Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Varianty pojmu užitočnosti informácie

Bakalárska práca

2023
Vincent Hlaváč

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Varianty pojmu užitočnosti informácie

Bakalárska práca

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	prof. RNDr. Branislav Rovan, PhD.

Bratislava, 2023
Vincent Hlaváč

77747164

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Vincent Hlaváč
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Varianty pojmu užitočnosti informácie
Variants of the notion of usefulness of information

Anotácia: Práca bude pokračovaním skúmania pojmu užitočnosti informácie. Cieľom je definovať a analyzovať modifikácie pojmu užitočnosti informácie. Napríklad zaviesť možnosť viacnásobnej rady alebo zaviesť prísnejšie podmienky na užitočnosť.

Cieľ: Práca bude pokračovaním skúmania pojmu užitočnosti informácie. Cieľom je definovať a analyzovať modifikácie pojmu užitočnosti informácie. Napríklad zaviesť možnosť viacnásobnej rady alebo zaviesť prísnejšie podmienky na užitočnosť.

Vedúci: prof. RNDr. Branislav Rovan, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 12.10.2022

Dátum schválenia: 13.10.2022

doc. RNDr. Dana Pardubská, CSc.
garant študijného programu

.... študent

.... vedúci práce

Poďakovanie: Ďakujem môjmu skvelému školiteľovi, profesorovi Rovanovi, za vedenie pri práci a ochotu odpovedať na všetky moje otázky.

Abstrakt

V tejto práci pokračujeme v skúmaní pojmu užitočnosti informácie pri riešení problému. Berieme problémy formalizované regulárnym jazykom L nad unárnou abecedou a za zložitosť problému považujeme stavovovú zložitosť minimálneho automatu A akceptujúceho jazyk L. Zisťujeme či existuje dodatočná informácia L_{adv}, ktorá nám umožní riešiť problém ľahšie, teda nájsť nový problém L_{new} taký, že $L_{adv} \cap L_{new} = L$, pričom pre automaty A_{adv} a A_{new} akceptujúce jazyky L_{adv} a L_{new} musí platiť, že majú menšiu stavovú zložitosť ako automat A. Na toto sa pozeráme ako na rozklad automatu A na A_{adv} a A_{new}. Zavádzame možnosť druhej dodatočnej informácie L_{adv2} a skúmame rozklad automatu A na tri nové automaty A_{adv}, A_{adv2} a A_{new}, kde A_{adv2} akceptuje jazyk L_{adv2} a opäť je menšej stavovej zložitosti ako automat A. Ďalej skúmame kvalitu rozkladov, za ktorú berieme súčet stavových zložitostí automatov rozkladu. Ukážeme horné a dolné hranice kvality pre jednotlivé rozklady a porovnáme kvalitu rozkladov automatu A na dva a tri nové automaty.

Kľúčové slová: užitočnosť informácie, rada, unárny deterministický konečný automat, rozložiteľnosť, rozklad, kvalita rozkladu, stavová zložitosť

Abstract

In this thesis we continue the research of the notion of usefulness of information for problem solving. We deal with problems formalized by the unary regular language L and for the problem complexity we consider the state complexity of the minimal automaton A accepting language L. We determine if there exists an additional information L_{adv}, which will allow us to solve the problem more easily, thus find a new problem L_{new}, such that $L_{adv} \cap L_{new} = L$, while automata A_{adv} and A_{new} accepting languages L_{adv} and L_{new} have lower state complexity then automaton A. We formalize this situation as decomposition of the automaton A into automata A_{adv} and A_{new}. We introduce the option of the second additional information L_{adv2} and examine decomposition of the automaton A into three new automata A_{adv}, A_{adv2} and A_{new}, where automaton A_{adv2} accepts language L_{adv2} and once again it has lower state complexity then the automaton A. We further examine the quality of decomposition, for which we consider the sum of state complexities of automata forming decomposition. We give upper and lower bounds for quality of decompositions and compare the quality of decompositions of the automaton A into two and three new automata.

Keywords: usefulness of information, advice, unary deterministic finite automaton, decomposability, decomposition, quality of decomposition, state complexity

Obsah

Zoznam obrázkov

Úvod

V tejto práci budeme pokračovať v skúmaní pojmu *informácie*. Keď hovoríme o pojme informácia, môžu nás zaujímať jej rôzne aspekty ako *množstvo*, *aktuálnosť* alebo *užitočnosť*. Pri množstve nás zaujíma ako veľká je informácia, ktorú sme dostali, respektíve koľko informácie potrebujeme. To korešponduje s reálnym životom, kde často na riešenie nejakého problému potrebujeme informáciu určitého rozsahu alebo môžeme mať obmedzený priestor, kde môžeme danú informáciu zaznamenať. V prípade aktuálnosti nás zaujíma ako stará informácia je, respektíve kedy sme ju dostali. Opäť to korešponduje s reálnym životom, kde má význam, kedy sa nejakú informáciu dozvieme, pretože môže byť aktuálna len nejaký čas a neskôr by už pre nás nemala žiadny význam. V prípade užitočnosti informácie nás zaujíma ako užitočná informácia je, respektíve do akej miery nám pomôže. Aj v reálnom živote sú pre nás niektoré informácie užitočnejšie ako iné. Napríklad nám viac pomôžu pri riešení nejaké problému alebo nás len jednoducho viac zaujmú.

My sa budeme venovať práve skúmaniu užitočnosti informácie. Podstatu pojmu môžeme popísať takto: *Informáciu považujeme za užitočnú, ak nám pomôže riešiť problém ľahšie* [1]. Pre daný problém chceme zistiť či existuje dodatočná informácia o vstupe, ktorá by nám umožnila riešiť problém v istom zmysle ľahšie. Od dodatočnej informácie taktiež požadujeme, aby bola *rozumná*, teda overenie jej správnosti, by nemalo byť ťažšie ako riešenie pôvodného problému. Inak by mala takáto informácia príliš veľkú silu a riešenie problému by mohla urobiť triviálnym. Práve takáto informácia je pre nás užitočná, keďže nám zjednoduší riešený problém.

Budeme mať teda problém, pre ktorý budeme chcieť zistiť či existuje nejaká dodatočná informácia o vstupe a nejaký nový problém, ktoré spolu presne určia riešenie pôvodného problému. Od nového problému vyžadujeme, aby jeho riešenie bolo jednoduchšie ako riešenie pôvodného problému. Zároveň aj na dodatočnú informáciu, ktorú nazveme aj *rada*, sa môžeme pozerať ako na jednoduchšie riešenie nejakého ďalšieho nového problému. Na celú situáciu sa teda môžeme pozerať aj ako na rozklad problému, respektíve jeho riešenia na dva nové jednoduchšie problémy, respektíve ich riešenia.

Na formalizáciu využijeme teóriu formálnych jazykov a automatov, pričom problém budeme formalizovať jazykom L a za jeho riešenie budeme považovať automat A

akceptujúci daný jazyk. Pričom budeme skúmať možnosť rozkladu jazyka L na nové jazyky, respektíve automatu A na nové automaty. V posledných rokoch sa skúmali rôzne prípady, kde boli brané ako riešenia problémov deterministické konečné automaty DFA, nedeterministické konečné automnaty NFA, deterministické zásobníkové automaty dPDA, ale aj ďalšie varianty, kde bolo napríklad najprv potrebné rady preložiť. Prehľad je možné násjť v článku On Usefulness of Information: Framework and NFA Case [1].

