# UNIVERZÁLNÍ ALGEBRA

–"kostra" přednášky Libor Polák, Masarykova Univerzita Brno

## 1 Pojem $\tau$-algebry, kongruence

**Definice 1.1** *Systém $\tau = (n_\sigma)_{\sigma\in\Sigma}$ nezáporných celých čísel nazýváme **typem**. Zvolíme- li pro každé $\sigma \in \Sigma$ **operační symbol**, řekněme $f_\sigma$, hovoříme o **jazyku**; označení $\mathcal{L} = ((f_\sigma)_{\sigma\in\Sigma}; (n_\sigma)_{\sigma\in\Sigma})$. Často je $\Sigma = \{1, ..., m\}$. Pak máme $\tau = (n_1, ..., n_m)$ a $\mathcal{L} = (f_1, ..., f_m; n_1, ..., n_m)$.*

***Algebra typu** $\tau$ (nebo stručněji **$\tau$-algebra**) je uspořádaná dvojice $\mathcal{A} = (A, (f_\sigma^\mathcal{A})_{\sigma\in\Sigma})$, kde $A$ je množina a pro $\sigma \in \Sigma$ je $f_\sigma^\mathcal{A}$ $n_\sigma$-ární operace na množině $A$.*

**Poznámka 1.1** *Nulární operaci $f : A^\emptyset \to A$, tj. $f : \{\emptyset\} \to A$ chápeme jako výběr prvku z množiny $A$.*

**Definice 1.2** *Nechť $\mathcal{A} = (A, (f_\sigma^\mathcal{A})_{\sigma\in\Sigma})$ je $\tau$-algebra. Relaci ekvivalence $\rho$ na množině $A$ nazýváme **kongruencí** algebry $\mathcal{A}$, platí-li:*

$(\ \forall\ \sigma \in \Sigma\ )\ (\ \forall\ a_1, ..., a_{n_\sigma}, b_1, ..., b_{n_\sigma} \in A\ )$

$(a_1\ \rho\ b_1\ , ...,\ a_{n_\sigma}\ \rho\ b_{n_\sigma}\ \Rightarrow\ f_\sigma^\mathcal{A}(a_1, ..., a_{n_\sigma})\ \rho\ f_\sigma^\mathcal{A}(b_1, ..., b_{n_\sigma}))$ .

**Poznámka 1.2** *Pro $n_\sigma = 0$ je tato podmínka splněna triviálně.*

**Definice 1.3** *Na množině $A/\rho$ definujeme pro $\sigma \in \Sigma$ operaci $f_\sigma^{\mathcal{A}/\rho}$ předpisem*

$$f_\sigma^{\mathcal{A}/\rho}([a_1]_\rho, ..., [a_{n_\sigma}]_\rho) = [f_\sigma^\mathcal{A}(a_1, ..., a_{n_\sigma})]_\rho\ .$$

*$\tau$-algebru $\mathcal{A}/\rho = (A/\rho, (f_\sigma^{\mathcal{A}/\rho})_{\sigma\in\Sigma})$ nazýváme **faktorovou** algebrou algebry $\mathcal{A}$ podle kongruence $\rho$.*

Korektnost plyne okamžitě z definice kongruence.

**Poznámka 1.3** *Kongruence grup odpovídají jejim normálním podgrupám a kongruence okruhů jejich ideálům. Příslušné přiřazení je $\rho \mapsto \widetilde{\rho} = [1]_\rho$ respektive $\rho \mapsto [0]_\rho$. Pro grupu $(G, \cdot)$ je inverze tvaru $\widehat{N} \leftarrow N$, a $\widehat{N}\ b\ \Leftrightarrow\ ab^{-1} \in N$ pro $a, b \in G$. Přitom $(G, \cdot)/\rho$ a $(G, \cdot)/\widetilde{\rho}$ je tatáž grupa.*

**Věta 1.1** *Množina $\mathsf{Con}\,\mathcal{A}$ všech kongruencí algebry $\mathcal{A}$ tvoří vzhledem k množinové inkluzi úplný svaz. Je to úplný podsvaz svazu $(\mathsf{Ekv}\,A, \subseteq)$ všech ekvivalencí na množině $A$.*

*Důkaz.* ...

**Poznámka 1.4** *Libovolnou množinou $M$, $M \subseteq A\times A$ lze **generovat** kongruenci algebry $\mathcal{A}$.*

**Lemma 1.1** *Pro $\rho \in \mathsf{Con}\,\mathcal{A}$ platí $(\mathsf{Con}\,(\mathcal{A}/\rho), \subseteq) \cong (\{\tau \in \mathsf{Con}\,\mathcal{A} \mid \tau \supseteq \rho\}, \subseteq)$. Příslušný izomorfismus a jeho inverze jsou dány vztahy*

$$\sigma \mapsto \widetilde{\sigma},\ a\ \widetilde{\sigma}\ b\ \Leftrightarrow\ [a]_\rho\ \sigma\ [b]_\rho \text{ pro } a, b \in A \quad \widehat{\tau} \leftarrow \tau,\ [a]_\rho\ \widehat{\tau}\ [b]_\rho\ \Leftrightarrow\ a\ \tau\ b \text{ pro } a, b \in A\ .$$

*Navíc $(\mathcal{A}/\rho)/\widehat{\tau} \cong \mathcal{A}/\tau$.*

*Důkaz.* . .



## 2 Podalgebry

**Definice 2.1** *Nechť $\mathcal{A} = (A, (f_\sigma^\mathcal{A})_{\sigma\in\Sigma})$ a $\mathcal{B} = (B, (f_\sigma^\mathcal{B})_{\sigma\in\Sigma})$ jsou $\tau$-algebry. $\mathcal{B}$ nazveme **podalgebrou** algebry $\mathcal{A}$, platí-li:*

*(i)* $B \subseteq A$,

*(ii)* $(\ \forall\ \sigma \in \Sigma,\ b_1, \ldots, b_{n_\sigma} \in B)\ f_\sigma^\mathcal{B}(b_1, ..., b_{n_\sigma}) = f_\sigma^\mathcal{A}(b_1, ..., b_{n_\sigma})$.

*Píšeme $\mathcal{B} \leq \mathcal{A}$.*

**Definice 2.2** *Nechť $\mathcal{A} = (A, (f_\sigma^\mathcal{A})_{\sigma\in\Sigma})$ je $\tau$-algebra. Množinu $B$ nazveme **nosičem podalgebry** algebry $\mathcal{A}$, platí-li:*

*(i)* $B \subseteq A$,

*(ii)* $(\ \forall\ \sigma \in \Sigma,\ b_1, \ldots, b_{n_\sigma} \in B)\ f_\sigma^\mathcal{A}(b_1, ..., b_{n_\sigma}) \in B$.

