Formálne jazyky a automaty (1)
Zimný semester 2017/18

# Poznámky k cvičeniu č. 3

Peter Kostolányi

11. októbra 2017

### Bezkontextové a regulárne gramatiky

*Bezkontextové gramatiky* sú frázové gramatiky, v ktorých ľavá strana každého prepisovacieho pravidla pozostáva z jediného neterminálu. Keďže všeobecné definície pojmov súvisiacich s frázovými gramatikami boli zavedené na prednáške, tu sa obmedzíme výhradne na špeciálny prípad bezkontextových gramatík. V nasledujúcom budeme pre dvojicu množín $X, Y$ písať $X \subseteq_{kon} Y$, ak $X$ je *konečnou* podmnožinou množiny $Y$.

**Definícia 1.** *Bezkontextová gramatika* je štvorica $G = (N, T, P, \sigma)$, kde $N$ je abeceda[1] neterminálnych symbolov, $T$ je abeceda terminálnych symbolov, $N \cap T = \emptyset$, $P \subseteq_{kon} N \times (N \cup T)^*$ je konečná množina prepisovacích pravidiel a $\sigma \in N$ je počiatočný neterminál.

*Poznámka* 1. Prepisovacie pravidlá $(\xi, x) \in P$ obyčajne zapisujeme ako $\xi \to x$. Ide iba o špeciálny spôsob zápisu usporiadanej dvojice používaný v tomto kontexte a symbol $\to$ sám o sebe nemá definovaný žiaden význam. Zápis $\xi \to x_1, \xi \to x_2, \ldots, \xi \to x_k$ skracujeme aj ako $\xi \to x_1 \mid x_2 \mid \ldots \mid x_k$.

**Definícia 2.** Nech $G = (N, T, P, \sigma)$ je bezkontextová gramatika. *Krok odvodenia* v gramatike $G$ je binárna relácia $\Rightarrow_G$ na $(N \cup T)^*$ taká, že

$$\begin{aligned} &\forall u, v \in (N \cup T)^* : u \Rightarrow_G v \text{ práve vtedy, keď} \\ &\qquad \exists u_1, u_2, x \in (N \cup T)^* \; \exists \xi \in N : u = u_1 \xi u_2 \;\wedge\; v = u_1 x u_2 \;\wedge\; \xi \to x \in P. \end{aligned}$$

V prípade, že je gramatika $G$ zrejmá z kontextu, píšeme namiesto $\Rightarrow_G$ iba $\Rightarrow$.

Keďže je krok odvodenia $\Rightarrow$ definovaný ako relácia, dajú sa naň aplikovať všetky bežné operácie na reláciách. Pre $k \in \mathbb{N}$ tak napríklad môžeme hovoriť o $k$-tej mocnine relácie $\Rightarrow$, označovanej symbolom $\Rightarrow^k$. V relácii $\Rightarrow^k$ sú potom všetky dvojice slov $u$, $v$ také, že slovo $v$ sa dá odvodiť zo slova $u$ na práve $k$ krokov odvodenia. Podobne možno definovať reflexívno-tranzitívny uzáver $\Rightarrow^*$ a tranzitívny uzáver $\Rightarrow^+$ relácie $\Rightarrow$. V týchto reláciách sú všetky dvojice slov $u$, $v$ také, že slovo $v$ sa dá odvodiť zo slova $u$ na ľubovoľný resp. ľubovoľný nenulový počet krokov. Relácia $\Rightarrow^0$ je identita, podobne ako nultá mocnina ľubovoľnej inej relácie.

Zneužívajúc notáciu zvyčajne hovoríme o „odvodení $\sigma \Rightarrow w_1 \Rightarrow \ldots \Rightarrow w_n$“, o „odvodení $\sigma \Rightarrow^n w_n$“, alebo o „odvodení $\sigma \Rightarrow^* w_n$“, aj keď každý z týchto zápisov vyjadruje iba reláciu medzi slovami a ťažko tak hovoriť o „entite odvodenia“. Žiaden z uvedených zápisov navyše neposkytuje kompletnú informáciu, ktorá sa väčšinou od intuitívneho konceptu odvodenia očakáva. Problém formálneho uchopenia pojmu odvodenia sa však ukazuje ako pomerne delikátny a v literatúre sa často možno stretnúť s chybnými definíciami neskôr kompenzovanými intuíciou. My sa k týmto záležitostiam vrátime na nasledujúcom cvičení, kde sa pokúsime aj o formálne presnú definíciu. Väčšinou sa ale budeme pridŕžať zaužívaných zvyklostí z úvodu tohto odstavca.