V našej práci sa budeme venovať prípadu DFA nad unárnou abecedou, kde nadviažeme na existujúce výsledky, ktoré uvedieme v Kapitole 1. V Kapitole 2 budeme skúmať kvalitu kozkladov DFA. V Kapitole 3 uvedieme možnosť pridania druhej rady, teda budeme skúmať ako nám zjednoduchšia problém dve dodatočné informácie. Respektíve sa budeme pozerať na rozklad DFA na tri nové automaty. Rozklad na viac automatov zavedieme s myšlienkou zlepšenia kvality rozkladu oproti rozkladom na dva automaty. V záverečnej Kapitole 4 preskúmame kvalitu rozkladov DFA na tri nové automaty a porovnáme ju s kvalitou rozkladov DFA na dva nové automaty.

Pôvodnou motiváciou pre skúmanie pojmu užitočnosti informácie bolo využitie paralelizmu pri alternujúcich automatoch. Pri výpočte alternujúceho automatu môže dôjsť k rozdeleniu na dve vetvy, ktoré ďalej počítajú nezávisle od seba. Jedna vetva výpočtu akoby dostane radu od druhej a sama už rieši len nejaký jednoduchší problém, čo zodpovedá nami skúmanému rozkladu automatov.

Kapitola 1

Definície a stav problematiky

V tejto kapitole formálne definujeme rozklady jazykov a automatov na dva nové jazyky respektíve automaty v prípade DFA, ktorým sa budeme zaoberať. Ďalej uvedieme niektoré výsledky v danej oblasti, na ktoré v tejto práci nadviažeme. Okrem toho uvedieme aj niekoľko pomocných tvrdení z rôznych oblastí, ktoré budeme neskôr potrebovať.

1.1 Formalizácia

Pre formalizáciu sme zvolili teóriu formálnych jazykov a automatov. Budeme používať štandardné značenie (pozri napr. J.E. Hopcroft, J.D. Ullman [2]). Dĺžku vstupného slova w budeme označovať $|w|$, počet prvkov monžiny S budeme označovať $|S|$. Prázdne slovo budeme označovať ε a prázdnu množinu $\emptyset$. Deterministický konečný automat DFA je pätica $A = (Q, \Sigma, \delta, q_0, F)$, kde Q je konečná množina stavov a $F \subseteq Q$ množina akceptačných stavov, Σ je vstupná abeceda, teda konečná množina symbolov, $\delta : Q \times \Sigma \to Q$ je prechodová funkcia, ktorá je totálna a $q_0 \in Q$ je počiatočný stav. Konfigurácia je dvojica $(q, u) \in Q \times \Sigma^*$. Krok výpočtu automatu A je relácia na konfiguráciach $\vdash_A$, pričom platí, že dve konfigurácie sú spolu v relácii, ak sa dá z jednej dostať do druhej pomocou prechodovej funkcie, formálne $(q, au) \vdash_A (p, u)$ ak $\delta(q, a) = p$. Keď je z kontextu zjavné, že ide o automat A budeme krok výpočtu automatu A značiť len $\vdash$. Výpočet automatu A na slove w je postupnosť konfigurácii, kde prvá je tvaru (q_0, w) a posledná (p, ε) pre nejaké $p \in Q$, pričom každé dve po sebe idúce konfigurácie sú spolu v relácii $\vdash$. Akceptačný výpočet je výpočet končiaci v akceptačnom stave $p \in F$. Jazyk akceptovaný automatom A označujeme $L(A) = \{w \mid w \in \Sigma^*, \exists q \in F \ (q_0, w) \vdash^* (q, \varepsilon)\}$, teda sú to všetky také slová w, na ktorých existuje akceptačný výpočet automatu A. Počet stavov automatu A značíme $\#_S(A) = |Q|$. Stavová zložitosť automatu A je počet jeho stavov, teda $\#_S(A)$, budeme ju označovať $sc(A)$. Deterministický konečný automat

A_{min} akceptujujúci jazyk L je minimálny, ak neexistuje automat A akceptujúci L, pre ktorý platí, že $sc(A) < sc(A_{min})$. Deterministická stavová zložitosť regulárneho jazyka $L \in \mathcal{R}$ je stavová zložitosť minimálneho DFA akceptujúceho jazyk L, teda $min\{sc(A) \mid L(A) = L\}$, budeme ju označovať $sc(L)$.

1.2 Teória čísel

Uveďme niekoľko tvrdení z teórie čísel, ktoré budeme v práci potrebovať.

Veta 1 (Zovšeobecnená Čínska Zvyšková Veta (CRT) [3])**.** *Nech $n_1, \ldots, n_k$ sú kladné celé čísla a nech $a_1, \ldots, a_k$ sú ľubovoľné celé čísla. Potom systém kongruencii*

$$x \equiv a_1 \ (mod\ n_1), \quad \ldots, \quad x \equiv a_k \ (mod\ n_k)$$

má riešenie x práve vtedy, keď $gcd(n_i, n_j)$ delí $a_i - a_j$ pre každé $i \neq j$. Navyše ak riešenie x existuje, tak všetky riešenia sú navzájom kongruentné modulo n, kde $n = lcm(n_1, \ldots, n_k)$.

Poznámka 1. Ak zoberieme $n_1, \ldots, n_k$ po dvoch nesúdeliteľné, teda $gcd(n_i, n_j) = 1$ pre každé $i \neq j$, tak dostávame Čínsku Zvyškovú Vetu v štandardnom znení.

Poznámka 2. Uvedomme si, že podmienku $gcd(n_i, n_j)$ *delí* $a_i - a_j$ *pre každé* $i \neq j$ môžeme ekvivalentne prepísať na podmienku $a_i \equiv a_j \ (mod\ gcd(n_i, n_j))$ *pre každé* $i \neq j$.

Veta 2 (Euklidova Veta [3])**.** *Existuje nekonečne veľa prvočísel.*

Veta 3 (Nerovnosť Aritmetického a Geometrického Priemeru (AM-GM) [4])**.** *Nech $a_1, a_2, \ldots, a_n$ sú ľubovoľné kladné reálne čísla. Potom platí nerovnosť*

$$\frac{a_1 + a_2 + \ldots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n}$$

pričom rovnosť platí práve vtedy, keď $a_1 = a_2 = \ldots = a_n$.

