Kybernetika

Jan Mareš

Dvě vlastnosti výrazů v jisté volné univerzální algebře

Kybernetika, Vol. 5 (1969), No. 3, (190)--200

Persistent URL: http://dml.cz/dmlcz/125844

KYBERNETIKA ČÍSLO 3, ROČNÍK 5/1969

Dvě vlastnosti výrazů v jisté volné univerzální algebře

JAN MAREŠ

Článek se zabývá dvěma vlastnostmi výrazů v jisté volné univerzální algebře a to roznásobitelností výrazů zleva a zprava a existencí jediného úplného pravého vytknutí daného výrazu.

ÚVOD

Při abstraktní syntéze automatů pomocí regulárních výrazů, tak jak je popsána v [1], hraje jistou roli tvar (s ohledem na užití distributivních zákonů) regulárního výrazu, od kterého vycházíme. Pokus o nalezení jakéhosi v určitém smyslu „minimálního tvaru" daného konečného regulárního výrazu byl učiněn v [2]. Přitom se podstatně využívaly dvě vlastnosti konečných regulárních výrazů, a to:

1. Máme-li libovolný konečný regulární výraz, lze jej úplně roznásobit tím způsobem, že nejprve užíváme pouze levého distributivního zákona a potom pouze pravého distributivního zákona.
2. Máme-li „úplně roznásobený" konečný regulární výraz, můžeme v něm provádět vytýkání zprava tak dlouho, pokud to jde. Tak dostáváme pojem úplného pravého vytknutí daného výrazu. Toto úplné pravé vytknutí pak nezávisí podstatně (vzhledem k danému algoritmu syntézy) na způsobu, jakým vytýkáme.

V tomto článku jsou tyto vlastnosti dokázány obecněji jako vlastnosti „dobře utvořených" výrazů ve volné univerzální algebře s vlastnostmi odpovídajícími v podstatě vlastnostem algebry regulárních výrazů.

Volba roznásobitelnosti nejprve *zleva* a pak *zprava* a úplného *pravého* vytknutí je dána pouze motivací ve zmíněné syntéze automatů, kde hraje podstatnou úlohu. Analogicky by se zřejmě daly dokázat symetrické výsledky v případě, kdy by všude byla zaměněna slova „pravý" a „levý".

I. ROZNÁSOBITELNOST ZLEVA A ZPRAVA

Buď $\Sigma = \{x_1, \ldots, x_n\}$ abeceda, tj. konečná neprázdná množina libovolných symbolů. Uvažujme volnou univerzální algebru G s množinou volných prvků Σ a dvěma binárními operacemi $+a.$, ve které jsou splněny následující identity.

(Znak operace . ovšem vynecháváme, jak je to obvyklé.)

(1) $$(x + y) + z = x + (y + z),$$

(2) $$x + y = y + x,$$

(3) $$(xy)\,z = x(yz),$$

(4) $$(x + y)\,z = xz + yz,$$

(5) $$z(x + y) = zx + zy.$$

Tedy $G = (\Omega, I, \Sigma)$, kde $\Omega = \{+, .\}$ je množina operací a I je množina identit (1) až (5).

Definujme, co budeme rozumět *výrazy v algebře G.*

Definice 1. 1. x_i je výraz v G $(i = 1, \ldots, n)$; 2. jsou-li R_1 a R_2 výrazy v G, jsou také $R_1 + R_2$ a $(R_1)\,(R_2)$ výrazy v G, přičemž závorky napíšeme právě tehdy, je-li to nutné pro správnou interpretaci výrazu.

Jsou-li $R_1, \ldots, R_m$ výrazy v G, $m \geqq 2$, jsou zřejmě také $R_1 + \ldots + R_m$ a $R_1, \ldots, R_m$ (s nějakým uzávorkováním) výrazy v G; nazveme je po řadě *součet* a *součin* (výrazů $R_1, \ldots, R_m$); výraz $x_{i_1}, \ldots, x_{i_p}$, kde $x_{i_j} \in \Sigma$ pro $1 \leqq j \leqq p$, nazveme *elementárním součinem.* V dalším zahrneme elementární součin mezi součiny, takže za součin budeme považovat i jediný volný prvek.

Od tohoto okamžiku rovnost $R = S$ bude znamenat, že R a S jsou si rovny jako posloupnosti prvků „rozšířené abecedy"

$$\Sigma_1 = \Sigma \cup \{+, (,)\}.$$

Je-li R součet, rozumějme *uzávorkovaným součtem* (R). Je-li naopak S uzávorkovaný součet, $S = (R)$, definujme Int $S = R$.