**Definícia 3.** Nech $G = (N, T, P, \sigma)$ je bezkontextová gramatika. *Jazyk* generovaný gramatikou $G$ je definovaný ako $L(G) = \{w \in T^* \mid \sigma \Rightarrow^* w\}$.

Slová z jazyka $L(G)$ nazývame *slová generované gramatikou* $G$. Z definície vyplýva, že takéto slová pozostávajú výhradne z terminálnych symbolov. Slovo nad abecedou $N \cup T$, pre ktoré existuje v gramatike $G$ odvodenie, nazývame *vetnou formou* v gramatike $G$. Pre jazyk všetkých vetných foriem v gramatike $G$ budeme na týchto cvičeniach používať *neštandardné* označenie $F(G)$.

**Definícia 4.** Nech $G = (N, T, P, \sigma)$ je bezkontextová gramatika. *Vetná forma* v gramatike $G$ je slovo $x \in (N \cup T)^*$ také, že $\sigma \Rightarrow^* x$. Jazyk všetkých vetných foriem v gramatike $G$ označujeme ako $F(G) = \{x \in (N \cup T)^* \mid \sigma \Rightarrow^* x\}$.

[1] Čiže neprázdna konečná množina.

Jazyk sa nazýva bezkontextový, ak existuje bezkontextová gramatika, ktorá ho generuje:

**Definícia 5.** *Bezkontextový jazyk* je jazyk $L$, pre ktorý existuje bezkontextová gramatika $G$ taká, že $L(G) = L$. *Triedu* všetkých *bezkontextových jazykov* označujeme symbolom $\mathscr{L}_{CF}$.

*Poznámka* 2. Skutočnosť, že hovoríme o *triede* bezkontextových jazykov a nie o *množine* bezkontextových jazykov, nie je náhodná. Pokiaľ sa totiž neobmedzíme na nejakú konkrétnu množinu symbolov, ktoré môžu byť prvkami abecied, množina všetkých bezkontextových jazykov neexistuje. Trieda sa od množiny líši predovšetkým tým, že sama nie je množinou, a teda existuje napríklad aj trieda všetkých množín a podobne.

*Regulárne gramatiky* sú bezkontextové gramatiky, v ktorých sa môže každý neterminál prepísať iba na postupnosť terminálov nasledovanú najviac jedným neterminálom.

**Definícia 6.** *Regulárna gramatika* je bezkontextová gramatika $G = (N, T, P, \sigma)$, pre ktorú platí $P \subseteq_{kon} N \times (T^* \cup T^* N)$.

Keďže sme regulárne gramatiky definovali ako špeciálne bezkontextové gramatiky, vzťahuje sa väčšina definícií a označení zavedených vyššie aj na regulárne gramatiky. V nasledujúcom sa budeme zaoberať metódami dokazovania, že daná gramatika skutočne generuje zamýšľaný jazyk; aj keď budeme hovoriť o bezkontextových gramatikách vo všeobecnosti, rovnaké metódy bude možné použiť aj pre regulárne gramatiky, ktoré sú ich špeciálnym prípadom.

*Poznámka* 3. *Lineárna* gramatika je bezkontextová gramatika $G = (N, T, P, \sigma)$ taká, že platí $P \subseteq_{kon} N \times (T^* \cup T^* N T^*)$ – na pravej strane každého pravidla sa teda môže vyskytovať najviac jeden neterminál. Regulárne gramatiky sú očividne špeciálnym prípadom lineárnych gramatík a niekedy sa preto nazývajú aj *sprava lineárne gramatiky.* V literatúre sa navyše občas definujú sprava lineárne gramatiky ako v definícii 6, pričom pod regulárnymi gramatikami sa rozumie istý normálny tvar takýchto gramatík. My budeme chápať obidve pomenovania ako synonymá, pričom zvyčajne sa budeme držať termínu „regulárna gramatika“.