Tvrdenie 1. *Nech $x, y \in \mathbb{Z}$, nech $\lambda_1, \lambda_2 \in \mathbb{N}^+$. Ak $x \equiv y \ (mod\ lcm(\lambda_1, \lambda_2))$, tak potom aj $x \equiv y \ (mod\ \lambda_1)$ a tiež $x \equiv y \ (mod\ \lambda_2)$.*

Dôkaz. Nech x, y patria do $\mathbb{Z}$, nech λ_1, λ_2 patria do $\mathbb{N}^+$. Označme $lcm(\lambda_1, \lambda_2) = l$. Nech platí $x \equiv y \ (mod\ lcm(\lambda_1, \lambda_2))$, teda $x \equiv y \ (mod\ l)$. Vieme, že $l = \alpha_1\lambda_1 = \alpha_2\lambda_2$ pre nejaké α_1, α_2 z $\mathbb{N}$. Ďalej platí, že $x - y = kl$ pre nejaké k z $\mathbb{N}$. Teda $x - y = k\alpha_1\lambda_1$ a aj $x - y = k\alpha_2\lambda_2$. Potom $x - y = \beta_1\lambda_1$ pre $\beta_1 = k\alpha_1$, teda β_1 je z $\mathbb{N}$, rovnako aj $x - y = \beta_2\lambda_2$ pre $\beta_2 = k\alpha_2$, teda β_2 je z $\mathbb{N}$. Z toho dostávame, že $x \equiv y \ (mod\ \lambda_1)$ a aj $x \equiv y \ (mod\ \lambda_2)$. $\square$

Tvrdenie 2. *Nech $a, c \in N$ a nech navyše platí a/c. Potom pre každé $n \in N$ platí, že n mod $a = (n$ mod $c)$ mod a.*

Dôkaz. Nech a, c patria do $\mathbb{N}$ a platí a/c. Teda $c = \alpha a$ pre nejaké α z $\mathbb{N}$. Nech n patrí do $\mathbb{N}$. Nech $n \ mod \ a = x$, teda $n = k_1 a + x$ pre nejaké k_1 z $\mathbb{N}$ a tiež platí, že $x < a$. Nech $n \ mod \ c = y$, teda $n = k_2 c + y$ pre nejaké k_2 z $\mathbb{N}$ a tiež platí, že $y < c$. Nech $y \ mod \ a = z$, teda $y = k_3 a + z$ pre nejaké k_3 z $\mathbb{N}$ a tiež platí, že $z < a$. Z toho dostávame $n = k_2 c + y = k_2 \alpha a + k_3 a + z = (k_2 \alpha + k_3)a + z$. Tiež vieme, že $n = k_1 a + x$ a taktiež $z, x < a$. Teda platí $k_1 = k_2 \alpha + k_3$ a tiež $z = x$. Z toho dostávame $(n \ mod \ c) \ mod \ a = y \ mod \ a = z = x = n \ mod \ a$. □

1.3 2-rozložiteľnosť

Poďme bližšie pozrieť na 2-rozložiteľnosť v prípade deterministických konečných automatov DFA, na ktorý v tejto práci nadviažeme. Budeme sa zaoberať problémami formalizovanými nejakým regulárnym jazykom $L \in \mathcal{R}$, respektíve za problém môžeme považovať rozhodnutie či vstupné slovo w patrí do L ($w \in L$). DFA A akceptujúci jazyk L budeme považovať za jeho riešenie. Za zložitosť riešenia budeme uvažovať stavovú zložitosť automatu A ($sc(A)$). Za zložitosť problému L potom budeme uvažovať deterministickú stavovú zložitosť jazyka L ($sc(L)$).

Dodatočnú informáciu o vstupe w formalizujeme pomocou regulárneho jazyka $L_{adv} \in \mathcal{R}$, respektíve za radu považujeme informáciu, že $w \in L_{adv}$. Pre DFA A_{adv} akceptujúci radu L_{adv} musí platiť $sc(A_{adv}) < sc(A_{min})$, kde A_{min} je minimálny automat akceptujúci L, aby bola rada rozumná. Inak by existovalo riešenie pôvodného problému L, ktoré by bolo jednoduchšie ako overenie správnosti rady, teda príslušnosti vstupného slova w do jazyka L_{adv}. Ďalej budeme za radu vždy považovať rozumnú radu.

Zaujíma nás či pre daný problém L existuje taká rada L_{adv}, ktorá nám umožní nájsť jednoduchší problém L_{new}, pričom platí, že $L_{adv} \cap L_{new} = L$, teda riešenia nových dvoch problémov jednoznačne určujú riešenie pôvodného problému L. Problém L_{new} považujeme za jednoduchší ako L, ak pre riešenie problému, DFA A_{new} akceptujúci jazyk L_{new} platí, že $sc(A_{new}) < sc(A_{min})$. Na túto situáciu sa môžeme pozerať aj ako na rozklad jazyka L na jazyky L_{adv} a L_{new}, respektíve ako na rozklad automatu A_{min} na automaty A_{adv} a A_{new}. Teraz si to môžeme sformalizovať.

Definícia 1 ([5])**.** Nech A je DFA. Dvojicu DFA $[A_1, A_2]$ nazývame *2-rozklad* DFA A ak $L(A) = L(A_1) \cap L(A_2)$, $sc(A_1) < sc(A)$ a $sc(A_2) < sc(A)$. Ak takýto 2-rozklad A existuje, hovoríme, že A je *2-rozložiteľný*.

Poznámka 3. V pôvodnom článku [5] je v definícii namiesto pojmu 2-rozklad len rozklad a namiesto 2-rozložiteľný len rozložiteľný, keďže sa zaoberá len rozkladmi automatu A na dva nové automaty. My však neskôr (Kapitola 3) zavedieme 3-rozložiteľnosť, a preto sme si definíciu trochu upravili pre jednoznačné rozlíšenie daných pojmov. Obdobná situácia platí aj pre nasledujúcu definíciu. Rovnako v pôvodnom článku [5] nie je rozklad definovaný ako dvojica, ale len, že dva automaty tvoria rozklad. Túto úpravu sme urobili, aby sa nám ľahšie formálne definovala kvalita rozkladu (Kapitola 2).

Na jazyk $L(A_1)$ sa môžeme pozerať ako na nový jednoduchší problém, zatiaľ čo na jazyk $L(A_2)$ ako na radu. Ak je minimálny DFA A_{min} akceptujúci regulárny jazyk L 2-rozložiteľný, potom existujú DFA A_{adv}, A_{new} akceptujúce jazyky L_{adv}, L_{new} také, že $L = L_{adv} \cap L_{new}$ a platí $sc(A_{adv}) < sc(A_{min})$ a $sc(A_{new}) < sc(A_{min})$. Teda existujú jednoduchšie problémy L_{adv} a L_{new}, ktoré jednoznačne určujú riešenie problému L. Môžeme teda povedať, že jazyk L je *2-rozložiteľný*. Teraz si to môžeme sformalizovať.

Definícia 2 ([5])**.** Nech $L \in \mathcal{R}$. Hovoríme, že L je deterministicky 2-rozložiteľný ak minimálny DFA akceptujúci L je 2-rozložiteľný.

Poznámka 4. Všimnime si, že automaty A_1 respektíve A_2 tvoriace 2-rozklad minimálneho DFA A_{min} akceptujúceho L nemusia byť minimálne akceptujúce jazyky $L(A_1)$ respektíve $L(A_2)$. Stačí nám len existencia menších automatov ako automat A_{min} takých, že $L(A_1) \cap L(A_2) = L$, aby bol L 2-rozložiteľný.