Buď $R = y_1, \ldots, y_m$ výraz. (Symboly $y_1, \ldots, y_m$ jsou zde ovšem prvky abecedy Σ_1.) Každý výraz $y_k y_{k+1}, \ldots, y_t$ $(1 \leqq k \leqq t \leqq m)$, kde $y_{k-1} \notin \Sigma$ nebo $y_k \notin \Sigma$ a současně $y_t \notin \Sigma$ nebo $y_{t+1} \notin \Sigma$ nazveme *podvýrazem* výrazu R.

Uvažujme nyní množinu přepisovacích pravidel:

(A) $$x + y := y + x,$$

(B) $$xz + yz := (x + y)\,z,$$

(C) $$(x + y)\,z := xz + yz,$$

(D) $$z(x + y) := zx + zy.$$

Tato přepisovací pravidla se aplikují tak, jak je to obvyklé např. u gramatik, tj.:

„Dosadíme-li" za symboly x, y, z do levé strany některého pravidla (X) vhodné výrazy tak, že dostaneme nějaký podvýraz daného výrazu R, nahradíme tento

podvýraz v R výrazem vzniklým odpovídajícím dosazením do pravé strany pravidla (X) (X = A, ..., D). Přitom v pravidlech (B) a (C) budeme za symbol z dosazovat ne libovolný výraz, ale pouze elementární součin.

Je-li dán výraz R, označme $R^{(X)}$ výraz, který vznikne z R k-násobnou ($k = 0, 1$) aplikací pravidla (A) pro X = B (pro X = C, D nebudeme pravidlo (A) vůbec aplikovat), dále aplikací pravidla (X) a konečně odstraněním z takto vzniklé posloupnosti symbolů všech „zbytečných" závorek, tj. takových závorek, které nejsou nutné pro správnou interpretaci výrazu. Jestliže při žádné volbě aplikace pravidla (A) nelze aplikovat pravidlo (X), položme $R^{(X)} = R$ (X = B, ..., D). (Že $R^{(X)}$ je skutečně výraz plyne ihned z toho, že přepisovací pravidla (A) až (D) nejsou vlastně nic jiného než identity (2), (4) a (5). Jde samozřejmě o běžné užívání levého nebo pravého distributivního zákona jedním či druhým směrem.)

Výrazy $R^{(B)}$, $R^{(C)}$ a $R^{(D)}$ budeme v dalším označovat po řadě R', R^{P} a R^{L} a nazveme je po řadě *pravým elementárním vytknutím*, *pravým elementárním roznásobením* a *levým roznásobením výrazu* R.

Zaveďme ještě pojem kanonického způsobu vytýkání.

Při *kanonickém způsobu vytýkání* aplikujeme při přechodu od R k R' pravidlo (A) jen tehdy, umožní-li se tím aplikace pravidla (B) na součiny, na které jinak (B) aplikovat nelze, a pak aplikujeme (B) právě na tyto dva součiny a dále vytknutí provedeme tak, aby součin dosazovaný v (B) za xz „zůstal na místě", tj. aplikujeme případně pravidlo (A) vpravo od tohoto součinu (a ne vlevo). Navíc, při zvoleném součinu dosazeném za xz v (B), aplikujeme (je-li to vůbec třeba) pravidlo (A) na „nejlevější" podvýraz výrazu R, který lze dostat odpovídajícím dosazením za yz v (B).

Každý výraz $\alpha_1 + \ldots + \alpha_n$, kde je $n \geqq 1$, α_i elementární součin ($i = 1, \ldots, n$), nazveme *polynomem*.

Definice 2. Buď R výraz a nechť existuje posloupnost výrazů $P_1, \ldots, P_m, S_1, \ldots, S_n$ tak, že

$$P_1 = R\,, \quad P_{i+1} = P_i^{L} \quad (i = 1, \ldots, m-1)\,,$$

$$S_1 = P_m\,, \quad S_{j+1} = S_j^{P} \quad (j = 1, \ldots, n-1)\,.$$

1. Je-li S_n polynom, řekneme, že R je *roznásobitelný zleva a zprava*. Je-li navíc $m = 1$, řekneme, že R je *roznásobitelný zprava* (na výraz S_n).

2. Je-li $n = 1$, řekneme, že R je *roznásobitelný zleva na výraz* S_1.

Naším cílem je dokázat toto tvrzení:

Věta 1. *Každý výraz je roznásobitelný zleva a zprava.*

Dříve, než přikročíme k vlastnímu důkazu této věty, zavedeme některé pojmy a dokážeme několik pomocných tvrzení.