### Dokazovanie tvrdení typu $L(G) = L$

Samotná konštrukcia bezkontextovej gramatiky k nejakému jazyku ešte nedáva žiadne záruky ohľadom jej korektnosti. Tie poskytuje až formálny dôkaz, že gramatika skutočne generuje zamýšľaný jazyk. Proces dokazovania takýchto tvrdení je oproti procesu hľadania vhodnej gramatiky o poznanie menej tvorivý a minimálne pre „učebnicové“ príklady gramatík vykazuje takmer vždy určité spoločné znaky. Cieľom nasledujúcich partií tohto textu je demonštrovať tento proces na príklade a spomínané spoločné znaky identifikovať.

*Príklad* 1. Predpokladajme, že potrebujeme dokázať, že gramatika $G = (N, T, P, \sigma)$ s $N = \{\sigma\}$, $T = \{a, b\}$ a $P = \{\sigma \to a\sigma a \mid b\sigma b \mid a \mid b \mid \varepsilon\}$ generuje jazyk všetkých palindrómov nad abecedou $\{a, b\}$, čiže jazyk $L = \{w \in \{a, b\}^* \mid w = w^R\}$. Zapísané v stručnosti, treba dokázať $L(G) = L$.

Rovnosti medzi množinami (alebo v našom prípade medzi jazykmi) sa zvyčajne najlepšie dokazujú zvlášť pre každú z inklúzií, pričom inklúzia $X \subseteq Y$ sa obvykle dokazuje pomocou implikácie „ak $x \in X$, tak $x \in Y$“.[2] Dokázať $L(G) = L$ teda znamená dokázať $L(G) \subseteq L$ – čiže „ak $w \in L(G)$, tak $w \in L$“ – a $L(G) \supseteq L$ – čiže „ak $w \in L$, tak $w \in L(G)$“.

Uvažujme teraz inklúziu $L(G) \subseteq L$ a zodpovedajúcu implikáciu „ak $w \in L(G)$, tak $w \in L$“. Tú možno podľa definície 3 prepísať ako „ak $w \in T^*$ a $\sigma \Rightarrow^* w$, tak $w \in L$“. Keďže existencia odvodenia slova $w$ v gramatike $G$ je v zásade naším jediným netriviálnym predpokladom o $w$, prirodzeným prístupom k dôkazu takejto implikácie sa javí byť matematická indukcia vzhľadom na dĺžku odvodenia. To v podstate znamená dokázať vlastnosť $w \in L$ pre slová $w \in T^*$ s odvodením $\sigma \Rightarrow^k x \Rightarrow w$ na základe indukčného predpokladu ohľadom slov $y \in T^*$ s odvodením $\sigma \Rightarrow^k y$. Tu však narážame na problém: keďže platí $x \Rightarrow w$, musí slovo $x$ obsahovať aspoň jeden neterminál. Ide teda o vetnú formu v gramatike $G$, ale nie o slovo generované gramatikou. Preto sa na neho nevzťahuje indukčný predpoklad o príslušnosti do jazyka $L$.

[2] Symbolu $\Rightarrow$ sa ako označeniu pre implikáciu kvôli hroziacemu notačnému konfliktu v súvislosti s gramatikami radšej vyhýbame.

Na podobný problém čitateľ veľmi rýchlo narazí aj pri obdobnom priamočiarom pokuse o dôkaz opačnej inklúzie, kde sa vhodným prístupom javí byť indukcia vzhľadom na určitú štrukturálnu vlastnosť slova $w$ – v tomto prípade by mohlo ísť o hodnotu odvodenú od dĺžky slova $w$.