1.4 Unárne DFA

Teraz sa pozrime na regulárne jazyky nad unárnou abecedou. Takéto jazyky sú akceptované unárnym deterministickým konečným automatom UDFA, čiže klasickým DFA, ktorého vstupná abeceda má len jeden symbol. Potom v grafe takéhoto automatu ide z každého stavu najviac jedna šípka. Zároveň v našej definícii konečného automatu nepovolujeme, aby sa zasekol a nedočítal vstupné slovo, takže z každého stavu musí ísť práve jedna šípka vchádzajúca do iného. Takýto automat potom bude vyzerať ako reťaz, ktorá bude ukončená *cyklom*. Keďže počet stavov automatu musí byť konečný, na reťazi musí prísť stav, z ktorého pôjde šípka do nejakého predchádzajúceho stavu, čím vytvoríme na konci reťaze cyklus. Reťaz pred začiatkom cyklu nazývame *chvost*.

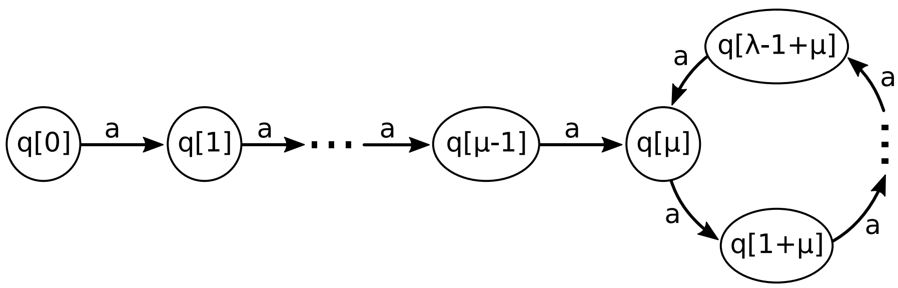
Prirodzene sa môžeme na veľkosť takéhoto automatu pozerať ako na veľkosť chvosta a veľkosť cyklu, ktoré meriame počtom ich stavov. Veľkosť chvosta budeme označovať $\mu \in \mathbb{N}$, veľkosť cyklu $\lambda \in \mathbb{N}$. Teraz formálne.

Definícia 3 ([5])**.** Veľkosť UDFA A je dvojica (λ, μ), kde λ je počet stavov cyklu automatu A a μ je počet stavov chvostu automatu A.

Poznámka 5. Všimnime si, chvost môže byť aj nulovej dĺžky, vtedy bude celý automat tvoriť len jeden cyklus. Rovnako môžeme mať len cyklus dĺžky jedna. Vtedy ak je stav v cykle akceptačný, tak akceptuje všetky slová dlhšie ako μ, naopak ak nie je akceptačný, tak akceptuje len konečný jazyk, v ktorom sú všetky slová kratšie ako μ.

Keď sa pozrieme na to, aké slová akceptuje UDFA A veľkosti (λ, μ), vo všeobecnosti môžeme povedať, že akceptačnými stavmi v cykle akceptuje slová nejakého konkrétneho tvaru, keďže sa vždy po prečítaní λ symbolov vráti do rovnakého stavu. Akceptačnými stavmi v chvoste akceptuje konečne veľa krátkych slov, ktoré nemusia spĺňať žiadny konkrény tvar, prípadne neakceptuje slová, ktoré spĺňajú potrebný tvar na akceptáciu podľa cyklu, ale sú príliš krátke. Krátkymi slovami myslíme slová kratšie než μ.

Značenie 1. Ďalej budeme za UDFA A_k veľkosti (λ, μ) uvažovať automat tvaru $A_k = (Q_k, \{a\}, \delta_k, q_k[0], F_k)$, kde $Q_k = \{q_k[i] \mid i \in \mathbb{Z}_{\mu+\lambda}\}$ a $\delta_k(q_k[i], a) = q_k[i+1]$ pre $i < \mu$, $\delta_k(q_k[i+\mu], a) = q_k[(i+1 \ mod \ \lambda) + \mu]$ pre každé $i \in \mathbb{Z}_\lambda$. Pre UDFA A analogický tvar, len bez dolného indexu k.



Obr. 1.1: UDFA A veľkosti (λ, μ)

Definícia 4 ([5])**.** Nech L je unárny regulárny jazyk, $\lambda \in \mathbb{N}$. Hovoríme, že L je λ-*cyklický* ak existuje UDFA A veľkosti $(\lambda, 0)$ taký, že $L(A) = L$. L nazývame *prísne* λ-*cyklický* ak je λ-cyklický a neexistuje $\lambda' < \lambda$ také, že L je λ'-cyklický. Hovoríme, že L je *v závere* λ-*cyklický* ak pre nejaké $\mu \in \mathbb{N}$ existuje UDFA A veľkosti (λ, μ) taký, že $L(A) = L$. L nazývame *prísne v závere* λ-*cyklický* ak je v závere λ-cyklický a neexistuje $\lambda' < \lambda$ také, že L je v závere λ'-cyklický.

Keďže sa pri skúmaní rozkladu jazyka L pozeráme na minimálny automat akceptujúci tento jazyk, potrebujeme charakterizovať minimálne UDFA pre daný jazyk L. Teda UDFA A také, že $L(A) = L$ a zároveň neexistuje UDFA A' také, že $L(A') = L$ a súčastne $sc(A') < sc(A)$. Keď je A veľkosti (λ, μ) a A' veľkosti (λ', μ'), tak chceme aby platilo $\lambda + \mu \leq \lambda' + \mu'$. Teda požadujeme, aby mal automat A minimálnu veľkosť cyklu a chvosta. Čo znamená, že nevieme nahradiť cyklus kratším tak, aby automat A akceptoval práve slová rovnakého tvaru ak sú dlhšie ako μ. V prípade chvosta to znamená, že nevieme časť chvosta takpovediac namotať na cyklus, teda, že z dvojice posledný stav chvosta a posledný stav cyklu je práve jeden akceptačný, inak by sme ich vedeli zlúčiť.

Veta 4 (Charakterizácia minimálneho UDFA [6]). *UDFA $A = (Q, \{a\}, \delta, q[0], F)$ veľkosti (λ, μ) je minimálny automat akceptujúci jazyk L práve vtedy keď platia nasledujúce podmienky:*

(i) Pre ľubovoľné $d \in \mathbb{N}$ také, že $d/\lambda \wedge d < \lambda$ existuje $h \in \mathbb{Z}_\lambda$ také, že $q[h+\mu] \in F$ práve vtedy, keď $q[((h+d) \ mod \ \lambda) + \mu] \notin F$, respektíve $a^{h+\mu} \in L$ práve vtedy, keď $a^{h+d+\mu} \notin L$.

(ii) Ak $\mu > 0$ potom $q[\mu - 1] \in F$ práve vtedy, keď $q[\lambda - 1 + \mu] \notin F$, respektíve $a^{\mu-1} \in L$ práve vtedy, keď $a^{\lambda-1+\mu} \notin L$.

Na základe toho je ľahké nahliadnuť, že pre prísne λ-cyklický jazyk L je minimálny UDFA akceptujúci A veľkosti $(\lambda, 0)$. Obdobne pre prísne v závere λ-cyklický jazyk L je minimálny UDFA akceptujúci A veľkosti (λ, μ), kde μ je minimálne, teda chvost sa už nedá viac namotať.

Teraz uvedieme dve ľahké tvrdenia, ktoré budeme potrebovať v dôkazoch mnohých ďalších tvrdení o existencii jazykov s nejakými vlastnosťami.