*Píšeme $B \leq \mathcal{A}$.*

**Poznámka 2.1** *Zřejmě platí:*

*1. Je-li $\mathcal{B} = (B, (f_\sigma^\mathcal{B})_{\sigma\in\Sigma})$ podalgebra algebry $\mathcal{A} = (A, (f_\sigma^\mathcal{A})_{\sigma\in\Sigma})$, je $B$ nosič podalgebry algebry $\mathcal{A}$.*

*2. Je-li $B$ nosič podalgebry algebry $\mathcal{A}$, je $(B, (f_\sigma^\mathcal{A}|B^{n_\sigma})_{\sigma\in\Sigma})$ její podalgebrou.*

**Věta 2.1** *Množina $S\mathcal{A}$ všech nosičů podalgeber algebry $\mathcal{A}$ tvoří vzhledem k množinové inkluzi úplný svaz. Infima jsou průniky.*

**Poznámka 2.2** *Libovolnou množinou $M$, $M \subseteq A$ lze **generovat** nosič podalgebry algebry $\mathcal{A}$.*

## 3 Homomorfismy

**Definice 3.1** *Nechť $\mathcal{A} = (A, (f_\sigma^\mathcal{A})_{\sigma\in\Sigma})$ a $\mathcal{B} = (B, (f_\sigma^\mathcal{B})_{\sigma\in\Sigma})$ jsou $\tau$-algebry. Zobrazení $\alpha : A \to B$ nazýváme **$\tau$-homomorfismem**, platí-li:*

$$(\ \forall\ \sigma \in \Sigma,\ a_1, ..., a_{n_\sigma} \in A) \quad \alpha(f_\sigma^\mathcal{A}(a_1, ..., a_{n_\sigma})) = f_\sigma^\mathcal{B}(\alpha(a_1), ..., \alpha(a_{n_\sigma}))\ ;$$

*píšeme $\alpha : \mathcal{A} \to \mathcal{B}$. Dále:*
***izomorfismus** = bijektivní homomorfismus,*
***endomorfismus** = homomorfismus do sebe,*
***automorfismus** = izomorfismus do sebe.*
*$\tau$-algebry $\mathcal{A}$ a $\mathcal{B}$ jsou **izomorfní**, existuje-li $\tau$-izomorfismus $\alpha : \mathcal{A} \to \mathcal{B}$; píšeme $\mathcal{A} \cong \mathcal{B}$ a konečně $\mathcal{B}$ je **homomorfní obraz** algebry $\mathcal{A}$, existuje-li surjektivní $\tau$-homomorfismus $\alpha : \mathcal{A} \to \mathcal{B}$.*

**Poznámka 3.1**

*(i) Nechť* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ *a* $\rho \in \mathsf{Con}\,\mathcal{A}$. *Pak zobrazení*

$$\rho^\# : A \to A/\rho,\ a \mapsto [a]_\rho$$

*je surjektivní homomorfismus* $\mathcal{A}$ *na* $\mathcal{A}/\rho$ *– nazýváme ho* ***přirozený homomorfismus na faktoralgebru****.*

*(ii) Je-li dále* $\mathcal{B} = (B, (f_\sigma^{\mathcal{B}})_{\sigma\in\Sigma})$, $\mathcal{B} \leq \mathcal{A}$, *pak zobrazení* $\iota : B \to A,\ b \mapsto b$ *je injektivní homomorfismus* $\mathcal{B}$ *do* $\mathcal{A}$ *– nazýváme ho* ***přirozené vnoření****.*

**Lemma 3.1 (o faktorizaci)** *Nechť* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ *a* $\mathcal{B} = (B, (f_\sigma^{\mathcal{B}})_{\sigma\in\Sigma})$ *jsou* $\tau$*-algebry, nechť* $\alpha : \mathcal{A} \to \mathcal{B}$ *je* $\tau$*-homomorfismus, nechť* $\rho \in \mathsf{Con}\,\mathcal{A}$, $\rho \subseteq \ker\alpha = \{(a,a') \in A^2 \mid \alpha(a) = \alpha(a')\}$. *Pak* $[a]_\rho \mapsto \alpha(a)$ *definuje (jediný) homomorfismus* $\beta : \mathcal{A}/\rho \to \mathcal{B}$ *takový, že* $\beta \circ \rho^\# = \alpha$. *Podmínka* $\ker\alpha \supseteq \rho$ *je pro faktorizaci nutná.*

*Důkaz.* . .

**Věta 3.1 (o homomorfismu)** *Nechť* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ *a* $\mathcal{B} = (B, (f_\sigma^{\mathcal{B}})_{\sigma\in\Sigma})$ *jsou* $\tau$*-algebry, nechť* $\alpha : \mathcal{A} \to \mathcal{B}$ *je* $\tau$*-homomorfismus. Pak* $\ker\alpha \in \mathsf{Con}\,\mathcal{A}$, $\alpha(A) \leq \mathcal{B}$ *a zobrazení* $\beta : A/\ker\alpha \to \alpha(A)$, $[a]_{\ker\alpha} \mapsto \alpha(a)$ *je izomorfismus* $\mathcal{A}/\ker\alpha$ *na* $\alpha(\mathcal{A})$ *splňující* $\alpha = \iota \circ \beta \circ (\ker\alpha)^\#$. *Přitom* $\alpha(\mathcal{A})$ *je podalgebra algebry* $\mathcal{B}$ *na nosiči* $\alpha(A)$ *a* $\iota : \alpha(\mathcal{A}) \to \mathcal{B}$ *je přirozené vnoření.*

*Důkaz.* . .

**Důsledek 3.1** *Homomorfní obrazy dané algebry jsou až na izomorfismus právě její faktoralgebry.*

# 4 Součiny a podpřímé součiny

**Definice 4.1** *Nechť* $\mathcal{A}_i = (A_i, (f_\sigma^{\mathcal{A}_i})_{\sigma\in\Sigma})$ *je* $\tau$*-algebra pro* $i \in I$. *Na množině* $A = \prod_{i\in I} A_i$ *pro* $\sigma \in \Sigma$ *definujme operaci* $f_\sigma^{\mathcal{A}} : A^{n_\sigma} \to A$ *vztahem*

$$f_\sigma^{\mathcal{A}}((a_i^1)_{i\in I}, ..., (a_i^{n_\sigma})_{i\in I}) = (f_\sigma^{\mathcal{A}_i}(a_i^1, ..., a_i^{n_\sigma}))_{i\in I}\ .$$

$\tau$*-algebru* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ *nazýváme* ***součinem*** *systému algeber* $(\mathcal{A}_i)_{i\in I}$. *Píšeme* $\mathcal{A} = \prod_{i\in I} \mathcal{A}_i$ *a pro* $I = \{1, ..., m\}$ *názorněji* $\mathcal{A}_1 \times ... \times \mathcal{A}_m$. *Zobrazení* $\varepsilon_i : A \to A_i$, $(a_j)_{j\in I} \mapsto a_i$ *nazýváme* $i$***-tou projekcí****. Platí, že v případě* $A_i \neq \emptyset$ *pro* $i \in I$ *je to surjektivní homomorfismus* $\mathcal{A}$ *na* $\mathcal{A}_i$. *(AC)*

*Je-li* $\mathcal{B} = (B, (f_\sigma^{\mathcal{B}})_{\sigma\in\Sigma})$ *podalgebra algebry* $\mathcal{A}$ *taková, že všechny* $\varepsilon_i|B : B \to A_i$ *jsou surjektivní, hovoříme o* ***podpřímém součinu****.*

**Věta 4.1** *Nechť* $\mathcal{B}$ *je podpřímým součinem systému* $(\mathcal{A}_i)_{i\in I}$, $I \neq \emptyset$. *Pak* $\bigcap_{i\in I} \ker(\varepsilon_i|B) = \Delta_B$.



*Důkaz.* .

**Věta 4.2** *Nechť* $\rho_i \in \mathsf{Con}\,\mathcal{B}$, $i \in I$, $I \neq \emptyset$., $\bigcap_{i\in I} \rho_i = \Delta_B$. *Pak* $\mathcal{B}$ *je izomorfní s podpřímým součinem systému* $(\mathcal{B}/\rho_i)_{i\in I}$.