Nechť $R = y_1, \ldots, y_t$ je výraz, $1 \leqq k \leqq t$. Nechť m resp. n je počet výskytů symbolu levá závorka resp. symbolu pravá závorka *před* y_k (tj. v „podřetězu" $y_1, \ldots, y_{k-1}$).

Označme $h(y_k) = m - n$ $(h(y_k) \geqq 0)$. *Hloubkou* výrazu R rozumíme číslo $h = \operatorname{Max}_{1 \leqq k \leqq t} h(y_k)$.

Definujme nyní pojem, který se ukáže být ekvivalentní pojmu roznásobitelnosti zprava. Tak dostaneme jakousi „popisnou" charakteristiku výrazů roznásobitelných zprava, kterou je výhodné použít v důkaze věty 1.

Je-li $R = R_1\alpha$, kde R_1 je uzávorkovaný součet a α je elementární součin, označme $\bar{R} = R_1$.

Buďte R a S výrazy. Řekneme, že R *má tvar* F, jestliže $R = R_1 + \ldots + R_m$, kde je $m \geqq 1$ a R_i je buď elementární součin nebo je $R_i = S_i\alpha_i$, kde S_i je uzávorkovaný součet a α_i je elementární součin $(i = 1, \ldots, m)$. Řekneme, že S *má tvar* Tot F, jestliže má tvar F a jestliže pro každý podvýraz P výrazu S, který má tvar F, $P = P_1 + \ldots + P_n$, $n \geqq 1$, má Int $\bar{P}_i$, pokud existuje, tvar F $(i = 1, \ldots, n)$.

Uveďme lemma, které využijeme v důkaze tvrzení 1:

Lemma 1. *Buď R výraz roznásobitelný zprava a nechť existuje $\bar{R}$. Pak také* Int $\bar{R}$ *je roznásobitelný zprava.*

Důkaz se provede indukcí dle počtu „činitelů" v součinu α a dle hloubky výrazu Int $\bar{R}$.

Tvrzení 1. *Výraz R je roznásobitelný zprava právě tehdy, když má tvar* Tot F.

Dokažme nejdříve

pomocné tvrzení 1. *Nechť R je výraz, který nemá tvar* F. *Pak R není roznásobitelný zprava.*

Důkaz. Je $R = R_1 + \ldots + R_m$, $m \geqq 1$, R_i jsou součiny a existuje k, $1 \leqq k \leqq m$ tak, že R_k nemá tvar daných vlastností. Zřejmě nyní stačí dokázat, že R_k není roznásobitelný zprava.

Řekneme, že výraz V má vlastnost v, lze-li psát

$$V = Y_1Y_2Y_3 \quad \text{nebo} \quad V = Y_1Y_2\,,$$

kde Y_2 je uzávorkovaný součet.

Dá se dokázat toto: Má-li výraz V vlastnost v a je-li $V_1, \ldots, V_t$ *libovolná* posloupnost výrazů taková, že

$$V_1 = V, \quad V_{i+1} = V_i^{\mathrm{P}} \quad (i = 1, \ldots, t-1)\,,$$

má výraz V_i vlastnost v $(i = 1, \ldots, t)$. (Speciálně tedy výraz s vlastností v není roznásobitelný zprava.)

Stačí tedy ukázat, že R_k má vlastnost v. Buď $R_k = XY$. Je-li Y elementární součin, nemůže být X elementární součin ani uzávorkovaný součet a lze tedy psát

$$X = Y_1Y_2\bar{Y}_3 \quad \text{resp.} \quad X = Y_1Y_2\,,$$

kde Y_2 je uzávorkovaný součet, $\tilde{Y}_3$ je elementární součin; stačí tedy položit

$$Y_3 = \tilde{Y}_3 Y \quad \text{resp.} \quad Y_3 = Y.$$

Nechť Y není elementární součin. Potom je Y buď uzávorkovaný součet nebo lze psát

$$Y = \tilde{Y}_1 Y_2 Y_3 \quad \text{resp.} \quad Y = \tilde{Y}_1 Y_2 \quad \text{resp.} \quad Y = Y_2 Y_3$$

a Y_2 je uzávorkovaný součet. V prvním případě stačí položit

$$Y_1 = X\,, \quad Y_2 = Y,$$

ve druhém

$$Y_1 = X\tilde{Y}_1 \quad \text{resp.} \quad Y_1 = X\bar{Y}_1 \quad \text{resp.} \quad Y_1 = X\,.$$

Důkaz tvrzení 1. 1. Nechť R *má* tvar Tot F. Indukcí dle hloubky R. Má-li R hloubku 0, implikace zřejmě platí. (R je totiž v tomto případě polynom.)