Tvrdenie 3. *Nech $L = \{a^{\alpha k} \mid k \in \mathbb{N}\}$ pre nejaké fixné $\alpha \in \mathbb{N}$. Potom L je prísne λ-cyklický jazyk pre $\lambda = \alpha$ a minimálny automat akceptujúci L je UDFA veľkosti $(\alpha, 0)$, kde $F = \{q[0]\}$.*

Dôkaz. Nech $L = \{a^{\alpha k} \mid k \in \mathbb{N}\}$ pre nejaké fixné $\alpha \in \mathbb{N}$. Nech A je UDFA veľkosti $(\alpha, 0)$ štandardného tvaru (Značenie 1), kde $F = \{q[0]\}$. Najprv ukážeme, že platí $L(A) = A$.

Poďme dokázať, že $L \subseteq L(A)$. Nech w leží v L, teda w je tvaru $a^{\alpha k}$ pre nejaké k z $\mathbb{N}$. Výpočet A na w bude tvaru $(w, q[0]) \vdash_A^* (\varepsilon, q[\alpha k \ mod \ \alpha])$. Keďže platí kongruencia $\alpha k \equiv 0 \ (mod \ \alpha)$, tak výpočet A na w končí v stave $q[0]$, čo je akceptačný stav v A. Teda w leží v jazyku $L(A)$.

Teraz poďme dokázať druhú inklúziu, teda že platí aj $L(A) \subseteq L$. Nech w leží v $L(A)$. Vieme, že w je tvaru a^m pre nejaké m z $\mathbb{N}$. Keďže $q[0]$ je jediný akceptačný stav v A, tak výpočet A na w končí práve v stave $q[0]$. Potom platí, že $m \equiv 0 \ (mod \ \alpha)$. Platí teda $m - 0 = \alpha l$ pre nejaké l z $\mathbb{N}$. Z toho dostávame, že w je tvaru $a^{\alpha l}$ pre l z $\mathbb{N}$. Čiže w leží v L.

Tým sme dokázali, že $L(A) = L$. Teraz ukážeme, že A je minimálny automat akceptujúci L pomocou charakterizácie minimálneho UDFA (4). Aby bol A minimálny, musí platiť, že pre ľubovoľné d z $\mathbb{N}$ také, že d/α a $d < \alpha$ existuje h zo $\mathbb{Z}_\alpha$ také, že

$q[h] \in F$ práve vtedy, keď $q[h + d \ mod \ \alpha] \notin F$. Ak zoberieme $h = 0$, tak $q[0] \in F$ a $q[d \ mod \ \alpha] \notin F$ pre každé d spĺňajúce dané podmienky. Teda pre každé d spĺňajúce dané podmienky existuje h, konkrétne 0, pre ktoré je tvrdenie pravdivé. Zároveň vieme, že A má nulovú dĺžku chvosta. Podľa charakterizácie minimálneho UDFA (4) potom A je minimálny automat akceptujúci jazyk L.

Keďže jazyk L je akceptovaný automatom A veľkosti $(\alpha, 0)$, tak L je λ-cyklický jazyk pre $\lambda = \alpha$. Nech UDFA B veľkosti $(\beta, 0)$ kde $\beta < \alpha$ akceptuje L. Platí $sc(B) < sc(A)$ a A je minimálny automat akceptujúci L. Teda takéto UDFA B nemôže existovať, a teda neexistuje $\lambda' < \alpha$ také, že L je λ'-cyklický jazyk. Potom L je prísne λ-cyklický jazyk pre $\lambda = \alpha$. □

Tvrdenie 4. *Nech* $L = \{a^{\alpha k} \mid k \in \mathbb{N}\}$ *pre nejaké fixné* $\alpha \in \mathbb{N}$. *Nech* $A_1, \ldots, A_n$ *sú UDFA veľkostí* $(\lambda_1, 0), \ldots, (\lambda_n, 0)$, *kde* $F_i = \{q_i[0]\}$ *pre každé* $i \in \{1, \ldots, n\}$. *Nech* $lcm(\lambda_1, \ldots, \lambda_n) = \alpha$. *Potom* $\bigcap_{i=1}^{n} L(A_i) = L$.

Dôkaz. Nech $L = \{a^{\alpha k} \mid k \in \mathbb{N}\}$ pre nejaké fixné α z $\mathbb{N}$. Označme množinu $I = \{1, \ldots, n\}$. Nech $A_1, \ldots, A_n$ sú UDFA veľkostí $(\lambda_1, 0), \ldots, (\lambda_n, 0)$ štandardného tvaru (Značenie 1), kde $F_i = \{q_i[0]\}$ pre každé i z I. Nech $lcm(\lambda_1, \ldots, \lambda_n) = \alpha$. Teraz postupne pomocou dvoch inklúzii ukážeme, že $\bigcap_{i=1}^{n} L(A_i) = L$.

Najprv dokážeme, že $L \subseteq \bigcap_{i=1}^{n} L(A_i)$. Nech w leží v L, teda w je tvaru $a^{\alpha k}$ pre nejaké k z $\mathbb{N}$. Pre každé i z I výpočet A_i na w bude tvaru $(w, q_i[0]) \vdash_{A_i}^{*} (\varepsilon, q_i[\alpha k \ mod \ \lambda_i])$. Nech platí kongruencia $\alpha k \equiv x_i \ (mod \ \lambda_i)$ ked $x_i < \lambda_i$. Potom výpočet A_i na w končí v stave $q_i[x_i]$. Keďže platí $lcm(\lambda_1, \ldots, \lambda_n) = \alpha$ tak pre každé i z I platí, že λ_i / α, teda $\alpha = \lambda_i \beta_i$ kde β_i leží v $\mathbb{N}$. Potom teda platí $\lambda_i \beta_i k \equiv x_i \ (mod \ \lambda_i)$. Keďže $x_i < \lambda_i$ tak musí platiť $x_i = 0$. Teda výpočet A_i na w končí v stave $q_i[0]$, čo je akceptačný stav v A_i. Potom w leží v jazyku $L(A_i)$ a to platí pre každé i z I. Teda w leží aj v ich prieniku $\bigcap_{i=1}^{n} L(A_i)$.

Teraz dokážeme druhú inklúziu, teda že platí aj $\bigcap_{i=1}^{n} L(A_i) \subseteq L$. Nech w leží v $\bigcap_{i=1}^{n} L(A_i)$, teda w leží v $L(A_i)$ pre každé i z I. Vieme, že w je tvaru a^m pre nejaké m z $\mathbb{N}$. Keďže $q_i[0]$ je jediný akceptačný stav v A_i, tak výpočet A_i na w končí práve v stave $q_i[0]$, čo platí pre každé i z I. Potom nasledujúca kongruencia $m \equiv 0 \ (mod \ \lambda_i)$ platí pre každé i z I. Majme systém n kongruncii $x \equiv 0 \ (mod \ \lambda_i)$ pre i z I. Určite existuje riešenie tohto systému kongruencii, napríklad práve m. Podľa CRT (1) sú všetky riešenia tohto systému kongruencii navzájom kongruentné modulo $lcm(\lambda_1, \ldots, \lambda_n)$. Zjavne ďalším riešením tohto systému kongruencii je 0. Dostávame teda $m \equiv 0 \ (mod \ lcm(\lambda_1, \ldots, \lambda_n))$. Platí teda $m - 0 = lcm(\lambda_1, \ldots, \lambda_n)l$ pre nejaké l z $\mathbb{N}$. Z toho dostávame $m = \alpha l$ a teda w je tvaru $a^{\alpha l}$ pre l z $\mathbb{N}$. Čiže w leží v L.

