1 \wedge y_2) = y_2 \wedge (x \vee y_2) = y_2 \wedge \top = y_2$$

Def: Modely CLASS-TRUTH-VALUES jsou Booleany algebry.



Př.: $\perp = T$
 Booleana alg.



$\langle \text{exp}(\emptyset), \subseteq \rangle$
 \emptyset

$\langle \text{exp} \{a\}, \subseteq \rangle$
 \emptyset
 $\{a\}$

$\langle \text{exp} \{a, b\}, \subseteq \rangle$
 $\{a\}$
 $\{b\}$
 $\{a, b\}$

$\langle \text{exp} \{a, b, c\}, \subseteq \rangle$

Tvrzení: Každá konečná Booleana algebra je izomorfní $\langle \text{exp}(M), \subseteq \rangle$ pro nějakou konečnou M.

$S \neq \emptyset$ (množina sort)

Př.: $\text{push}(-, -) : \text{alphabet}, \text{stack} \rightarrow \text{stack}$

Připomenutí: n-ární formální operace $\omega \in \Omega_n$ bylo interpretována $\omega_x : X^n \rightarrow X$

Def.: S-sortová množina $X = \langle X_s \mid s \in S \rangle$ systém vzájemně disj. množin.

S-sortové zobrazení: $f : X \rightarrow Y$

$f = \langle f_s \mid s \in S \rangle$
 $f_s : X_s \rightarrow Y_s$

$S = \{s\}$ $X^3 = X^{sss} := X_s \times X_s \times X_s$

arita: (w, s)
 $w \in S^+$ $s \in S$
 $\Omega(w, s)$

$\omega \in \Omega(w, s)$ $\omega_x : X^w \rightarrow X_s$

$X^w = X_{s_1} \times X_{s_2} \times \dots \times X_{s_n}$ $w = s_1 \dots s_n$
 $X^\epsilon = 1$

Predikátová logika (Mat. logika kap. 11, 12, 14)

Resoluční algoritmus

Problém: M (konečná) množina sentencí P.L. φ sekvence P.L.
 Plati $M \models \varphi$?

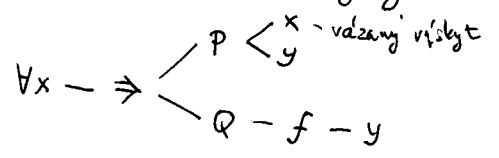
Plati věta (důkaz sporem): $M \models \varphi$ iff $X = M \cup \{\neg \varphi\}$ je nesplnitelná

ČISTĚ SYNTAKTICKÝ
 (RESOLUČNÍ ALGORITMUS)

0. rozecení sentencí (popis jazyka P.L.)
1. úprava na kausální tvar pro CNF
2. resolventy kloumání (unifikace)

Ad. 0.: Př.: $\forall x (P(x, y) \Rightarrow Q(f(y)))$ Je to formule P.L.? NE: neznám jazyk

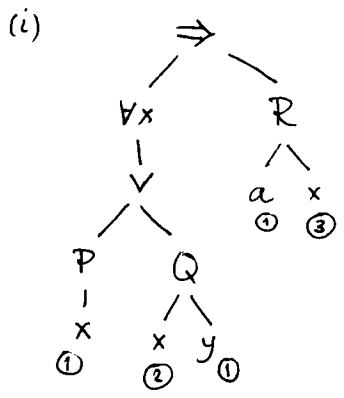
jazyk
 predik. symboly: P ar 2; Q ar 1
 fcní. symboly: y ar 0; f ar 1
 std. prom: x



Je to sentence? ANO, protože všechny výskyt všechny proměnných jsou vázane. 34

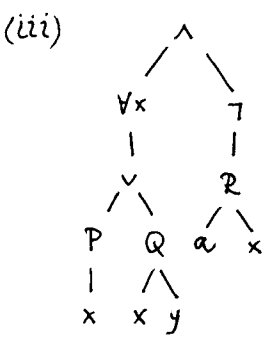
Ad. 0.: Pr.: $(\forall x (P(x) \vee Q(x,y))) \Rightarrow R(a,x)$