Nechť dokazovaná implikace platí pro výrazy hloubky nejvýše n, $n \geqq 0$ a nechť R má hloubku $n + 1$. Je

$$R = R_1 + \ldots + R_m\,, \quad m \geqq 1\,.$$

Zřejmě stačí ukázat, že R_i je roznásobitelný zprava pro všechna i. Zvolme tedy k, $1 \leqq k \leqq m$. Je-li R_k elementární součin, jsme hotovi. Jinak má však Int $\bar{R}_k$ hloubku nejvýše n a je tedy dle indukčního předpokladu roznásobitelný zprava. Dále je to zřejmé.

2. Nechť R *nemá* tvar Tot F. Indukcí dle hloubky R: R samozřejmě nemůže mít hloubku 0. Nechť tedy hloubka R je 1. Pak však R nemá tvar Tot F právě tehdy, když nemá tvar F, takže dle pomocného tvrzení 1 není R roznásobitelný zprava.

Nechť dokazovaná implikace platí pro výrazy hloubky nejvýše n, $n \geqq 1$ a nechť R má hloubku $n + 1$,

$$R = R_1 + \ldots + R_m\,, \quad m \geqq 1\,.$$

Rozlišujme tyto případy:

A. R nemá tvar F. Pak není R roznásobitelný zprava dle pomocného tvrzení 1.

B. R má tvar F. Stačí dokázat, že aspoň jeden R_k, $1 \leqq k \leqq m$, není roznásobitelný zprava.

Existuje podvýraz S výrazu R tak, že S má tvar F, $S = S_1 + \ldots + S_t$ a aspoň jeden Int $\bar{S}_k$, $1 \leqq k \leqq t$, nemá tvar F.

a) $S = R$. Tedy $t = m$, $S_i = R_i$ $(i = 1, \ldots, m)$ a aspoň jeden Int $\bar{R}_k$ nemá tvar F. Int $\bar{R}_k$ není tedy roznásobitelný zprava a dle lemmatu 1 není ani R_k roznásobitelný zprava.

b) $S \neq R$. S je podvýrazem některého R_k. Nemá-li R_k tvar F, jsme hotovi. Jinak Int $\bar{R}_k$ nemá tvar Tot F a má hloubku nejvýše n; tedy dle indukčního předpokladu

není Int $\bar{R}_k$ roznásobitelný zprava. Dle lemmatu 1 není ani R_k roznásobitelný zprava.

Dokažme nyní konečně větu 1. Položme

$$\langle P\rangle = \begin{cases} (P), & \text{je-li } P \text{ součet}, \\ P, & \text{je-li } P \text{ součin}. \end{cases}$$

Zřejmě stačí dokázat tvrzení (T):

(T) *Každý výraz je roznásobitelný zleva na výraz, který je roznásobitelný zprava.*

Buď R libovolný výraz. Indukcí dle hloubky výrazu R:

Má-li R hloubku 0, je to polynom a jsme hotovi.

Nechť tvrzení (T) platí pro všechny výrazy mající hloubku nejvýše s, $s \geqq 0$ a nechť R má hloubku $s+1$, $R = R_1 + \ldots + R_n$, $n \geqq 1$, $R_1, \ldots, R_n$ jsou součiny. Buď k libovolné, $1 \leqq k \leqq n$. Zřejmě stačí dokázat, že (T) platí pro součin R_k.

Položme $S = R_k$; je-li S elementární součin, je to zřejmé; jinak pišme $S = \langle S_1\rangle \ldots \langle S_m\rangle$, $m \geqq 2$, kde S_i je buď elementární součin nebo součet $(i = 1, \ldots, m)$ a S_j, S_{j+1} nejsou současně elementární součiny $(j = 1, \ldots, m-1)$.

S_i má hloubku nejvýše s a tedy dle indukčního předpokladu je roznásobitelný zleva na výraz P_i, který je roznásobitelný zprava; čili P_i má tvar Tot F $(i = 1, \ldots, m)$.

Stačí nyní dokázat toto:

Je-li $T = \langle T_1\rangle \langle T_2\rangle$, kde T_1 a T_2 mají tvar Tot F, je T roznásobitelný zleva na výraz, který má tvar Tot F (a je tedy roznásobitelný zprava).

Indukcí dle hloubky $\langle T_2\rangle$: (Hloubkou uzávorkovaného součtu U rozumíme ovšem hloubku Int U zvětšenou o jedničku.)