Spojením dvoch dokázaných inklúzii dostávame, že platí $L = \bigcap_{i=1}^{n} L(A_i)$. □

Platnosť predchádzajúcich dvoch tvrdení (3)(4) budeme ďalej v texte implicitne predpokladať bez toho, aby sme sa na ne priamo odkazovali.

1.5 Rozklad lambda cyklických jazykov

Na charakterizáciu 2-rozložiteľných λ-cyklických jazykov využívame *graf indukovaný jazykom* a zovšeobecnenie čínskej zvyškovej vety (1).

Definícia 5 ([5])**.** Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$, nech $\lambda_1, \lambda_2 \in \mathbb{N}$. Graf indukovaný L, λ_1, λ_2 je bipartitný graf $G = (V, E)$, kde
$V = V_1 \cup V_2$, kde pre každé $i \in \{1, 2\}$ $V_i = \{[r, i] \mid r \in \mathbb{Z}_{\lambda_i}\}$
$E = \{([r, i], [p, j]) \in V \times V \mid i \neq j,\ (\exists m \in \mathbb{N})\ m \equiv r\ (mod\ \lambda_i)\ \wedge\ m \equiv p\ (mod\ \lambda_j)\ \wedge\ a^m \in L\}$

Intuitívne, vrcholy grafu sú rozdelené do dvoch množín, respektíve zafarbené dvomi farbami, pričom vrcholy farby i prislúchajú prvkom z $\mathbb{Z}_{\lambda_i}$. Každému slovu $w = a^m$ z L prislúcha v grafe G hrana, pričom koncové vrcholy tejto hrany prislúchajú prvkom kongruentným s m modulo príslušné λ_i.

Definícia 6 ([5])**.** Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$, nech $\lambda_1, \lambda_2 \in \mathbb{N}$. Nech G je graf indukovaný L, λ_1, λ_2. Nech pre všetky $i \in \{1, 2\}$ $V_i' = \{r \mid r \in V_i,\ d_G(r) > 0\}$, teda V_i' vznikne z V_i odstránením všetkých vrcholov nulového stupňa. Hovoríme, že graf G rozkladá L práve vtedy, keď pre všetky dvojice $([r, 1], [p, 2]) \in V_1' \times V_2'$ platí, že ak existuje $m \in \mathbb{N}$ také, že $m \equiv r\ (mod\ \lambda_1) \wedge m \equiv p\ (mod\ \lambda_2)$, tak G obsahuje hranu $([r, 1], [p, 2])$.

Intuitívne graf G indukovaný L, λ_1, λ_2 rozkladá L, ak po zanedbaní všetkých vrcholov nulového stupňa v G platí, že pre každé dva vrcholy rôznej farby neexistuje m kongruentné s prvkami prislúchajúcimi daným vrcholom alebo dané vrcholy spája hrana, a teda pre nejaké m, ktoré spĺňa danú kongruenciu, a^m patrí do jazyka L.

Poznámka 6. Oproti pôvodnému článku [5] sme definíciu indukovaného grafu rozkladajúceho jazyk L rozdelili na dve a ľahkou úpravou odstránili niektoré formálne nedostatky.

Ak by sme chceli rozkladať minimálny UDFA A akceptujúci nejaký prísne λ-cyklický jazyk L, tak zvolíme $\lambda_1, \lambda_2 < \lambda$ tak, aby $lcm(\lambda_1, \lambda_2) = \lambda$ a zostrojíme graf G indukovaný L, λ_1, λ_2. Vrcholy jednej farby by prislúchali stavom jedného z nových automatov a vrcholy nenulového stupňa jeho akceptačným stavom. Zároveň keďže $lcm(\lambda_1, \lambda_2) = \lambda$, tak výpočty nových automatov na slovách $a^{k\lambda+n}$ kde k je z $\mathbb{N}$ a $n < \lambda$ skončia všetky v rovnakých stavoch, obdobne ako tomu je aj pri výpočtoch automatu A. Čiže sa nám stačí pozerať len či nové automaty akceptujú dobré slová kratšie ako λ. Iba také slová budeme uvažovať v nasledujúcich úvahách.

Ak slovo $w = a^m$ leží v jazyku L, tak medzi vrcholmi kongruentnými s m modulo príslušné λ_i je hrana. Práve v stavoch prislúchajúcich týmto vrcholom by skončili výpočty nových automatov na w a keďže tieto vrcholy sú nenulového stupňa, tak tieto stavy sú akceptačné, a teda slovo w by oba nové automaty akceptovali.

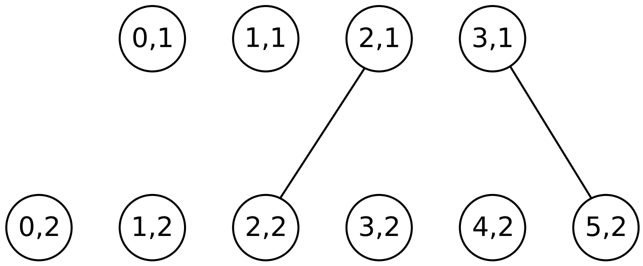
Ak slovo $w = a^m$ leží v prieniku jazykov akceptovaných takto zostrojenými novými automatmi, ich výpočty na w skončia v stavoch, ktoré prislúchajú prvkom zo $\mathbb{Z}_{\lambda_i}$ kongruentným s m modulo príslušné λ_i a tie musia byť akceptačné. Keďže graf G rozkladá L, tak medzi vrcholmi prislúchajúcimi týmto stavom leží hrana, ktorá bola do grafu pri jeho konštrukcii pridaná na základe toho, že nejaké slovo tvaru $u = a^n$, kde n je kongruentné s danými vrcholmi modulo príslušné λ_i leží v jazyku L. Podľa CRT (1) potom m a n sú navzájom kongruentné modulo λ, keďže sú riešeniami rovnakého systému kongruencii, a teda výpočty automatu A na týchto slovách skončia v rovnakých stavoch. Potom $w = a^m$ tiež patrí do jazyka L.

Takto zostrojené automaty teda budú akceptovať jazyky, ktorých prienik sa rovná L. Potom tvoria 2-rozklad automatu A. Existencia indukovaného grafu G, ktorý rozkladá L je teda postačujúcou podmienkou pre 2-rozložiteľnosť prísne λ-cyklického jazyka L. Ukázalo sa, že je aj nutnou a z toho dostávame charakterizáciu 2-rozložiteľných prísne λ-cyklických jazykov.