*Důkaz.* .

**Definice 4.2** *Netriviální algebru* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ *(t.j.* $|A| \geq 2$*) nazýváme* ***podpřímo nerozložitelnou****, platí-li pro každý neprázdný systém jejích kongruencí* $(\rho_i)_{i\in I}$ *vlastnosti* $\bigcap_{i\in I} \rho_i = \Delta_A$, *že některá z nich je rovna* $\Delta_A$.

**Věta 4.3 (Hlavní věta (AC))** *Každá netriviální algebra je izomorfní podpřímému součinu podpřímo nerozložitelných algeber téhož typu, z nichž každá je homomorfním obrazem této algebry.*

*Důkaz.* . . .

**Věta 4.4** *Dvouprvkový svaz je až na izomorfismus jediným podpřímo nerozložitelným distributivním svazem.*

*Důkaz.* . .

**Důsledek 4.1 (AC)**

*(i) Libovolný distributivní svaz je izomorfní okruhu množin.*

*(ii) Libovolný Booleův svaz je izomorfní poli množin.*

*Důkaz.* . .

# 5 Termy, identity

**Definice 5.1** *Nechť* $\mathcal{L}$ *je jazyk a nechť* $M$ *je množina. Množinu* $F_{\mathcal{L}}(M)$ *všech* $\mathcal{L}$**-slov** *nad* $M$ *definujme induktivně takto:*

*(i)* $M \subseteq F_{\mathcal{L}}(M)$,

*(ii) je-li* $\sigma \in \Sigma$ *a* $p_1, ..., p_{n_\sigma} \in F_{\mathcal{L}}(M)$, *pak i* $f_\sigma(p_1, ..., p_{n_\sigma}) \in F_{\mathcal{L}}(M)$,

*(iii) do* $F_{\mathcal{L}}(M)$ *patří jen to, co vzniklo v konečném počtu kroků (i), (ii).*

*Pro* $\sigma \in \Sigma$ *definujme na této množině operaci* $f_\sigma^{\mathcal{F}_{\mathcal{L}}(M)}$ *vztahem*

$$f_\sigma^{\mathcal{F}_{\mathcal{L}}(M)}(p_1, ..., p_{n_\sigma}) = f_\sigma(p_1, ..., p_{n_\sigma})\ .$$

$\tau$*-algebru*

$$\mathcal{F}_{\mathcal{L}}(M) = (F_{\mathcal{L}}(M), (f_\sigma^{\mathcal{F}_{\mathcal{L}}(M)})_{\sigma\in\Sigma})$$

*nazýváme* $\tau$***-algebrou*** $\mathcal{L}$***-slov*** *nad množinou* $M$ *nebo též* ***absolutně volnou*** $\tau$***-algebrou*** *nad množinou* $M$.

**Definice 5.2** *Nechť* $X = \{x_1, x_2, ...\}$ *je množina tzv.* ***proměnných***, $X_n = \{x_1, ..., x_n\}$, $n$ *nezáporné celé číslo. Prvky množiny* $F_{\mathcal{L}}(X)$ *nazýváme* ***termy*** *a prvky množiny* $F_{\mathcal{L}}(X_n)$ *nazýváme* $n$-***ární termy***.

*Definujeme* ***realizaci*** $p^{\mathcal{A},n}$ *termu* $p \in F_{\mathcal{L}}(X_n)$ *na algebře* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ $n$-*ární operací na množině* $A$ *takto:*

$$\text{pro } a_1, ..., a_n \in A,\ x_i^{\mathcal{A},n}(a_1, ..., a_n) = a_i,$$

$$(f_\sigma(p_1, ..., p_{n_\sigma}))^{\mathcal{A},n}(a_1, ..., a_n) = f_\sigma^{\mathcal{A}}(p_1^{\mathcal{A},n}(a_1, ..., a_n), ..., p_{n_\sigma}^{\mathcal{A},n}(a_1, ..., a_n)) \ .$$

***Identitou*** *rozumíme uspořádanou dvojici* $(p, q)$ *termů; píšeme* $p \simeq q$. *Nechť* $p, q \in F_{\mathcal{L}}(X_n)$. $\tau$-*algebra* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ ***splňuje*** *identitu* $p \simeq q$ *jestliže* $p^{\mathcal{A},n} = q^{\mathcal{A},n}$; *píšeme* $\mathcal{A} \models p \simeq q$.

**Poznámka 5.1** *Pro* $m \geq n$, $a_1, ..., a_m \in A$ *je* $p^{\mathcal{A},m}(a_1, ..., a_m) = p^{\mathcal{A},n}(a_1, ..., a_n)$ – *formální důkaz snadno indukcí – proto výše uvedená definice nezávisí na* $n$.

**Definice 5.3** *Nechť* $\Pi$ *je nějaký systém identit v jazyce* $\mathcal{L}$. *Třídu všech* $\tau$-*algeber splňujících všechny identity z* $\Pi$ *značíme* $\mathsf{Mod}\,\Pi$. *Třídy tohoto tvaru nazýváme* ***variety***. *Pro třídu* $\mathcal{V}$ $\tau$-*algeber značí* $\mathsf{Id}\,\mathcal{V}$ *množinu všech identit platných ve* $\mathcal{V}$. *(Identita platí ve třídě algeber, platí-li v každé algebře této třídy.)*

**Lemma 5.1** *Nechť* $\alpha : \mathcal{A} \to \mathcal{B}$ *je homomorfismus* $\tau$-*algeber,* $p \in F_{\mathcal{L}}(X_n)$. *Pak*

$$(\forall\ a_1, ..., a_n \in A) \quad \alpha(p^{\mathcal{A},n}(a_1, ..., a_n)) = p^{\mathcal{B},n}(\alpha(a_1), ..., \alpha(a_n)) \ .$$

*Důkaz.* Indukcí vzhledem ke složitosti termu $p$.

**Věta 5.1** *Nechť* $\alpha : \mathcal{A} \to \mathcal{B}$ *je surjektivní homomorfismus* $\tau$-*algeber, nechť* $p, q \in F_{\mathcal{L}}(X_n)$ *a nechť* $\mathcal{A} \models p \simeq q$. *Pak také* $\mathcal{B} \models p \simeq q$.

*Důkaz.* Snadno z Lemmatu 1.

**Lemma 5.2** *Nechť* $\mathcal{B} = (B, (f_\sigma^{\mathcal{B}})_{\sigma\in\Sigma})$ *je podalgebra* $\tau$-*algebry* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$, $p \in F_{\mathcal{L}}(X_n)$. *Pak*

$$(\forall\ b_1, ..., b_n \in B) \quad p^{\mathcal{B},n}(b_1, ..., b_n) = p^{\mathcal{A},n}(b_1, ..., b_n) \ .$$

*Důkaz.* Vezměme v Lemmatu 1 za $\alpha$ přirozené vnoření $\iota : \mathcal{B} \to \mathcal{A}$.

**Věta 5.2** *Nechť* $\mathcal{B} = (B, (f_\sigma^{\mathcal{B}})_{\sigma\in\Sigma})$ *je podalgebra* $\tau$-*algebry* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$, $p, q \in F_{\mathcal{L}}(X_n)$, *nechť* $\mathcal{A} \models p \simeq q$. *Pak také* $\mathcal{B} \models p \simeq q$.

*Důkaz.* Okamžitě z Lemmatu 2.