Má-li $\langle T_2\rangle$ hloubku 0, je T_2 elementární součin, čili $\langle T_1\rangle T_2$ má tvar Tot F. Nechť tvrzení platí již pro $\langle T_2\rangle$ mající hloubku nejvýše r a nechť nyní $\langle T_2\rangle$ má hloubku $r+1$. Je buď $T_2 = D_1 + \ldots + D_t$ nebo $T_2 = (D_1 + \ldots + D_t)\,\delta$, kde $t \geqq 2$, δ je elementární součin a D_i je součin $(i = 1, \ldots, t)$. Označme $D = (D_1 + \ldots + D_t)$. Pak $\langle T_1\rangle D$ je jistě roznásobitelný zleva na $\langle T_1\rangle D_1 + \ldots + \langle T_1\rangle D_t$ a D_i má tvar Tot F a hloubku nejvýše r. Dle indukčního předpokladu je tedy $\langle T_1\rangle D_i$ roznásobitelný zleva na výraz, který má tvar Tot F $(i = 1, \ldots, t)$. Celkem je tedy $\langle T_1\rangle \langle T_2\rangle$ roznásobitelný zleva na výraz, který má tvar Tot F.

Tím je věta 1 dokázána.

II. ÚPLNÉ PRAVÉ VYTKNUTÍ

V tomto paragrafu bude výhodné uvažovat algebru $G = (\Omega, I, \Sigma)$ s jednotkovým prvkem I, tj. $\Omega = \{+, ., I\}$, kde I je nulární operace „vzetí jednotkového prvku". Tuto jednotku budeme považovat za prázdný elementární součin, tj. součin neobsahující žádné „činitele". Je nutné dodat, že v přepisovacích pravidlech (B) až (D) není dovoleno „dosazovat" za z jednotku.

Každý výraz $R = \alpha_1 + \ldots + \alpha_n$, kde je $n \geqq 1$, α_i elementární součin, $\alpha_i \neq \alpha_j$ pro $i \neq j$ $(i, j = 1, \ldots, n)$ nazveme *prostým polynomem*. V dalším budeme slovo „prostý" vynechávat, neboť k omylu nemůže dojít. Označme ještě $r(R) = \{\alpha_1, \ldots, \alpha_n\}$.

Definice 3. Buď R polynom a nechť $R_1, \ldots, R_m$ je posloupnost výrazů taková, že

$$R_1 = R\,, \quad R_{i+1} = R_i' \quad (i = 1, \ldots, m-1) \quad \text{a} \quad R_m' = R_m\,.$$

Pak výraz R_m označíme R^T a nazveme jej *úplným* (pravým) *vytknutím* výrazu R. (Slovo „pravé" budeme vynechávat.)

Je vidět, že každý polynom má aspoň jedno úplné vytknutí. Cílem tohoto paragrafu je ukázat, že toto úplné vytknutí je *právě jedno až na užití komutativního zákona.*

Dále se budou vyskytovat pouze takové výrazy, které mají tvar Tot F. (To plyne z toho, že má-li S tvar Tot F, má zřejmě i S' tvar Tot F.)

Buď R výraz, který má tvar Tot F a nechť $R_1, \ldots, R_m$ je posloupnost výrazů taková, že

$$R_1 = R\,, \quad R_{i+1} = R_i^{\mathrm{p}} \quad (i = 1, \ldots, m-1) \quad \text{a} \quad R_m^{\mathrm{p}} = R_m\,.$$

Pak výraz R_m označíme R_T a nazveme jej *úplným roznásobením* výrazu R. (R_T je ovšem polynom.)

Je-li $\alpha = x_1, \ldots, x_n$ elementární součin, rozumějme minus k-tým prvkem součinu α prvek x_{n-k+1} $(k = 1, \ldots, n)$.

Buď R polynom s následujícími vlastnostmi:

1. $R = R^1 + \ldots + R^m$, kde $m \geqq 1$ a R^j $(j = 1, \ldots, m)$ je součet právě těch elementárních součinů z množiny $r(R)$, které mají stejný minus první prvek (R^j se ovšem může redukovat na jediný elementární součin).