- (i) popište jazyk ve kterém jde o formuli.
- (ii) je to sentence
- (iii) znegujte



jazyk:
 predikáty P ar 1, Q ar 2, R ar 2
 fcní symb.
 proměnné: x, y, a

- (ii) prom x: ①, ② vázane; ③ volný výskyt
- prom y: ① volný výskyt
- prom a: ① volný výskyt



Ad. 0. Pr.: Někteří studenti nemluví ani německy ani španělsky.
 Zformalizujte v P.L.

jazyk	interpretace
predikát: N(x) ar 1	D... studenti student x mluví německy student x mluví španělsky
S(x) ar 1	
prom: x	
$\exists x (\neg N(x) \wedge \neg S(x))$	Někteří studenti...

Ad. 0. Pr. ! Zformalizujte v P.L.
 1. Všichni vražedci jsou šílenci.
 2. Jekyll je Hyde.
 3. Hyde je vrah.

jazyk	interpretace
predik.: V(x) ar 1	D... lit. postavy x je vrah x je šílený
S(x) ar 1	
fnzní symb: h ar 0	- Hornost (NEJDE JINAK) Hyde Jekyll
j ar 0	
prom: x	
$\forall x (V(x) \Rightarrow S(x))$	(1)
$j = h$	(2)
$V(h)$	(3)

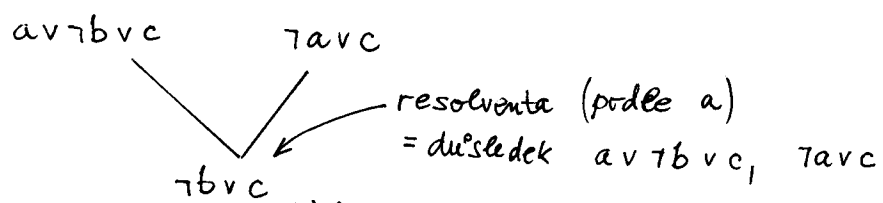
Ad. 0. PŘ.: Zformalizujte v P.L.: Kdo jine'mu ja'mu kopa', se'm do ni' pada'.

jazyk	interpretace
predik: $\check{C}(x)$	x je \check{C} lovek
$J(x)$	x je ja'ma
= pred. rovnosti	
$K(x,y,z)$	
$P(x,y)$	

$$\forall x \forall y \forall z ((\check{C}(x) \wedge J(x) \wedge \check{C}(z)) \Rightarrow ((\neg(x=z) \wedge K(x,y,z)) \Rightarrow P(x,y)))$$

Ad. 1. PŘ.: $A_t = \{a, b, c\}$
 $a \vee \neg b \vee c$ - klousule pro CNF

CNF $\alpha \equiv \underbrace{\quad}_{\text{klousule pro CNF}} \wedge \dots \wedge \underbrace{\quad}_{\text{klousule pro CNF}}$

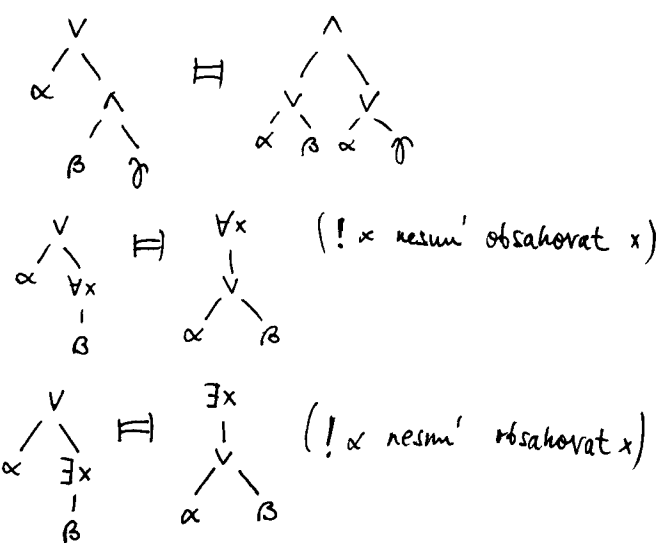
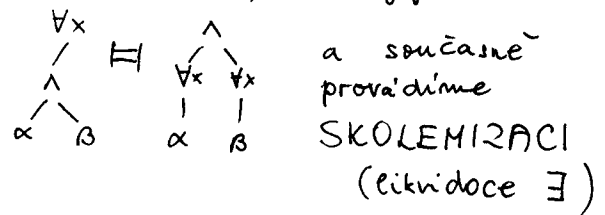