Z uvedených dôvodov vzniká potreba zosilniť dokazované tvrdenie tak, aby sa vzťahovalo na *všetky vetné formy* v gramatike $G$. To v prvom rade znamená identifikovať jazyk $F$ všetkých vetných foriem v gramatike $G$, pre ktorý zrejme musí platiť $F \cap T^* = L$ (v opačnom prípade ide o signál, že minimálne jeden z jazykov $F$ a $L$ nebol identifikovaný správne). Následne je potrebné dokázať, že skutočne platí $F(G) = F$. Toto tvrdenie je analogické pôvodne dokazovanému tvrdeniu $L(G) = L$, avšak bez predpokladu terminálnosti slov v jednotlivých jazykoch. Je navyše zrejmé, že $F(G) \cap T^* = L(G)$. Z rovnosti $F(G) = F$ teda vyplýva aj rovnosť $L(G) = L$, čo znamená, že tvrdenie $F(G) = F$ je skutočne *zosilnením* pôvodne dokazovaného tvrdenia $L(G) = L$.

V našom prípade možno ľahko dôjsť k hypotéze, že pre vetné formy $x$ v gramatike $G$ vždy platí $x = uzu^R$, kde $u \in T^*$ a $z \in \{\varepsilon, a, b, \sigma\}$.[3] Jazyk $F$ z predchádzajúceho odstavca tak pozostáva z práve takýchto slov; v nasledujúcom budeme dokazovať, že $F(G) = F$. Dokazované tvrdenie teda možno zapísať nasledovne:

$$\forall x \in (N \cup T)^* : \sigma \Rightarrow^* x \text{ práve vtedy, keď } x = uzu^R \text{ pre nejaké } u \in T^* \text{ a } z \in \{\varepsilon, a, b, \sigma\}.$$

Takéto tvrdenie je silnejšie, než pôvodne dokazovaná rovnosť $L(G) = L$, keďže platí $F \cap T^* = L$ (kde $F$ je jazyk opísaný vyššie). Ak totiž $w \in F \cap T^*$, nutne $w = uzu^R$ pre nejaké $u \in T^*$ a $z \in \{\varepsilon, a, b\}$ (očividne nemôže platiť $z = \sigma$, lebo slovo $w$ by potom nebolo terminálne) a opačne. Z implikácie „zľava doprava“ teda priamo vyplýva $L(G) \subseteq L$ a z implikácie „sprava doľava“ vyplýva $L(G) \supseteq L$. Samotný dôkaz tvrdenia $L(G) = L$ potom môže vyzerať napríklad nasledovne:

$\subseteq$: Pre všetky $x \in (N \cup T)^*$ dokážeme nasledujúcu implikáciu:

$$\text{Ak } \sigma \Rightarrow^n x \text{ pre nejaké } n \in \mathbb{N}, \text{ tak } x = uzu^R \text{ pre nejaké } u \in T^* \text{ a } z \in \{\varepsilon, a, b, \sigma\}.$$

Indukciou vzhľadom na $n$.

1. Nech $n = 0$. Potom $x = \sigma$ a tvrdenie platí pre $u = \varepsilon$ a $z = \sigma$.
2. Nech tvrdenie platí pre $n = k$. Dokážeme, že platí aj pre $n = k + 1$.
   Nech $x \in (N \cup T)^*$ je slovo také, že $\sigma \Rightarrow^{k+1} x$. To možno rozpísať ako $\sigma \Rightarrow^k y \Rightarrow x$. Na odvodenie $\sigma \Rightarrow^k y$ sa vzťahuje indukčný predpoklad, a teda $y = vz'v^R$ pre nejaké $v \in T^*$ a $z' \in \{\varepsilon, a, b, \sigma\}$.
   Keďže platí $y \Rightarrow x$, musí slovo $y$ obsahovať aspoň jeden neterminál. Z toho vyplýva $z' = \sigma$, a teda $y = v\sigma v^R$ pre nejaké $v \in T^*$.
   Slovo $x$ je možné odvodiť z $y$ použitím niektorého z prepisovacích pravidiel z $P$ na neterminál $\sigma$. V prípade, že ide o niektoré z pravidiel $\sigma \to a\sigma a$ alebo $\sigma \to b\sigma b$, dostávame $x = va\sigma av^R$ resp. $x = vb\sigma bv^R$ a tvrdenie platí pre $u = va$ resp. $u = vb$ a $z = \sigma$. V prípade, že ide o niektoré z pravidiel $\sigma \to a$, $\sigma \to b$, alebo $\sigma \to \varepsilon$, dostávame $x = vav^R$, $x = vbv^R$, resp. $x = vv^R$ a tvrdenie platí pre $u = v$ a $z = a$, $z = b$, resp. $z = \varepsilon$.