2. Nechť $d + 1$ je maximum z počtu „činitelů" elementárních součinů patřících do $r(R)$ a nechť R_k je libovolný podvýraz výrazu R, který je součtem právě těch elementárních součinů z množiny $r(R)$, které mají na minus i-tém místě $(i = 1, \ldots, k)$ stejný prvek $(k = 1, \ldots, d)$. Pak je $R_k = R_k^1 + \ldots + R_k^{t_k}$, kde $t_k \geqq 1$ a R_k^j $(j = 1, \ldots, t_k)$ je součet právě těch elementárních součinů z množiny $r(R_k)$, které mají stejný minus $k + 1$-ní prvek. (Přitom minus $k + 1$-ním prvkem elementárního součinu o k „činitelích" rozumějme symbol $\lambda \notin \Sigma$.)

Potom výraz R nazveme *normálním* polynomem.

Charakterizujme nyní jisté výrazy pomocí vektorů. Nechť $R = R_1 + \ldots + R_m$, $m \geqq 1$ je výraz, který má tvar Tot F. Nechť $f(i)$ označuje minus první prvek elementárního součinu α_i (kde $R_i = \bar{R}_i \alpha_i$ resp. $R_i = \alpha_i$) $(i = 1, \ldots, m)$. Je-li $R_j = 1$, položme $f(j) = \lambda$.

Výrazu R přiřadíme vektor $V(R) = [y_1, \ldots, y_n]$, $n \leqq m$, následujícím způsobem: buď n počet všech vesměs různých $f(i)$ $(i = 1, \ldots, m)$; položme

$$y_1 = f(1)\,;$$

je-li

$$y_k = f(t) \quad (1 \leqq k \leqq t)\,,$$

položme

$$y_{k+1} = f(t + p)\,,$$

kde $p \geqq 1$ je nejmenší číslo takové, že $f(t + p) \neq y_1, \ldots, y_k$. Počet složek vektoru $V(R)$ označme $v(R)$ (tj. $v(R) = n$).

Konečně označme $T(R) = [f(1), \ldots, f(m)]$; $T(R)$ nazveme koncovou posloupností výrazu R.

Snadno lze dokázat

Lemma 2. *Buď M množina normálních polynomů taková, že*

1. $r(R_1) = r(R_2)$ *pro* $R_1, R_2 \in M$;
2. *je-li N libovolná množina elementárních součinů patřících do $r(R)$ pro $R \in M$ a majících stejný minus první prvek, je pořadí součinů množiny N stejné ve všech polynomech množiny M.*

Pak zobrazení V je prosté na M.

Tvrzení 2. *Při kanonickém způsobu vytýkání existuje k danému normálnímu polynomu nejvýše jedno jeho úplné vytknutí.*

Předpokládejme nyní, že tvrzení 2 platí a dokažme, že pak platí

Věta 2. *Při kanonickém způsobu vytýkání existuje k danému polynomu právě jedno jeho úplné vytknutí.*

Důkaz. Buď R *libovolný* polynom. Zřejmě stačí ukázat, že úplné vytknutí existuje nejvýše jedno.

Označme M množinu všech výrazů $(R^T)_T$ (tj. množinu úplných roznásobení všech úplných vytknutí polynomu R). Dá se ukázat, že množina M splňuje předpoklady lemmatu 2. (Zde se právě využije kanoničnosti způsobu vytýkání.)

Ponecháme-li v koncové posloupnosti $T(R)$ pouze „nejlevější výskyt" každého prvku a ostatní výskyty vynecháme, dostaneme jednak $T(R^T)$ (pro libovolné R^T – to je také důsledek kanoničnosti), jednak $V(R)$, tedy $T(R^T) = V(R)$. Posloupnost $T((R^T)_T)$ dostaneme z $T(R^T)$ tak, že některé prvky nahradíme několika exempláři těchto prvků, takže $V((R^T)_T) = V(R^T)$. Protože však zřejmě $V(R^T) = T(R^T)$, máme celkem $V((R^T)_T) = V(R)$ pro libovolné R^T. Podle lemmatu 2 je tedy množina M jednoprvková.

Buďte nyní R_1 a R_2 dvě úplná vytknutí polynomu R. Označme $S = (R_1)_T = (R_2)_T$. Je snadno vidět, že R_1 a R_2 jsou úplná vytknutí polynomu S, který je normální a tedy dle tvrzení 2 je $R_1 = R_2$.

Zbývá tedy dokázat tvrzení 2.

Důkaz tvrzení 2. Buď R normální polynom, $k \geqq 1$, $m_i \geqq 0$ $(i = 1, \ldots, k)$, $R = a_{11}, \ldots, a_{1m_1} + \ldots + a_{k1}, \ldots, a_{km_k}$.