**Lemma 5.3** *Nechť* $(\mathcal{A}_i)_{i\in I}$ *je systém* $\tau$-*algeber,* $I \neq \phi$, $p \in F_{\mathcal{L}}(X_n)$. *Pak*

$$(\forall\ (a_i^1)_{i\in I}, ..., (a_i^n)_{i\in I} \in \prod_{i\in I} A_i)\ p^{\prod_{i\in I}\mathcal{A}_i,n}((a_i^1)_{i\in I}, ..., (a_i^n)_{i\in I}) = (p^{\mathcal{A}_i,n}(a_i^1, ..., a_i^n))_{i\in I} \ .$$



*Důkaz.* Vezměme v Lemmatu 1 za $\alpha$ projekce $\varepsilon_i : \prod_{j\in I}\mathcal{A}_j \to \mathcal{A}_i$.

**Věta 5.3** *Nechť* $(\mathcal{A}_i)_{i\in I}$ *je systém* $\tau$-*algeber,* $p, q \in F_{\mathcal{L}}(X_n)$, *nechť* $(\forall i \in I)\ \mathcal{A}_i \models p \simeq q$. *Pak také* $\prod_{i\in I}\mathcal{A}_i \models p \simeq q$.

*Důkaz.* Okamžitě z Lemmatu 3.

**Věta 5.4** *Nechť* $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ *je* $\tau$-*algebra,* $M \subseteq A$. *Pak nosič podalgebry algebry* $\mathcal{A}$ *generovaný množinou* $M$ *je roven*

$$B = \{\ p^{\mathcal{A},n}(a_1, ..., a_n) \mid n \geq 0,\ p \in F_{\mathcal{L}}(X_n),\ a_1, ..., a_n \in M\ \} \ .$$

*Důkaz.* (i) $M \subseteq B$ neboť $a \in M$ je tvaru $x_1^{\mathcal{A},1}(a)$.

(ii) Nechť $\sigma \in \Sigma$, $n = n_\sigma$ a nechť

$$p_1^{\mathcal{A},m_1}(a_{11}, \ldots, a_{1m_1}), \ldots, p_n^{\mathcal{A},m_n}(a_{n1}, \ldots, a_{nm_n}) \in B \ .$$

Ukážeme, že

$$a = f_\sigma^{\mathcal{A}}(p_1^{\mathcal{A},m_1}(a_{11}, \ldots, a_{1m_1}), \ldots, p_n^{\mathcal{A},m_n}(a_{n1}, \ldots, a_{nm_n})) \in B \ .$$

Nechť $m = m_1 + \cdots + m_n$. Definujme $m$-ární termy

$$q_1 = p_1\langle x_1, \ldots, x_{m_1}\rangle,\ q_2 = p_2\langle x_{m_1+1}, \ldots, x_{m_1+m_2}\rangle, \ldots, q_n = p_n\langle x_{m_1+\cdots+m_{n-1}+1,\ldots,x_m}\rangle \ ,$$

kde $p\langle r_1, \ldots, r_k\rangle$ je term vzniklý z $p$ dosazením termů $r_j$ za $x_j$, $j = 1, \ldots, k$.

Nyní pro $i = 1, \ldots, n$ dostáváme indukcí vzhledem ke složitosti termu $p_i$, že

$$q_i^{\mathcal{A},m}(a_{11}, \ldots, a_{nm_n}) = p_i^{\mathcal{A},m_i}(a_{i1}, \ldots, a_{im_i}) \ .$$

Proto

$$a = f_\sigma^{\mathcal{A}}(q_1^{\mathcal{A},m}(a_{11}, \ldots, a_{nm_n}), \ldots, q_n^{\mathcal{A},m}(a_{11}, \ldots, a_{nm_n})) = (f_\sigma(q_1, \ldots, q_n))^{\mathcal{A},m}(a_{11}, \ldots, a_{nm_n}) \ .$$

(iii) Nechť $C$ je nosič podalgebry algebry $\mathcal{A}$. Indukcí vzhledem ke složitosti termu $p$ dokážeme, že $p^{\mathcal{A},n}(a_1, \ldots, a_n) \in C$.

**Poznámka 5.2**

*1. V předchozí větě lze psát*

$$B = \{p^{\mathcal{A},n}(a_1, ..., a_n) \mid n \geq 0,\ p \in F_{\mathcal{L}}(X_n),\ a_1, ..., a_n \in M \text{ po 2 různá } \} \ .$$

*2. Pro* $M = \{a_1, ..., a_n\}$ *máme dokonce* $B = \{p^{\mathcal{A},n}(a_1, ..., a_n) \mid p \in F_{\mathcal{L}}(X_n)\}$.

Obě tvrzení snadno plynou z předchozí věty.

# 6 Volné algebry

**Definice 6.1** *Nechť $\mathcal{V}$ je třída $\tau$-algeber a $M$ množina. $\tau$-algebru $\mathcal{F} = (F, (f_\sigma^{\mathcal{F}})_{\sigma\in\Sigma})$ nazýváme **volnou nad** $M$ **ve třídě** $\mathcal{V}$ **vzhledem k zobrazení** $\iota$, platí-li:*

*(i) $\iota : M \to F$,*

*(ii) $\mathcal{F} \in \mathcal{V}$,*

*(iii) $\iota(M)$ generuje $\mathcal{F}$,*

*(iv) pro libovolnou $\tau$-algebru $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma}) \in \mathcal{V}$ a pro libovolné zobrazení $\alpha : M \to A$ existuje homomorfismus $\beta : \mathcal{F} \to \mathcal{A}$ tak, že $\beta \circ \iota = \alpha$.*

**Poznámka 6.1**

*1. Často je $M \subseteq F$, $\iota$ přirozené vnoření. Pak říkáme jen, že $\mathcal{F}$ je **volná nad** $M$ **ve třídě** $\mathcal{V}$.*

*2. Vzhledem k Větě 5.4. a podmínce (iii) je zobrazení $\beta$ určeno jednoznačně :*

$$\beta(p^{\mathcal{F},n}(\iota(a_1), \dots, \iota(a_n))) = p^{\mathcal{A},n}(\alpha(a_1), \dots, \alpha(a_n)) \ .$$

*3. Nechť ve $\mathcal{V}$ existuje netriviální (t.j. alespoň 2-prvková) algebra. Pak je zobrazení $\iota$ prosté. (Důkaz. Volme vhodné $\alpha$.)*

**Věta 6.1** *Nechť $\mathcal{F}$, $\mathcal{F}'$ jsou volné nad $M$ ve třídě $\mathcal{V}$ vzhledem k $\iota$ respektive $\iota'$. Pak existuje izomorfismus $\varphi : \mathcal{F} \to \mathcal{F}'$ takový, že $\varphi \circ \iota = \iota'$.*

*Důkaz.* . .

**Věta 6.2** *$\tau$-algebra $\mathcal{F}_{\mathcal{L}}(M)$ je volná nad množinou $M$ ve třídě všech $\tau$-algeber.*

*Důkaz.* . .