$\supseteq$: Pre všetky $x \in (N \cup T)^*$ dokážeme nasledujúcu implikáciu:

$$\text{Ak } x = uzu^R \text{ pre nejaké } u \in T^* \text{ a } z \in \{\varepsilon, a, b, \sigma\}, \text{ tak } \sigma \Rightarrow^* x.$$

Indukciou vzhľadom na $|u|$.

1. Nech $|u| = 0$. Potom $x \in \{\varepsilon, a, b, \sigma\}$ a tvrdenie platí, lebo očividne $\sigma \Rightarrow^0 \sigma$, $\sigma \Rightarrow \varepsilon$, $\sigma \Rightarrow a$ a $\sigma \Rightarrow b$.
2. Nech tvrdenie platí pre $|u| = k$. Dokážeme, že platí aj pre $|u| = k + 1$.
   Nech $x = uzu^R$ pre nejaké $u \in T^{k+1}$ a $z \in \{\varepsilon, a, b, \sigma\}$. Potom existuje slovo $v \in T^k$ a písmeno $c \in T$ tak, že $x = vczcv^R$. Z indukčného predpokladu vyplýva $\sigma \Rightarrow^* v\sigma v^R$.

[3] Čitateľ si je snáď vedomý toho, že takto definované $z$ je vo všeobecnosti slovo a nie symbol.

Použitím pravidla $\sigma \to c\sigma c$ dostávame $\sigma \Rightarrow^* v\sigma v^R \Rightarrow vc\sigma cv^R$. To je v prípade $z = \sigma$ už postačujúce. V opačnom prípade obsahuje množina $P$ pravidlo $\sigma \to z$, použitím ktorého dostávame $\sigma \Rightarrow^* v\sigma v^R \Rightarrow vc\sigma cv^R \Rightarrow vczcv^R$.

Tvrdenie $L(G) = L$ je týmto dokázané.

Podobný postup možno pre „učebnicové" gramatiky použiť skoro univerzálne, pričom komplikovanosť dôkazu závisí od komplikovanosti gramatiky. Základné body takéhoto postupu možno zhrnúť nasledovne:

1. Identifikuj jazyk $F$ všetkých vetných foriem v $G$ a over, že platí $F \cap T^* = L$.
2. Namiesto $L(G) \subseteq L$ dokáž silnejšie tvrdenie $F(G) \subseteq F$, čiže „ak $\sigma \Rightarrow^* x$, tak $x \in F$" – zvyčajne indukciou vzhľadom na dĺžku odvodenia.
3. Namiesto $L(G) \supseteq L$ dokáž silnejšie tvrdenie $F(G) \supseteq F$, čiže „ak $x \in F$, tak $\sigma \Rightarrow^* x$" – zvyčajne indukciou vzhľadom na určité štrukturálne vlastnosti slova $x$. Často je potrebné využiť viac ako jednu štrukturálnu vlastnosť, čiže je nutné urobiť aj niekoľko indukcií.

Zvyčajne si pritom vystačíme aj bez toho, aby sme jazyk $F$ konštruovali explicitne – akákoľvek charakterizácia množiny všetkých vetných foriem je ale implicitnou definíciou tohto jazyka. Nasledujúca ukážková riešená úloha má za cieľ demonštrovať možnosti využitia uvedeného postupu.

**Úloha 1.** Nech $L = \{a^n cwcb^{2n} \mid n \in \mathbb{N};\ w \in \{a,b\}^*;\ \#_a(w) = \#_b(w)\}$. Zostrojte bezkontextovú gramatiku generujúcu jazyk $L$ a správnosť svojej konštrukcie dokážte.