Veta 5 ([5]). *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. L je deterministicky 2-rozložiteľný práve vtedy, keď existuje $\lambda_1, \lambda_2 \in \mathbb{N}$ také, že $\lambda_1, \lambda_2 < \lambda$, $lcm(\lambda_1, \lambda_2) = \lambda$ a graf G indukovaný L, λ_1, λ_2 rozkladá L.*

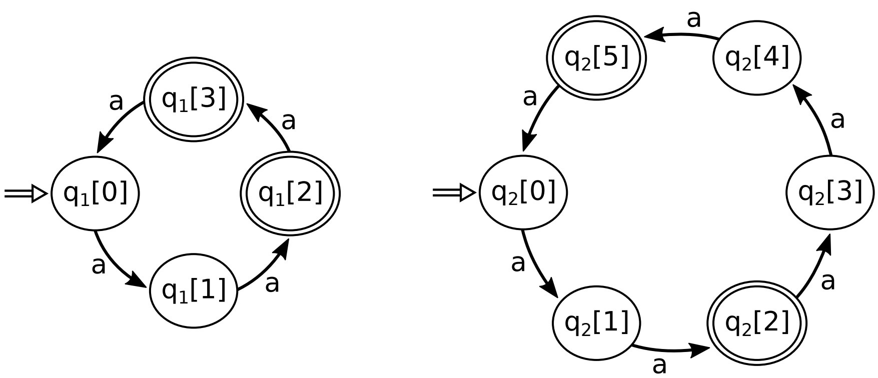
Uveďme si ilustračný príklad pre lepšie pochopenie charakterizácie 2-rozložiteľnosti.

Príklad 1. Zoberme jazyk $L = \{a^{12k+2}, a^{12k+11} \mid k \in \mathbb{N}\}$. Dá sa ukázať, že minimálny automat akceptujúci tento jazyk je UDFA A veľkosti $(12, 0)$, teda L je prísne λ-cyklický jazyk pre $\lambda = 12$. Zvolme $\lambda_1 = 4$, $\lambda_2 = 6$. Zostrojme graf G indukovaný L, λ_1, λ_2 (Obrázok 1.2). Aby graf G rozkladal L, tak pre každú dvojicu vrcholov nenulového stupňa rôznej farby buď neexistuje m z $\mathbb{N}$ kongruentné s príslušnými vrcholmi modulo príslušné λ_i alebo ich spája v grafe G hrana. Dvojice $[2, 1], [2, 2]$ a $[3, 1], [5, 2]$ spája v grafe G hrana. Pre dvojicu $[2, 1], [5, 2]$ nesmie existovať riešenie systému kongruencii $x \equiv 2 \ (mod\ 4)$, $x \equiv 5 \ (mod\ 6)$, aby graf G rozkladal L. Podľa CRT (1) má daný systém kongruencii riešenie ak $2 \equiv 5 \ (mod\ gcd(4, 6))$, teda ak $2 \equiv 5 \ (mod\ 2)$. Čo neplatí, keďže 2 je párne a 5 je nepárne číslo. Rovnako pre dvojicu $[3, 1], [2, 2]$ nesmie existovať riešenie systému kongruencii $x \equiv 3 \ (mod\ 4)$, $x \equiv 2 \ (mod\ 6)$, aby graf G rozkladal L. Podľa CRT (1) má daný systém kongruencii riešenie ak $3 \equiv 2 \ (mod\ gcd(4, 6))$, teda ak $3 \equiv 2 \ (mod\ 2)$. Čo opäť neplatí, keďže 2 je párne a 3 je nepárne číslo. Iné dvojice vrcholov nenulového stupňa v grafe nemáme, a teda podmienka je splnená, čiže indukovaný graf G rozkladá L.



Obr. 1.2: Graf G indukovaný $L = \{a^{12k+2}, a^{12k+11} \mid k \in \mathbb{N}\}, \lambda_1, \lambda_2$, kde $\lambda_1 = 4$ a $\lambda_2 = 6$

Zároveň pre λ_1, λ_2 platí, že $lcm(\lambda_1, \lambda_2) = \lambda$ a $\lambda_1, \lambda_2 < \lambda$. Potom vieme podľa grafu G uvedeným spôsobom zostrojiť automaty A_1, A_2 (Obrázok 1.3) veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$, ktoré tvoria 2-rozklad automatu A. Keďže sme našli takýto 2-rozklad A, tak potom L je deterministicky 2-rozložiteľný.



Obr. 1.3: UDFA A_1, A_2 veľkostí $(4,0),(6,0)$ tvoriace rozklad minimálneho UDFA A akceptujúceho jazyk $L = \{a^{12k+2}, a^{12k+11} \mid k \in \mathbb{N}\}$

Kapitola 2

Kvalita rozkladov

V tejto kapitole formálne zadefinujeme kvalitu rozkladov vo všeobecnosti a budeme skúmať kvalitu 2-rozkladov λ-cyklických jazykov, kde budeme uvažovať súčet stavových zložitostí automatov rozkladu.

Vždy keď hovoríme o problémoch alebo výpočtových modeloch akými sú turingove stroje či v našom prípade konečné automaty, nás zaujíma zložitosť daného problému či modelu. Zaujíma nás výpočtová zložitosť, teda ako dlho bude daný výpočet trvať alebo koľko pamäte naň použijeme, ale rovnako nás zaujíma aj popisná zložitosť daného výpočtového modelu ako počet stavov automatu. My zložitosť deterministického konečného automatu A meriame práve formou stavovej zložitosti $sc(A)$. Rovnako zložitosť problému, teda jazyka L, meriame stavovou zložitosťou minimálneho automatu akceptujúceho tento jazyk.

Pri rozklade automatu A na nové automaty A_1, A_2 vyžadujeme aby stavová zložitosť oboch nových automatov bola menšia ako zložitosť pôvodného, teda aby platilo $sc(A_1) < sc(A)$ a taktiež $sc(A_2) < sc(A)$. Ľahko si však môžeme všimnúť, že pre mnohé automaty existuje veľa rôznych dvojíc automatov A_1, A_2 takých, že tvoria rozklad pôvodného automatu. A hoci všetky spĺňajú podmienku $sc(A_1) < sc(A)$ a $sc(A_2) < sc(A)$, je prirodzené očakávať, že nie všetky tieto rozklady budú z pohľadu zložitosti nových automatov rovnako dobré. Tak vyvstáva prirodzená potreba nejako merať a následne porovnávať kvalitu jednotlivých rozkladov. Keďže zložitosť pôvodného automatu A meriame jeho stavovou zložitosťou $sc(A)$, Môžeme využiť rovnaký prístup a merať kvalitu rozkladu pomocou funkcie závislej od stavových zložitostí nových automatov $sc(A_1)$ a $sc(A_2)$.

Prístup, ktorý uplatníme, je brať ako kvalitu rozkladu súčet stavových zložitostí dvoch nových automatov A_1, A_2, teda $sc(A_1) + sc(A_2)$. Takto berieme do úvahy celú stavovú zložitosť rozkladu. Počet stavov nových automatov sa nám síce znížil oproti pôvodnému, ale zase sme pridali jeden nový automat. Takto zahrnieme aj tento nárast zložitosti spôsobenej vzniknutým paralelizmom.

Značenie 2. Označme $\mathcal{D} = \{[A_1, \dots, A_n] \mid (\forall i \in \{1, \dots, n\})\ A_i\ je\ DFA;\ A_1, \dots, A_n$ $tvoria\ n{-}rozklad\ nejak\acute{e}ho\ DFA\ A;\ n \geq 2\}$ množinu všetkých n-rozkladov všetkých DFA A, kde $n \geq 2$.