**Definice 6.2** *Pro třídu $\mathcal{V}$ $\tau$-algeber klademe*
$\mathsf{H}\,\mathcal{V}$ *– třída všech homomorfních obrazů algeber z $\mathcal{V}$,*
$\mathsf{S}\,\mathcal{V}$ *– třída všech podalgeber algeber z $\mathcal{V}$,*
$\mathsf{P}\,\mathcal{V}$ *– třída všech součinů systémů algeber z $\mathcal{V}$ (včetně prázdného),*
$\mathsf{I}\,\mathcal{V}$ *– třída všech algeber izomorfních algebrám z $\mathcal{V}$.*
*Pravíme, že $\mathcal{V}$ je **uzavřená** vzhledem k operátoru $\mathsf{O}$, platí-li $\mathsf{O}\,\mathcal{V} \subseteq \mathcal{V}$.*

**Věta 6.3** *Nechť $\mathcal{V}$ je třída $\tau$-algeber uzavřená vzhledem k operátorům $\mathsf{S}$, $\mathsf{P}$. Pak nad libovolnou množinou $M$ existuje ve $\mathcal{V}$ volná algebra.*

*Důkaz.* Nechť $(\rho_i)_{i\in I}$ je systém všech kongruencí algebry $\mathcal{F}_{\mathcal{L}}(M)$ takových, že $\mathcal{F}_{\mathcal{L}}(M)/\rho_i \in \mathsf{I}\,\mathcal{V}$. Součin prázdného systému je jednoprvková algebra a proto $I \neq \emptyset$. Nechť $\mathcal{G} = \prod_{i\in I} \mathcal{F}_{\mathcal{L}}(M)/\rho_i$. Pak $\mathcal{G} \in \mathcal{V}$. Nechť $\iota : M \to G$, $a \mapsto (a\rho_i)_{i\in I}$, nechť $\mathcal{F}$ je podalgebra algebry $\mathcal{G}$ generovaná množinou $\iota(M)$. Ukážeme, že $\mathcal{F}$ je volná nad $M$ ve $\mathcal{V}$ vzhledem k $\iota$ (chápanému jako zobrazení do množiny $F$).

Především $\mathcal{F} \in \mathcal{V}$. Nechť $\mathcal{A} \in \mathcal{V}$ a nechť $\alpha : M \to A$.

. . . . . . . . . . . . . . . .



**Lemma 6.1** *Nechť $\mathcal{F}$ je volná nad $M$ vzhledem k $\iota$ ve třídě $\mathcal{V}$ $\tau$-algeber, nechť $p, q \in F_{\mathcal{L}}(X_n)$. Nechť $a_1, ..., a_n \in M$ jsou po dvou různé, nechť*

$$p^{\mathcal{F},n}(\iota(a_1), ..., \iota(a_n)) = q^{\mathcal{F},n}(\iota(a_1), ..., \iota(a_n)) \ .$$

*Pak $p \simeq q \in \mathsf{Id}\,\mathcal{V}$.*

*Důkaz.* . .

**Poznámka 6.2** *Uvedené Lemma mj. říká, že když identita $p \simeq q$, $p, q \in F_{\mathcal{L}}(X_n)$ platí ve volné algebře ve $\mathcal{V}$ nad alespoň n-prvkovou množinou, tak platí v celé varietě. Pozor: volná grupa nad 1-prvkovou množinou je komutativní (je to $(\mathbb{Z}, +)$ ).*

**Lemma 6.2** *Nechť $\mathcal{F}$ je volná nad $M$ vzhledem k $\iota$ ve třídě $\mathcal{V}$ $\tau$-algeber. Pak $\mathcal{F}$ je volná nad $M$ vzhledem k $\iota$ i ve třídě $\mathsf{Mod}\,\mathsf{Id}\,\mathcal{V}$.*

*Důkaz.* . .

**Věta 6.4** *Nechť $\mathcal{V}$ je varieta $\tau$-algeber. Pak relace $\rho = \mathsf{Id}\,\mathcal{V}$ je kongruencí algebry $\mathcal{F}_{\mathcal{L}}(X)$ a $\mathcal{F}_{\mathcal{L}}(X)/\rho$ je volnou algebrou ve $\mathcal{V}$ vzhledem k $\iota : x_i \mapsto [x_i]_\rho$.*

*Důkaz.* . .

**Definice 6.3** *Efektivní popis relace $\mathsf{Id}\,\mathcal{V}$ je **řešením problému identit** pro varietu $\mathcal{V}$.*

**Poznámka 6.3** *Řešení problému identit pro danou varietu nám často nabízí vhodný model volné algebry nad $X$. Tak je tomu například v případě*
*pologrup,*
*komutativních pologrup nad $X_n$,*
*(někdy je popis volné algebry nad $X_n$ více transparentní)*
*polosvazů,*
*pologrup levých nul,*
*rektangulárních bandů,*
*levých normálních bandů,*
*normálních bandů,*
*monoidů,*
*komutativních monoidů nad $X_n$,*
*komutativních grup nad $X_n$,*
*komutativních okruhů nad $X_n$,*
*vektorových prostorů nad daným tělesem nad $X_n$,*
*distributivních svazů,*
*Booleových algeber nad $X_n$.*

# 7 Birkhoffova věta

**Poznámka 7.1** *Nechť $\Pi$, $\Pi'$ jsou systémy identit jazyka $\mathcal{L}$, nechť $\mathcal{V}$, $\mathcal{V}'$ jsou třídy $\tau$-algeber. Pak:*

*(1)* $\Pi \subseteq \Pi' \;\Rightarrow\; \mathsf{Mod}\,\Pi \supseteq \mathsf{Mod}\,\Pi'$.

*(2)* $\mathcal{V} \subseteq \mathcal{V}' \;\Rightarrow\; \mathsf{Id}\,\mathcal{V} \supseteq \mathsf{Id}\,\mathcal{V}'$.

*(3)* $\mathsf{Id}\,\mathsf{Mod}\,\Pi \supseteq \Pi$.

*(4)* $\mathsf{Mod}\,\mathsf{Id}\,\mathcal{V} \supseteq \mathcal{V}$.

**Věta 7.1** *Pro třídu $\mathcal{V}$ $\tau$-algeber je ekvivalentní:*

*(1)* $\mathcal{V}$ *je varieta.*

*(2)* $\mathcal{V}$ *je uzavřená vzhledem k operátorům* $\mathsf{H}, \mathsf{S}, \mathsf{P}$.

*(3)* $\mathsf{Mod}\,\mathsf{Id}\,\mathcal{V} = \mathcal{V}$.

*Důkaz.*
(1) $\Rightarrow$ (2) plyne z Vět 5.1.,5.2. a 5.3.
(3) $\Rightarrow$ (1) dostáváme z definice variety.
(2) $\Rightarrow$ (3): Třída $\mathcal{V}$ je uzavřená na operátory $\mathsf{I}, \mathsf{S}, \mathsf{P}$ a proto podle Věty 6.3. nad libovolnou množinou $M$ existuje volná algebra $\mathcal{F}_{\mathcal{V}}(M)$. Ta je podle Lemmatu 6.2. volná i ve $\mathcal{W} = \mathsf{Mod}\,\mathsf{Id}\,\mathcal{V}$.

Nechť $\mathcal{A} \in \mathcal{W}$ a nechť $M$ je nějaká její množina generátorů. Pak $\mathcal{A} \in \mathsf{H}\,(\mathcal{F}_{\mathcal{V}}(M)) \subseteq \mathcal{V}$.