*Riešenie.* Dokážeme, že jazyk $L$ je generovaný bezkontextovou gramatikou $G = (N, T, P, \sigma)$, kde $N = \{\sigma, \alpha\}$, $T = \{a, b, c\}$ a $P = \{\sigma \to a\sigma bb \mid c\alpha c, \alpha \to \alpha a\alpha b\alpha \mid \alpha b\alpha a\alpha \mid \varepsilon\}$.

Identita $L(G) = L$ vyplynie zo silnejšieho tvrdenia, že $x$ je vetná forma v gramatike $G$ práve vtedy, keď je splnená niektorá z nasledujúcich podmienok:

(*i*) $x = a^i\sigma b^{2i}$ pre nejaké $i \in \mathbb{N}$, alebo

(*ii*) $x = a^i cycb^{2i}$ pre nejaké $i \in \mathbb{N}$, kde $y = z_0 d_1 z_1 \dots z_{2j-1} d_{2j} z_{2j}$ pre nejaké číslo $j \in \mathbb{N}$, slová $z_0, \dots, z_{2j} \in \{\varepsilon, \alpha\}$ a symboly $d_1, \dots, d_{2j} \in \{a, b\}$, pričom platí $\#_a(y) = \#_b(y)$.

Práve sformulované tvrdenie implikuje $L(G) = L$, pretože jazyk *terminálnych* slov $x$ spĺňajúcich niektorú z podmienok (*i*) alebo (*ii*) je zjavne rovný jazyku $L$. Pristúpme teda k dôkazu jednotlivých inklúzií.

$\subseteq$: Nech $x \in (N \cup T)^*$. Dokážeme, že ak pre nejaké $n \in \mathbb{N}$ platí $\sigma \Rightarrow^n x$, tak je splnená jedna z podmienok (*i*), (*ii*). Indukciou vzhľadom na $n$.

1. Pre $n = 0$ je $x = \sigma$, a teda platí (*i*).
2. Predpokladajme, že tvrdenie platí pre $n = k$. Dokážeme, že platí aj pre $n = k + 1$. Nech $\sigma \Rightarrow^{k+1} x$. To možno rozpísať ako $\sigma \Rightarrow^k x' \Rightarrow x$. Na odvodenie $\sigma \Rightarrow^k x'$ sa vzťahuje indukčný predpoklad, a teda pre vetnú formu $x'$ platí (*i*) alebo (*ii*):
   a) Nech pre $x'$ platí (*i*). Potom $x' = a^{i'}\sigma b^{2i'}$ pre nejaké $i' \in \mathbb{N}$. Keďže $x' \Rightarrow x$, vetná forma $x$ musí byť odvoditeľná z $x'$ použitím niektorého z pravidiel na $\sigma$. Ak ide o pravidlo $\sigma \to a\sigma bb$, dostávame $x = a^{i'}a\sigma bbb^{2i'} = a^{i'+1}\sigma b^{2(i'+1)}$ a platí (*i*). V prípade, že ide o pravidlo $\sigma \to c\alpha c$, $x = a^{i'}c\alpha cb^{2i'}$ a platí (*ii*) pre $y = \alpha$ a $j = 0$.
   b) Nech pre $x'$ platí (*ii*). Potom máme $x' = a^{i'}cy'cb^{2i'}$ pre nejaké $i' \in \mathbb{N}$ a nejaké $y' = z_0'd_1'z_1' \dots z_{2j'-1}'d_{2j'}'z_{2j'}'$, kde $j' \in \mathbb{N}$, $z_0', \dots, z_{2j'}' \in \{\varepsilon, \alpha\}$, $d_1', \dots, d_{2j'}' \in \{a, b\}$ a $\#_a(y') = \#_b(y')$. Keďže $x' \Rightarrow x$, vetná forma $x$ musí byť odvoditeľná z $x'$ použitím niektorého z pravidiel na $z_s' = \alpha$ pre nejaké $s \in \{0, \dots, 2j'\}$. Potom $x = a^{i'}cy''cb^{2i'}$, kde $y'' = z_0'd_1'z_1' \dots d_s'ud_{s+1}' \dots z_{2j'-1}'d_{2j'}'z_{2j'}'$ a $u$ je pravá strana pravidla $\alpha \to u$ použitého v tomto kroku odvodenia, $u \in \{\varepsilon, \alpha a\alpha b\alpha, \alpha b\alpha a\alpha\}$. Pre všetky prípustné $u$ je pre $x$ splnená podmienka (*ii*).