Ad. 1. PŘ.: a

	$a \vee \neg b \vee c$	$\neg a \vee c$	Za'ver
1	1	1	1
0	1	1	1

$(\quad) \wedge (\quad) \wedge \dots \wedge (\quad)$
 klousule pro CNF
 $\hookrightarrow \forall x_1, \forall x_2, \dots, \forall x_n (L_1 \vee L_2 \vee \dots \vee L_k)$
 litera'l

- Ad. 1. Na'vrh postupu pro hleda'ní CNF
1. x -konverze: ka'zdy' kvantifikato'r at' kvantifikuje jinou prome'nou (fresh prome'na')
 2. Na'hra'dou spojku za \wedge, \vee, \neg
 3. \neg co nejnu'ize
 4. \vee (disjunkci) co nejnu'ize
 5. \wedge (a za'roveň) co nejvy'se



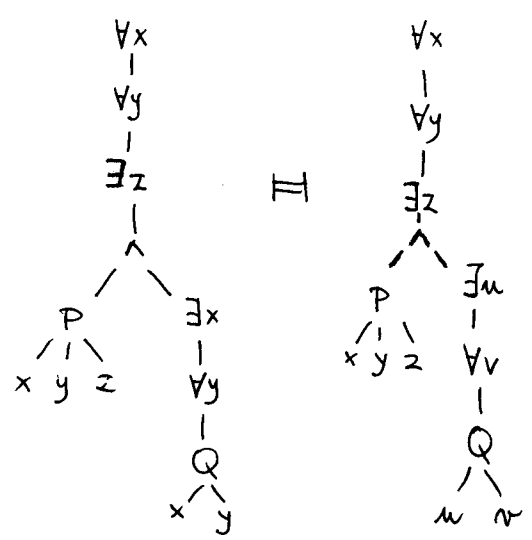
PF: $\int_0^1 x dx = \int_0^1 t dt$

for $i := 1$ to for $j := 1$ to

$\forall x \forall y \exists z (P(x,y,z) \wedge \exists x \forall y Q(x,y))$

pred.: P ar 3
 Q ar 2

prom.: x, y, z



PF: SKOLEMIZACE

(i) $\exists x P(x)$ $P(a)$

pred.: P ar 1

prom.: x

f. symbol: a ar 0 (zavedení konstanty)
 ↑ fresh symbol

(ii) $\forall x \exists y Q(x,y)$ $\forall x Q(x, f(x))$

pred.: Q ar 2

prom.: x, y

funční symb.: f ar 1
 ↑ fresh

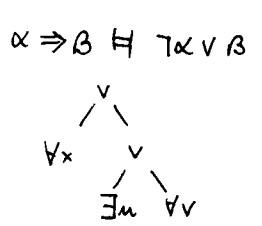
(i) $\forall x_1 \dots \forall x_n \exists y Z(x_1, \dots, x_n, y) \dots \forall x_1 \dots \forall x_n Z(x_1, \dots, x_n, g(x_1, \dots, x_n))$

prom.: x_1, \dots, x_n, y

pred.: Z ar $n+1$

f. s.: g ar n

PF: Převeďte do CNF:



$$\begin{aligned} & (\exists x S(x)) \Rightarrow (\forall x (P(x) \vee Q(x)) \Rightarrow \forall x \exists y T(x,y)) \\ & (\exists x S(x)) \Rightarrow (\forall u (P(u) \vee Q(u)) \Rightarrow \forall v \exists y T(v,y)) \\ & \neg (\exists x S(x)) \vee (\neg \forall u (P(u) \vee Q(u)) \vee \forall v \exists y T(v,y)) \\ & \forall x (\neg S(x)) \vee (\exists u (\neg P(u) \wedge \neg Q(u)) \vee \forall v \exists y T(v,y)) \\ & \forall x (\neg S(x) \vee (\exists u (\neg P(u) \wedge \neg Q(u)) \vee \forall v \exists y T(v,y))) \\ & \forall x (\neg S(x) \vee \forall v (\exists u (\neg P(u) \wedge \neg Q(u)) \vee \exists y T(v,y))) \\ & \forall x (\neg S(x) \vee \forall v (\exists y (\exists u (\neg P(u) \wedge \neg Q(u)) \vee T(v,y)))) \\ & \forall x (\neg S(x) \vee \forall v \exists y \exists u ((\neg P(u) \wedge \neg Q(u)) \vee T(v,y))) \\ & \forall x \forall v \exists y \exists u (\neg S(x) \vee ((\neg P(u) \wedge \neg Q(u)) \vee T(v,y))) \end{aligned}$$

jazyk
pred.: S ar 1
 P ar 1
 Q ar 1
 T ar 1
prom.: x, y, u, v, w

$\forall x \forall v \exists y \exists u (\neg S(x) \vee ((\neg P(u) \vee T(v,y)) \wedge (\neg Q(u) \vee T(v,y)))$
 $\forall x \forall v \exists y \exists u ((\neg S(x) \vee \neg P(u) \vee T(v,y)) \wedge (\neg S(x) \vee \neg Q(u) \vee T(v,y)))$