**Lemma 7.1** *Nechť $\mathcal{V}$ je třída $\tau$-algeber. Pak platí*
$\mathsf{H}\,\mathsf{H}\;V = \mathsf{H}\,\mathcal{V}$, $\mathsf{S}\,\mathsf{S}\,\mathcal{V} = \mathsf{S}\,\mathcal{V}$, $\mathsf{I}\,\mathsf{P}\,\mathsf{P}\,\mathcal{V} = \mathsf{I}\,\mathsf{P}\,\mathcal{V}$, $\mathsf{I}\,\mathsf{I}\,\mathcal{V} = \mathsf{I}\,\mathcal{V}$, $\mathsf{S}\,\mathsf{I}\,\mathcal{V} = \mathsf{I}\,\mathsf{S}\,\mathcal{V}$, $\mathsf{H}\,\mathsf{S}\,\mathcal{V} \supseteq \mathsf{S}\,\mathsf{H}\,\mathcal{V}$, $\mathsf{H}\,\mathsf{P}\,\mathcal{V} \supseteq \mathsf{P}\,\mathsf{H}\,\mathcal{V}$, $\mathsf{S}\,\mathsf{P}\,\mathcal{V} \supseteq \mathsf{P}\,\mathsf{S}\,\mathcal{V}$.

*Důkaz.*
Ukážeme například inkluzi $\mathsf{H}\,\mathsf{S}\,\mathcal{V} \supseteq \mathsf{S}\,\mathsf{H}\,\mathcal{V}$ :
Nechť $\mathcal{A} \in \mathcal{V}$, nechť $\alpha : \mathcal{A} \to \mathcal{B}$ je surjektivní homomorfismus a nechť $C$ je nosič podalgebry algebry $\mathcal{B}$. Pak $\alpha^{-1}(C)$ je nosič podalgebry algebry $\mathcal{A}$ a $\alpha|\alpha^{-1}(C) : \alpha^{-1}(C) \to C$ definuje surjektivní homomorfismus.

**Věta 7.2** *Nechť $\mathcal{V}$ je třída $\tau$-algeber. Pak $\mathsf{H}\,\mathsf{S}\,\mathsf{P}\,\mathcal{V}$ je (vzhledem k inkluzi) nejmenší varieta $\tau$-algeber obsahující třídu $\mathcal{V}$.*

*Důkaz.* .

# 8 Ekvacionální logika

**Definice 8.1** *Identita $\pi$ je **důsledkem** systému identit $\Pi$, platí-li pro každou $\tau$-algebru $\mathcal{A}$: jakmile $\mathcal{A} \models \Pi$, pak i $\mathcal{A} \models \pi$; píšeme $\Pi \models \pi$. Systém identit $\Pi$ je **uzavřený** na důsledky, platí-li: $\Pi \models \pi$ implikuje $\pi \in \Pi$.*



**Poznámka 8.1** *Pro libovolnou třídu $\mathcal{V}$ $\tau$-algeber je $\mathsf{Id}\,\mathcal{V}$ uzavřený systém identit a $\mathsf{Id}\,\mathsf{Mod}\,\Pi$ je (vzhledem k inkluzi) nejmenší uzavřený systém identit obsahující daný systém identit $\Pi$.*

**Definice 8.2** *Kongruence $\rho$ $\tau$-algebry $\mathcal{A} = (A, (f_\sigma^{\mathcal{A}})_{\sigma\in\Sigma})$ je **úplně invariantní**, platí-li*

$$(\forall\; a, b \in A,\;\; \alpha \in \mathsf{End}\,\mathcal{A}) \quad a\; \rho\; b \text{ implikuje } \alpha(a)\; \rho\; \alpha(b)\;.$$

**Věta 8.1** *Nechť $\rho \subseteq F_{\mathcal{L}}(X) \times F_{\mathcal{L}}(X)$. Pak $\rho$ je uzavřený systém identit právě když je úplně invariantní kongruencí algebry $\mathcal{F}_{\mathcal{L}}(X)$.*

*Důkaz.* . . .

**Věta 8.2** *Množina všech variet algeber daného typu tvoří vzhledem k inkluzi tříd úplný svaz (pozor na teorii množin !). Množina všech úplně invariantních kongruencí na $\mathcal{F}_{\mathcal{L}}(X)$ tvoří vzhledem k inkluzi množin též úplný svaz. Zobrazení* $\mathsf{Id}$ *a* $\mathsf{Mod}$ *jsou vzájemně inverzní izomorfismy prvního se svazů na svaz duální ke druhému z nich a zpět.*

*Důkaz.* . .

**Poznámka 8.2** *Máme-li jazyk binárního operačního symbolu $\cdot$ a mezi identitami asociativitu, lze místo (grupoidových) termů uvažovat prvky volné pologrupy $X^+$ nad $X$, tj. konečné neprázdné posloupnosti prvků z $X$. Označme ještě $X^* = X^+ \cup \{\lambda\}$, kde $\lambda$ je symbol pro posloupnost délky 0.*

Následující věta má poněkud jednoduší formulaci pro pologrupy než v obecném případě.

**Věta 8.3 (o úplnosti ekvacionální logiky)** *Pologrupová identita $v \simeq w$ je důsledkem systému (pologrupových) identit $\Pi$, právě když $w$ vznikne z $v$ v konečném počtu kroků tvaru*

$$t \cdot p(s_1, s_2, ...) \cdot u \longrightarrow t \cdot q(s_1, s_2, ...) \cdot u\;,$$

*kde $p \simeq q$ nebo $q \simeq p \in \Pi$, $s_1, s_2, ... \in X^+$, $t, u \in X^*$ a $r(s_1, s_2, ...)$ značí term vzniklý z $r \in X^+$ dosazením $s_i$ za každý výskyt $x_i$.*

*Důkaz.* . .

**Příklad 8.1** *Nechť $\Pi$ se sestává z jediné identity $x^{n+d} \simeq x^n$ $(n, d \in \mathbb{N})$. Pak $\Pi \models v \simeq w$ právě když $w$ vznikne z $v$ v konečném počtu kroků tvaru*

$$ts^{n+d}u \longrightarrow ts^n u$$

*kde $s \in X^+$, $t, u \in X^*$ a kroků k nim inverzních.*

***Ekvacionální klasifikací*** algeber z variety $\mathcal{V}$ rozumíme popis svazu všech podvariet variety $\mathcal{V}$.

Nechť $\mathcal{AG}_n$ $(n \geq 0)$ značí třídu všech komutativních grup splňujících identitu $x^n \simeq 1$. Platí

**Věta 8.4** *Variety komutativních grup jsou právě třídy tvaru $\mathcal{AG}_n$, kde $n \geq 0$. Přitom $\mathcal{AG}_m \subseteq \mathcal{AG}_n$ právě když $m \mid n$.*

*Důkaz.* . .

Poněkud netriviální pojednání o ekvacionální klasifikaci tzv. úplně regulárních pologup naleznete na `http://www.math.muni.cz/~polak`

# 9 Přepisovací systémy

**Definice 9.1** *Nechť $T$ je nějaká neprázdná množina (často množina termů daného jazyka) a nechť $\to$ je relace na této množině. Pravíme, že*

*(i) $\to$ je **noetherovská**, neexistuje-li nekonečná posloupnost $t_1 \to t_2 \to \dots,\ t_1, t_2 \in T$;*

*(ii) $\to$ je **lokálně konfluentní**, jestliže kdykoliv $t \to u,\ t \to v$ tak i $u \to u_1 \to \dots \to u_k,\ v \to v_1 \to \dots \to v_l,\ u_k = v_l\ (k, l \geq 0)$;*

*(iii) $\to$ je **konfluentní**, jestliže kdykoliv $t \to t_1 \to \dots \to t_p = u,\ t \to t'_1 \to \dots \to t'_q = v\ (p, q \geq 0)$ tak i $u \to u_1 \to \dots \to u_k,\ v \to v_1 \to \dots \to v_l,\ u_k = v_l\ (k, l \geq 0)$.*

**Věta 9.1** *Libovolná noetherovská lokálně konfluentní relace je i konfluentní.*

*Důkaz.* . .