$\supseteq$: Nech $x \in (N \cup T)^*$. Dokážeme, že ak pre $x$ platí $(i)$ alebo $(ii)$, tak $\sigma \Rightarrow^* x$.

a) Nech pre $x$ platí $(i)$, t.j. $x = a^i \sigma b^{2i}$ pre nejaké $i \in \mathbb{N}$. Indukciou na $i$ dokážeme $\sigma \Rightarrow^* x$.

   1. Pre $i = 0$ je $x = \sigma$ a platí $\sigma \Rightarrow^0 \sigma = x$.
   2. Nech tvrdenie platí pre $i = k$ a $\sigma \Rightarrow^* a^k \sigma b^{2k}$. Potom $\sigma \Rightarrow^* a^k \sigma b^{2k} \Rightarrow a^{k+1} \sigma b^{2(k+1)}$ a tvrdenie platí aj pre $i = k + 1$.

b) Nech pre $x$ platí $(ii)$. Potom $x = a^i cycb^{2i}$ pre nejaké $i \in \mathbb{N}$, kde $y = z_0 d_1 z_1 \dots z_{2j-1} d_{2j} z_{2j}$ pre nejaké $j \in \mathbb{N}$, $z_0, \dots, z_{2j} \in \{\varepsilon, \alpha\}$ a $d_1, \dots, d_{2j} \in \{a, b\}$, pričom platí $\#_a(y) = \#_b(y)$. Indukciou vzhľadom na $j$ dokážeme, že $\sigma \Rightarrow^* x$.

   1. Nech $j = 0$. Potom $y = z_0 \in \{\varepsilon, \alpha\}$. Z tvrdenia dokázaného v bode a) ale vyplýva $\sigma \Rightarrow^* a^i \sigma b^{2i} \Rightarrow a^i c\alpha c b^{2i}$ a $\sigma \Rightarrow^* a^i \sigma b^{2i} \Rightarrow a^i c\alpha c b^{2i} \Rightarrow a^i ccb^{2i}$.
   2. Nech tvrdenie platí pre $j = k$. Ukážeme, že platí aj pre $j = k + 1$.
      Keďže pre slovo $y = z_0 d_1 z_1 \dots z_{2k+1} d_{2(k+1)} z_{2(k+1)}$ platí $\#_a(y) = \#_b(y)$, musí existovať $s \in \{0, \dots, 2k + 1\}$ také, že $d_s = a$ a $d_{s+1} = b$ alebo naopak. Inými slovami: existuje $s$ také, že platí buď $y = z_0 \dots d_{s-1} z_{s-1} a z_s b z_{s+1} d_{s+2} \dots z_{2(k+1)}$, alebo $y = z_0 \dots d_{s-1} z_{s-1} b z_s a z_{s+1} d_{s+2} \dots z_{2(k+1)}$.
      Pre slovo $y' = z_0 \dots d_{s-1} \alpha d_{s+2} \dots z_{2(k+1)}$ zrejme tiež platí $\#_a(y') = \#_b(y')$, čo znamená, že na slovo $x' = a^i c y' c b^{2i}$ sa vzťahuje indukčný predpoklad a $\sigma \Rightarrow^* x'$.
      Keďže ale zjavne $y' = z_0 \dots d_{s-1} \alpha d_{s+2} \dots z_{2(k+1)} \Rightarrow^* z_0 \dots d_{s-1} u d_{s+2} \dots z_{2(k+1)}$ pre všetky $u \in \{z'_{s-1} d'_s z'_s d'_{s+1} z'_{s+1} \mid z'_{s-1}, z'_s, z'_{s+1} \in \{\varepsilon, \alpha\};\ d'_s \neq d'_{s+1} \in \{a, b\}\}$, platí aj $\sigma \Rightarrow^* x' \Rightarrow x$, čo bolo treba dokázať.

Tvrdenie je dokázané. $\square$