Indukcí dle čísla k. Je-li $k = 1$, je $R^T = R$ a jsme hotovi. Nechť tvrzení platí pro $1 \leqq k \leqq p$ a buď $k = p + 1$. Buď dále

$$V(R) = [b_1, \ldots, b_n], \quad n \leqq p + 1 .$$

1. Nechť nejdříve $n \geqq 2$. Označme R_i součet všech elementárních součinů $\alpha \in r(R)$, jejichž minus první prvek je b_i $(i = 1, \ldots, n)$. Pak je $R = R_1 + \ldots + R_n$ a každý R_i je normální polynom a přitom součtem nejvýše p elementárních součinů $(i = 1, \ldots, n)$. Dále se snadno zjistí, že $R^T = R_1^T + \ldots + R_n^T$. Odtud a z indukčního předpokladu tvrzení ihned plyne.

2. Buď tedy $n = 1$. Definujme posloupnosti $\{R^i\}$ a $\{b^i\}$:

$$R^1 = R\,, \quad (b^1 = b_1)\,;$$

je-li $t \geqq 1$ a $v(R^t) = 1$, položme $[b^t] = V(R^t)$; R^{t+1} dostaneme z R^t vynecháním všech minus prvních prvků elementárních součinů patřících do $r(R^t)$;

je-li $v(R^t) \neq 1$, b^t ani R^{t+1} nedefinujeme.

Nechť nyní existuje $t_0 \geqq 1$ tak, že R^{t_0+2} není už definováno, tj. $v(R^{t_0+1}) \geqq 2$. Ukážeme, že pak je

$$(R^1)^T = ((R^{t_0+1})^T)\, b^{t_0}, \ldots, b^1\,.$$

Odtud bude tvrzení plynout dle případu 1 tohoto důkazu. (R^t je totiž normální polynom pro každé t.) Stačí zřejmě dokázat, že pro každé t, $1 \leqq t \leqq t_0$, je

$$(R^t)^T = (R^{t+1})^T b^t\,.$$

Snadno se ukáže, že $(R^t)^T = Xb^t$, kde X (v případě $t = t_0$ ovšem Int X) je nějaký výraz. Z definice posloupnosti $\{R^i\}$ ovšem plyne, že $X = (R^{t+1})^T$.

Buď $d = \min(m_1, \ldots, m_k)$. Dokážeme, že existuje t_0, $1 \leqq t_0 \leqq d$ tak, že $v(R^{t_0+1}) \geqq 2$. Tím budeme s celým důkazem hotovi.

Nechť nejdříve existují aspoň dva elementární součiny α, $\beta \in r(R)$ o d „činitelích", $\alpha = x_1, \ldots, x_d$, $\beta = y_1, \ldots, y_d$. Musí být $\alpha \neq \beta$, tedy existuje t tak, že $x_t \neq y_t$ a nechť t_1 je nejmenší z těchto t. Je-li $v(R^t) = 1$ pro $t < t_1$, můžeme položit $t_0 = t_1 - 1$. Nechť tedy existuje právě jeden elementární součin $\alpha \in r(R)$ o d „činitelích" a buď $v(R^i) = 1$ pro $i = 1, \ldots, d$, čili $(R^1)^T = ((R^{d+1})^T)\, b^d, \ldots, b^1$.

Mezi elementárními součiny patřícími do $r(R^{d+1})$ je ovšem právě jeden prázdný součin I a tedy $V(R^{d+1})$ má aspoň dvě složky, totiž nějaké $b \in \Sigma$ a λ, tedy $v(R^{d+1}) \geqq 2$.

Vyslovíme a dokážeme nyní hlavní větu tohoto paragrafu, která, stejně jako věta 2, je důsledkem tvrzení 2, ale má vzhledem k větě 2 poněkud slabší předpoklady i tvrzení.

Věta 3. *K danému polynomu existuje právě jedno jeho úplné vytknutí až na užití komutativního zákona.* (Tj.: *Libovolná dvě úplná vytknutí daného polynomu se dají převést jedno na druhé k-násobnou* $(k \geqq 0)$ *aplikací pravidla* (A).)

Důkaz. Je-li R libovolný polynom, dá se ukázat, že každé úplné vytknutí polynomu R je roznásobitelné zprava na právě jeden normální polynom. Naopak, existují-li úplná vytknutí P_1 a P_2 tak, že $(P_1)_T = (P_2)_T$, musí být $P_1 = P_2$ (neboť vytýkání „inversní k roznásobování" je kanonické).