Nechť $\sim$ je relace ekvivalence na množině $T$ generovaná relací $\to$. Zřejmě platí

**Lemma 9.1** *Nechť relace $\to \subseteq T \times T$ je noetherovská a konfluentní. Pak*

*(i) pro každé $t \in T$ existuje právě jedno $u \in T$ takové, že ( $t \to \dots \to u$ a neexistuje $v \in T,\ u \to v$ ). Píšeme $\overrightarrow{t} = u$.*

*(ii) pro $t, u \in T$ máme $t \sim u$ právě když $\overrightarrow{t} = \overrightarrow{u}$.*

**Příklad 9.1** *Relace $\to = \{\ (tssu, tsu) \mid t, u \in X^*,\ s \in X^+\ \}$ na množině $X^+$ není konfluentní, neboť např.*

$$xyxyzyxyz \to x \cdot yxyz \to xy \cdot z,\ \ xyxyzyxyz \to xy \cdot zyxyz\ .$$

Nechť pro $u \in X^+$ symbol $\mathsf{c}(u)$ značí množinu všech prvků z $X$, které se ve slově $u$ vyskytují a pro $u$ s $n = |\mathsf{c}(u)| \geq 2$ je $0(u)$ resp. $1(u)$ nejdelší prefix resp. sufix slova $u$ v $n-1$ proměnných. Platí

**Věta 9.2**

*1. Relace $\{\ (tsu, tu) \mid t, u \in X^*,\ s \in X^+,\ \mathsf{c}(s) \subseteq \mathsf{c}(t) = \mathsf{c}(u)\ \}$ je noetherovská a lokálně konfluentní.*

*2. Pro $u, v \in X^+$ s $\mathsf{c}(u) = \{x\}$ máme $u \sim v$ právě když $\mathsf{c}(v) = \{x\}$ a pro $|\mathsf{c}(u)| \geq 2$ je*

$$u \sim v \ \Leftrightarrow\ \mathsf{c}(u) = \mathsf{c}(v),\ 0(u) \sim 0(v),\ 1(u) \sim 1(v)\ .$$

Každá z obou částí věty dává řešení problému identit pro idempotentní pologrupy. V prvním případě jsme "zúplnili" relaci $\to$ na noetherovský konfluentní přepisovací systém; ve druhém případě řešíme problém pomocí "invariantů".

Na relaci (= přepisovací systém) $\to \subseteq T \times T$ se můžeme dívat jako na ***program***, na samotné přepisování jako na ***výpočet***. ***Vstupy*** i ***výstupy*** jsou prvky z $T$.

**Významný příklad.**
Definujme nulární termy dvou typů : $N$ (numbers) a $L$ (lists).



(i) $0 \in N,\ \mathsf{nil} \in L$,
(ii) pro $m, n \in N,\ l \in L$ je též $\mathsf{s}\,(m),\ \mathsf{max}\,(m, n),\ \mathsf{min}\,(m, n) \in N$, $\mathsf{sort}\,(l),\ \mathsf{cons}\,(m, l),\ \mathsf{insert}\,(m, l) \in L$,
(iii) do množin $N, L$ patří jen to, co vzniklo v konečném počtu kroků (i) a (ii).
Místo $\mathsf{s}\,(m)$ píšeme často $m'$.

Uvažujeme následující přepisovací systém

$$\mathsf{max}\,(0, m) \to m,\ \mathsf{max}\,(m, 0) \to m,\ \mathsf{max}\,(m', n') \to (\mathsf{max}\,(m, n))'\ ,$$

$$\mathsf{min}\,(0, m) \to 0,\ \mathsf{min}\,(m, 0) \to 0,\ \mathsf{min}\,(m', n') \to (\mathsf{min}\,(m, n))'\ ,$$

$$\mathsf{sort}\,(\mathsf{nil}\,) \to \mathsf{nil}\,,\ \mathsf{sort}\,(\mathsf{cons}\,(m, l)) \to \mathsf{insert}\,(m, \mathsf{sort}\,(l))\ ,$$

$$\mathsf{insert}\,(m, \mathsf{nil}\,) \to \mathsf{cons}\,(m, \mathsf{nil}\,),\ \mathsf{insert}\,(m, \mathsf{cons}\,(n, l)) \to \mathsf{cons}\,(\mathsf{max}\,(m, n), \mathsf{insert}\,(\mathsf{min}\,(m, n), l))\ .$$

**Věta 9.3** *Libovolný term z $L$ v operačních symbolech $0, \mathsf{s}\,, \mathsf{nil}\,, \mathsf{cons}\,, \mathsf{sort}$ má jedinou kánonickou formu. Ta neobsahuje operační symboly $\mathsf{sort}\,, \mathsf{insert}\,, \mathsf{max}\,, \mathsf{min}$ a její položky jsou uspořádány nerostoucím způsobem.*

Příklad. Pohrejte si s

$$\mathsf{sort}\,(\mathsf{cons}\,(0, \mathsf{cons}\,(0', \mathsf{cons}\,(0'', \mathsf{nil}\,)))) \to \dots \to \mathsf{cons}\,(0'', \mathsf{cons}\,(0', \mathsf{cons}\,(0, \mathsf{nil}\,)))\ .$$

# 10 Regulární jazyky

Je vhodné si připomenout sekci Syntaktický monoid z textu Algebra I – poznámky.

Nechť $A = \{a_1, \dots, a_n\}\ (n \geq 1)$ je konečná abeceda. Nulární termy jazyka nulárních operačních symbolů $0, a_1, \dots, a_n$, binárních operačních symbolů $\cdot, +$ a unárního operačního symbolu $^*$ nazýváme ***regulární výrazy*** nad abecedou $A$. Realizace těchto termů v algebře

$$\mathcal{L} = (2^{A^*}, \emptyset, \{a_1\}, \dots, \{a_n\}, \cdot, \cup, ^*)$$

všech podmnožin množiny $A^*$ všech slov nad $A$ jsou ***regulární jazyky*** nad $A$. Přitom $K \cdot L = \{uv \mid u \in K,\ v \in L\},\ K^* = \{u_1 \dots u_m \mid m \geq 0,\ u_1, \dots, u_m \in K\}$.

# 11 Kódy

Nechť $A$ je neprázdná konečná abeceda. Množinu $C \subseteq A^*$ nazýváme ***kódem***, je-li podmonoid $\langle C \rangle$ monoidu $(A^*, \cdot)$ generovaný množinou $C$ volný nad $C$. Ekvivalentní formulace je
( $\forall\ m, n \in \mathbb{N},\ c_1, \dots, c_m,\ d_1, \dots, d_n \in C$ )
( $c_1 \dots c_m = d_1 \dots d_n\ \Rightarrow\ m = n,\ c_1 = d_1, \dots, c_m = d_m$ ).

**Příklad 11.1** *1. Pro $A = \{a, b\}$ je $C_1 = \{aa, baa, ba\}$ kód – proč ?*
*2. $C_2 = \{a, ab, ba\}$ není kód, neboť $a \cdot ba = ab \cdot a$.*

Nechť $C \subseteq A^*$ je takové, že

$$( \forall \; c, d \in C, \; p \in A \; ) \; ( \; cp = d \; \Rightarrow \; p = \lambda \; ) \; .$$

Pak hovoříme o ***prefixovém kódu.***

**Příklad 11.2** *1. $C_1$ definované výše není prefixový kód, neboť $ba \cdot a = baa$.*
*2. $C_3 = \{b^k a^l ab \mid k, l \geq 0\}$ je prefixový kód – proč ?*

K dalšímu studiu : .....