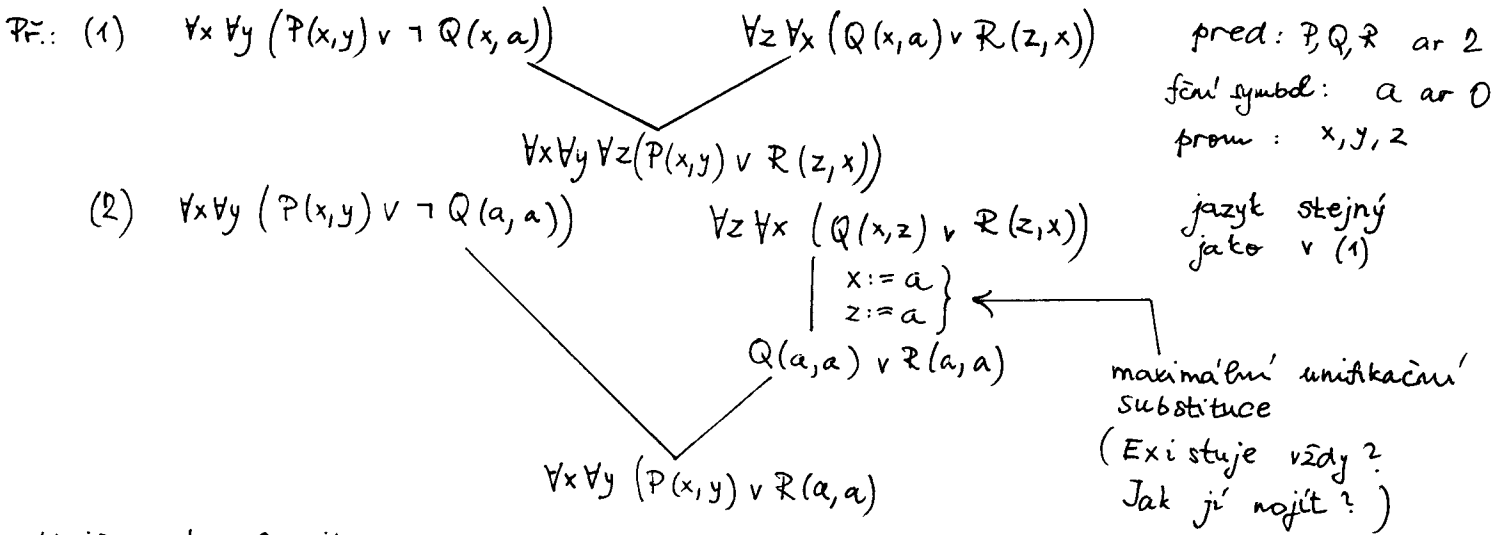
fresh
f. symbol: f ar 2
 g ar 2

$\forall x \forall v ((\neg S(x) \vee \neg P(g(x,v)) \vee T(v, f(x,v))) \wedge (\neg S(x) \vee \neg Q(g(x,v)) \vee T(v, f(x,v))))$
 $\forall x \forall v ((\neg S(x) \vee \neg P(g(x,v)) \vee T(v, f(x,v)))) \wedge \forall x \forall v ((\neg S(x) \vee \neg Q(g(x,v)) \vee T(v, f(x,v))))$

1. klousule 2. klousule

Poznámky: 1. α -konverze, skolemizace mění jazyk! 2. CNF není jednoznačně určena
3. klousalní tvar = seznam jednotlivých klousulí

Počítání resolvent = počítání důsledku



Unifikační algoritmus

vstup: 2 atomické formule

výstup: max. unif. subst. nebo m. u. s. neexistuje

PF: Unifikujte 1.

$Q(a,a)$	$Q(x,z)$	$\neg g := 0$
a, a	x, z	x := a
a, a	a, z	x := a, z := a
a	z	
a	a	x := a, z := a

PF: Unifikujte 2.

$Q(x,y,a)$	$Q(g(v),z,z)$	pred: Q ar 3
x, y, a	g(v), z, z	prom: x, y, v
g(v), y, a	g(v), z, z	f. s.: a ar 0
y, a	z, z	g ar 1
z, a	z, z	x := g(v), y := z
a	z	x := g(v), y := z, z := a
a	a	

PF: ! 3.

$Q(x,y,a)$	$Q(g(x),z,z)$	pred: Q ar 3
x, y, a	g(x), z, z	f. s.: g ar 1
g(x), y, a	g(g(x)), z, z	a ar 0
x, y, a	g(x), z, z	prom: x, y, z

~~x := g(x)~~

STOP! max. unif. subst. neexistuje
 (obecný případ: $x := g(\dots, x, \dots)$)

PF: Unifikujte 4.

$F(a,x)$	$F(f(x),y)$	pred: F ar 2
a, x	f(x), y	f. s.: a ar 0
		f ar 1
		prom: x, y

~~a := f(x)~~

STOP m. u. s. neex.

$f(\dots), \dots, g(\dots), \dots$
 a, \dots, b, \dots

PF: $\{ \forall x (P(x) \vee Q(x)), \exists x \neg P(x) \} \models \exists x Q(x)$

1. z definice

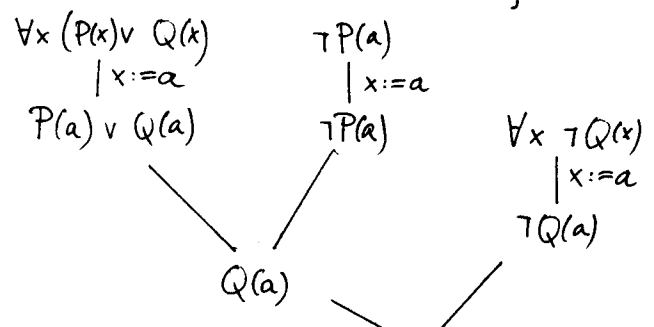
jazyk	klor. interpretace, kde $\forall x (P(x) \vee Q(x)), \exists x \neg P(x)$ jsou pravda	$D \neq \emptyset$
prom: x		
pred: Par 1	$[P] \subseteq D$	
Q ar 1	$[Q] \subseteq D$	
	$[P] \cup [Q] = D$	$D \setminus [P] \neq \emptyset$