Přiřadíme-li tedy každému úplnému vytknutí P normální polynom P_T, dostaneme

prosté zobrazení f množiny *všech* úplných vytknutí polynomu R *na* množinu všech normálních polynomů, které lze dostat z R užitím komutativního zákona, tj. k-násobnou ($k \geqq 0$) aplikací pravidla (A). K důkazu věty tedy stačí ukázat, že platí tvrzení (T):

(T) *Jsou-li* R_1 *a* R_2 *libovolné dva normální polynomy takové, že* $r(R_1) = r(R_2)$, *lze užitím komutativního zákona převést* $f^{-1}(R_1)$ *na* $f^{-1}(R_2)$.

Mějme tedy dva takové polynomy R_1 a R_2 a nechť

$$V(R_1) = [a_1, \ldots, a_n], \quad V(R_2) = [a_{i_1}, \ldots, a_{i_n}],$$

kde $i_1, \ldots, i_n$ je nějaká permutace čísel $1, \ldots, n$.

Je-li S polynom, položme $M(S) = \max \{t \mid x_1, \ldots, x_t \in r(S)\}$.

Tvrzení (T) dokážeme indukcí dle čísla $M(R_1)$.

Je-li $M(R_1) = 1$, je vše jasné. (Případ $M(R_1) = 0$ je triviální.) Nechť tedy je $M(R_1) = s + 1$, $s \geqq 1$ a nechť (T) platí pro polynomy R_1, pro které je $M(R_1) \leqq s$.

Označme A_i součet všech elementárních součinů z $r(R_1)$, jejichž minus první prvek je a_i $(i = 1, \ldots, n)$ a položme $R = A_{i_1} + \ldots + A_{i_n}$. (Z vlastností polynomů R_1 a R_2 plyne, že můžeme přejít od R_1 k R_2 tak, že nejdříve utvoříme R a pak užijeme komutativního zákona na jednotlivé polynomy $A_1, \ldots, A_n$.)

Zřejmě

$$f^{-1}(R_1) = f^{-1}(A_1) + \ldots + f^{-1}(A_n),$$
$$f^{-1}(R) = f^{-1}(A_{i_1}) + \ldots + f^{-1}(A_{i_n}),$$

tedy $f^{-1}(R_1)$ lze převést na $f^{-1}(R)$ užitím komutativního zákona. Stačí tedy ukázat, že $f^{-1}(R)$ lze převést na $f^{-1}(R_2)$ užitím komutativního zákona.

Pišme $R_2 = B_{i_1} + \ldots + B_{i_n}$, kde $r(B_i) = r(A_i)$ $(i = 1, \ldots, n)$. Zvolme k, $1 \leqq k \leqq n$ libovolně. Označme $\tilde{A}_k$ resp. $\tilde{B}_k$ polynomy, které vzniknou z A_k resp. B_k vynecháním všech minus prvních prvků elementárních součinů patřících do $r(A_k)$. Pak je $M(\tilde{A}_k) \leqq s$, $r(A_k) = r(B_k)$ a tedy dle indukčního předpokladu lze převést $f^{-1}(A_k)$ na $f^{-1}(B_k)$ užitím komutativního zákona.

Dále je zřejmé, že

$$f^{-1}(R) = \langle f^{-1}(\tilde{A}_{i_1}) \rangle a_{i_1} + \ldots + \langle f^{-1}(\tilde{A}_{i_n}) \rangle a_{i_n},$$
$$f^{-1}(R_2) = \langle f^{-1}(\tilde{B}_{i_1}) \rangle a_{i_1} + \ldots + \langle f^{-1}(\tilde{B}_{i_n}) \rangle a_{i_n}.$$

Tím je věta 3 dokázána.

(Došlo dne 28. května 1968.)

[1] В. М. Глушков: Синтез цифровых автоматов. Москва 1962.
[2] Mareš: Regulární jazyky a jejich využití při syntéze automatů. Diplomová práce, MFF UK, Praha 1966.

SUMMARY

Two Properties of Expressions in a Certain Free Universal Algebra

JAN MAREŠ

In this paper there is considered a certain free universal algebra, i.e. a set of free generators together with two binary operations + (addition) and . (multiplication) and with some identities. A sum of products of free generators is here said to be a polynomial. Expressions in the algebra are defined as usual. We use the left and right distributivity in the one or in the other direction in order to "transform" one expression into another one.

The proof of the following two statements is given:

1. Let R be an expression. Then it is possible to transform this R into a polynomial, using first the left distributivity only and then the right one only.

2. No matter how we use the right distributivity in one direction beginning with a polynomial and continuing as long as possible, we obtain in all cases the same expression.

Jan Mareš, Matematický ústav ČSAV, Žitná 25, Praha 1.