# 12 Unifikace

Příklad syntaktické unifikace :
Máme jazyk binárních operačních symbolů $F, H$ a unárního operačního symbolu $G$. Máme “unifikovat”

$$F(G(x), H(x,u)) = F(z, H(F(y,y), z)) \; .$$

Klademe $z \to G(x)$ a řešíme $H(x,u) = H(F(y,y), G(x))$. Proto $x \to F(y,y)$ a $u \to G(F(y,y))$.

Zajímavější bývá tzv. ekvacionální unifikace. Např. : ve volné pologrupě nad $\{a, b\}$ řešte $xauzau = yzbxaaby$. Řešením je např. $x \to abb, \; y \to ab, \; z \to ba, \; u \to ....$

Nebo : v komutativních grupách řešte $x^5 y^7 = c^8 d^2 e^3$. Lze ukázat, že $x \to c^{-4} d^{-1} e^{-5} z^{-7}, \; y \to c^4 d e^4 z^5$ je “nejobecnější” řešení.

# 13 Primální algebry

Na množině $\{0, 1\}$ pravdivostních hodnot je 16 binárních operací (logických spojek). Libovolnou z nich lze “vygenerovat” pomocí unární negace a binární konjunkce. Dokonce binární spojka “ani … ani …” na to stačí sama.

Zobecníme tyto poznatky na libovolnou konečnou množinu.

***Algebra*** je uspořádaná dvojice $\mathcal{A} = (A, F)$, kde $A$ je množina a $F$ je množina operací na $A$.

Nechť $m, n \in \mathbb{N}, \; f : A^n \to A, \; \tau : \{1, ..., n\} \to \{1, ..., m\}$. Klademe

$$f_\tau(a_1, \ldots, a_m) = f(a_{\tau(1)}, ..., a_{\tau(n)}), \; a_1, \ldots, a_m \in A.$$

Pak $f_\tau : A^m \to A$ a pravíme, že $f_\tau$ vznikla z $f$ ***transformací argumentů***.

Nechť $f : A^n \to A, \; g : A^m \to A, \; m, n \in \mathbb{N}$. Klademe

$$(f(g))(a_1, \ldots, a_{m+n-1}) = f(g(a_1, \ldots, a_m), a_{m+1}, \ldots, a_{m+n-1}), \; a_1, \ldots, a_{m+n-1} \in A.$$

Pak $f(g) : A^{m+n-1} \to A$ a pravíme, že $f(g)$ vznikla ***kompozicí*** $f$ a $g$.

Nechť $\mathcal{A} = (A, F)$ je algebra. Množina všech jejích ***algebraických operací*** $T(\mathcal{A})$ je nejmenší množina splňující:



(i) $F \subseteq T(\mathcal{A})$,
(ii) identické zobrazení množiny $A$ na sebe patří do $T(\mathcal{A})$,
(iii) $T(\mathcal{A})$ je uzavřená na transformace argumentů,
(iv) $T(\mathcal{A})$ je uzavřená na kompozice.

Algebra $\mathcal{A}$ je ***primální***, je-li libovolná operace na množině $A$ nenulové arity algebraickou operací algebry $\mathcal{A}$.

Následující tvrzení jsou pozoruhodná:

**Věta 13.1 (Sierpiński)** *Libovolná operace nenulové arity vznikne z binárních operací transformacemi argumentů a kompozicemi.*

**Věta 13.2 (Post)** *Algebra $\mathcal{A} = (\{0, 1, ..., n-1\}, \; \wedge, \; g)$, kde $i \wedge j = min\{i, j\}, \; g(i) = i + 1$ pro $i = 0, ..., n-2, \; g(n-1) = 0$, je primální.*

Nejprve dokážeme:

**Lemma 13.1 (Post)** *Nechť $A$ je alespoň dvouprvková konečná množina, nechť $0, 1 \in A$, nechť $\wedge, \vee$ jsou binární operace na $A$ splňující*

$$( \; \forall \; a \in A) \; (a \wedge 0 = 0, \; a \wedge 1 = a, \; a \vee 0 = a = 0 \vee a).$$

*Nechť $c_a$ je unární konstanta na prvek $a, \; a \in A$,*
*nechť $\chi_a(b) = 0$ pro $a \neq b, \; \chi_a(a) = 1$ pro $a, b \in A$ je rovněž unární.*
*Pak je algebra $\mathcal{A} = (A, 0, 1, \wedge, \vee, \; (c_a)_{a \in A}, \; (\chi_a)_{a \in A})$ primální.*

*Důkaz lemmatu.*
Nechť $f$ je $n$-ární operace na množině $A$.
Položme

$$\chi_{(a_1, \ldots, a_n)}(b_1, \ldots, b_n) = (...(\chi_{a_1}(b_1) \wedge \chi_{a_2}(b_2)) \wedge ...) \wedge \chi_{a_n}(b_n) \; .$$

Pak $\chi_{(a_1, \ldots, a_n)}(b_1, \ldots, b_n) = 0$ pro $(a_1, \ldots, a_n) \neq (b_1, \ldots, b_n), \; \chi_{(a_1, \ldots, a_n)}(a_1, \ldots, a_n) = 1.$

Položme

$$f_{(a_1, \ldots, a_n)}(b_1, \ldots, b_n) = c_{f(a_1, \ldots, a_n)}(b_1) \wedge \chi_{(a_1, \ldots, a_n)}(b_1, \ldots, b_n) \; .$$

Pak $f_{(a_1, \ldots, a_n)}(b_1, \ldots, b_n) = 0$ pro $(a_1, \ldots, a_n) \neq (b_1, \ldots, b_n)$,
$f_{(a_1, \ldots, a_n)}(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$.

Nechť $A^n = \{(a_{11}, ..., a_{1n}), ..., (a_{s1}, ..., a_{sn})\}, \; s = |A|^n$. Máme

$$f(b_1, \ldots, b_n) = (...(f_{(a_{11}, \ldots, a_{1n})}(b_1, \ldots, b_n) \vee f_{(a_{21}, \ldots, a_{2n})}(b_1, \ldots, b_n)) \vee ...) \vee f_{(a_{11}, \ldots, a_{sn})}(b_1, \ldots, b_n) \; .$$

*Důkaz Postovy věty.*
Prvky $0, 1$ z lemmatu značme $\underline{0}, \underline{1}$. Položme

$$\underline{0} = 0, \; \underline{1} = n-1, \; c_0(a) = a \wedge g(a) \wedge ... \wedge g^{n-1}(a), \; c_i(a) = g^i(c_0(a)) \text{ pro } i \geq 1 \; ,$$

$$\chi_i(a) = g^{n-1}(1 \wedge g^{n-i}(a)),\ a \vee b = g(g^{n-1}(a) \wedge g^{n-1}(b))\ .$$

*Důkaz Sierpińského věty.*
Pro konečnou množinu $A$ to plyne z Postovy věty, pro nekonečnou množinu to zatím dokazovat nebudeme.

**Věta 13.3 (Webb)** *Algebra* $(\{0, 1, ..., n-1\}, |)$, *kde* $i \mid j = ...$ *je primální.*

*Důkaz.* Položme $i \wedge j = ...,\ g(i) = ....$

To byla ukázka, jak dokazovat primalitu. Dokázat, že daná algebra není primální vyžaduje nové metody. Snad později.

---

verze 2.6.2003