Platí tedy $[Q] \neq \emptyset$? Ano: $d \in D \setminus [P]$, pak ale $d \in [Q]$

2. Rezoluce

$X := \{ \forall x (P(x) \vee Q(x)), \exists x \neg P(x), \neg \exists x Q(x) \}$ splnitelnost?

klauzalní tvar (X) = $\{ \forall x (P(x) \vee Q(x)), \neg P(a), \forall x \neg Q(x) \}$



jazyk
 prom: x
 pred: P ar 1
 Q ar 1
 f.s.: a ar 0

F - Není splnitelná
 $\{ \dots \} = \dots$ PLATÍ

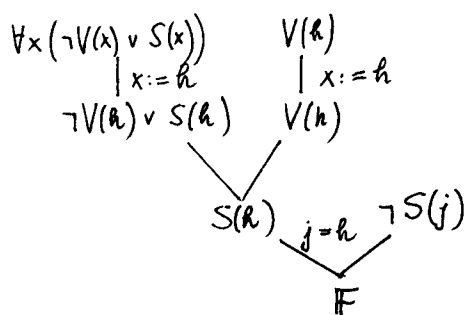
- Př. (1) Všichni vražedci jsou šílenci
 (2) Hyde je vrah
 (3) Jekyll je Hyde

 (4) Jekyll je šílený.

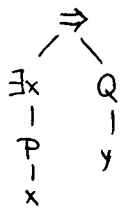
jazyk
 pred: V ar 1
 S ar 1
 = roznost
 f.s.: j ar 0
 h ar 0
 prom: x

$\{ \forall x (V(x) \Rightarrow S(x)), V(h), j=h \} \models S(j)$

splnitelnost $\{ \forall x (V(x) \Rightarrow S(x)), V(h), j=h, \neg S(j) \}$
 $\{ \forall x (\neg V(x) \vee S(x)), V(h), j=h, \neg S(j) \}$

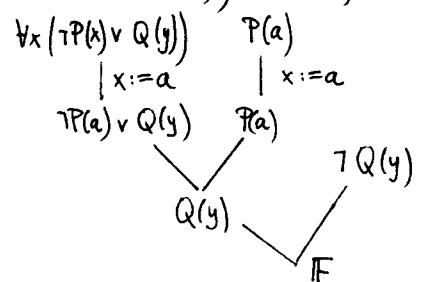


Př.: $(\exists x P(x)) \Rightarrow Q(y) \models \forall x (P(x) \Rightarrow Q(y))$



$\{ (\exists x P(x)) \Rightarrow Q(y), \neg \forall x (P(x) \Rightarrow Q(y)) \}$

$\{ \forall x (\neg P(x) \vee Q(y)), P(a), \neg Q(y) \}$



jazyk
 pred: P ar 1
 Q ar 1
 f.s.: y ar 0, PŘIDÁNÍ a ar 0
 prom: x
 $(\exists x P(x)) \Rightarrow Q(y) \quad \neg \forall x (P(x) \Rightarrow Q(y))$
 $\neg (\exists x P(x)) \vee Q(y) \quad \neg \forall x (\neg P(x) \vee Q(y))$
 $\forall x (\neg P(x)) \vee Q(y) \quad \exists x (P(x) \wedge \neg Q(y))$
 $\forall x (\neg P(x) \vee Q(y)) \quad P(a) \wedge \neg Q(y)$

Poznámka: Obecně (nenalezneme-li prvním stromem F) MUSÍME prozkoumat všechny možnosti vytvářením stromů. Pokud žádný ze stromů nekonečí F, řekneme, že příslušná množina je splnitelná.