Intuitívne prvky množiny $\mathcal{D}$ sú n-tice automatov také, že tvoria n-rozklad nejakého DFA A.

Definícia 7. Nech $\mathcal{D}$ je množina všetkých n-rozkladov všetkých DFA A, kde $n \geq 2$. Potom funkciu $f : \mathcal{D} \to \mathbb{N}$, pre ktorú platí, že $f([A_1, \dots, A_n]) = f([A_{\varphi(1)}, \dots, A_{\varphi(n)}])$ pre každú $[A_1, \dots, A_n] \in \mathcal{D}$ a pre každú permutáciu φ prvkov množiny $\{1, \dots, n\}$, nazývame *f-kvalita rozkladu*.

Poznámka 7. Ak n-tica automatov $[A_1, \dots, A_n]$ tvorí rozklad nejakého DFA A tak aj n-tica $[A_{\varphi(1)}, \dots, A_{\varphi(n)}]$ tvorí rozklad toho istého automatu A pre ľubovoľnú permutáciu φ prvkov množiny $\{1, \dots, n\}$. Potom teda všetky takéto n-tice (pre každú permutáciu) ležia v množine $\mathcal{D}$, a teda podmienka v definícii je korektne zadefinovaná. Zároveň ide o preusporiadanie tých istých automatov a teda vlastne o ten istý rozklad, čiže je pochopiteľné, aby sme vyžadovali, že musí mať rovnakú kvalitu.

Poznámka 8. Všimnime si, že sme f-kvalitu rozkladu definovali všeobecne pre ľubovoľné rozklady, nie len pre 2-rozklady, čo nám umožní použiť túto definíciu aj v budúcnosti pri skúmaní kvality rozkladu na viac ako dva nové automaty.

V našom prípade pri skúmaní f-kvality rozkladov budeme ako f používať funkciu *sum*, ktorá vracia súčet stavových zložitostí automatov daného rozkladu. Ale akúkoľvek zmysluplnú funkciu, ktorá rozumným spôsobom skombinuje nejakú rozumnú mieru zložitosti jednotlivých automatov rozkladu, môžeme zobrať za kvalitu rozkladu. Ďalšie možnosti, ktoré sa prirodzene ponúkajú je zobrať funkcie *max* alebo *mult*, ktoré by vraátili maximum respektíve súčin stavových zložitostí automatov rozkladu.

Aj keď to nevyžadujeme, môžeme rozumne očakávať, že funkcia f na lepšom rozklade vráti nižšiu hodnotu. Toto očakávanie je v súlade s nami používanou funkciou *sum*, ale aj navrhnutými funkciami *max* a *mult* pre stavové zložitosti jednotlivých automatov rozkladu. Teraz si môžeme funkciu *sum* formálne zadefinovať.

Definícia 8. Nech $D = [A_1, \dots, A_n]$, $D \in \mathcal{D}$ je n-rozklad nejakého DFA A. Funkciu $sum : \mathcal{D} \to \mathbb{N}$, definovanú ako

$$sum(D) = \sum_{i=1}^{n} sc(A_n)$$

nazývame *sum*-kvalita rozkladu.

2.1 Efektívne 2-rozklady λ-cyklických jazykov

Poďme sa pozrieť na kvalitu 2-rozkladov pre prísne λ-cyklické jazyky. Ako sme už spomenuli, pre daný regulárny 2-rozložiteľný jazyk L nad unárnou abecedou často existuje veľa rôznych rozkladov jeho minimálneho automatu A. Keď sa pozrieme na dva rôzne 2-rozklady $[A_1, A_2]$ a $[B_1, B_2]$ automatu A, automaty oboch rozkladov môžu akceptovať rovnaké jazyky, prípadne jedny z daných jazykov môžu byť rovnaké a druhé rôzne alebo aj oba jazyky môžu byť v daných dvoch rozkladoch rozdielne. Často sa stretneme aj s rozkladmi, ktoré sú vlastne pokazením iných rozkladov. Pokazením myslíme napríklad pridanie zbytočných akceptačných stavov tak, že novo akceptované slová sa nedostanú do prieniku dvoch nových jazykov. Ďalším pokazením môže byť napríklad zobratie väčších, v zmysle stavovej zložitosti, automatov akceptujúcich rovnaké jazyky. V oboch týchto prípadoch sme sa ale k daným pokazeným rozkladom dostali zobratím a následným upravením nejakého pekného rozkladu. Ukážeme, že keď máme 2-rozložiteľný prísne λ-cyklický jazyk L, tak pre každý 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A existuje jeho iný 2-rozklad $[B_1, B_2]$, ktorý je v istom zmysle pekný a pôvodný rozklad vznikol práve jeho pokazením jedným so spomenutých spôsobov. Alternatívne sa na to môžeme pozerať tak, že vieme každý 2-rozklad A upraviť na nejaký iný, v istom zmysle pekný 2-rozklad, ktorý bude aspoň tak dobrý ako pôvodný pri všetkých rozumných funkciami na meranie kvality rozkladu. Ešte predtým ako formálne sformulujeme a dokážeme toto tvrdenie o možnosti zlepšovania 2-rozkladov uveďme niekoľko tvrdení, ktoré použijeme v dôkaze.

Veta 6 ([6])**.** *Nech L_1 a L_2 sú dva unárne jazyky. Nech UDFA A_1 a A_2 veľkostí (λ_1, μ_1) respektíve (λ_2, μ_2) sú automaty akceptujúce jazyky L_1 respektíve L_2. Potom vieme zostrojiť UDFA A veľkosti $(lcm(\lambda_1, \lambda_2), max\{\mu_1, \mu_2\})$, ktorý akceptuje prienik jazykov L_1 a L_2.*

Lema 1 ([5])**.** *Nech L je 2-rozložiteľný prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Nech UDFA A je minimálny automat akceptujúci L. Nech UDFA A_1 veľkosti (λ_1, μ_1) a A_2 veľkosti (λ_2, μ_2) tvoria 2-rozklad A. Navyše nech A_1 a A_2 sú minimálne UDFA akceptujúce príslušné jazyky. Potom λ_1/λ a λ_2/λ.*

Lema 2 ([5])**.** *Nech L je 2-rozložiteľný prísne v závere λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Nech UDFA A veľkosti (λ, μ) je minimálny automat akceptujúci L. Nech UDFA A_1 veľkosti (λ_1, μ_1) a A_2 veľkosti (λ_2, μ_2) tvoria 2-rozklad A. Navyše nech A_1 a A_2 sú minimálne UDFA akceptujúce príslušné jazyky. Ak $\mu_1 \geq \mu$, tak existuje 2-rozklad $[A'_1, A_2]$ automatu A, kde A'_1 je UDFA veľkosti (λ_1, μ). Obdobne ak $\mu_2 \geq \mu$, tak existuje 2-rozklad $[A_1, A'_2]$ automatu A, kde A'_2 je UDFA veľkosti (λ_2, μ).*

Lema 3 (Odrolovacia Lema [5])**.** *Nech $A = (Q, \{a\}, \delta, q[0], F)$ je UDFA veľkosti (λ, μ). Potom pre ľubovoľné $\mu' \geq \mu$ a UDFA $A' = (Q', \{a\}, \delta', q'[0], F')$ veľkosti (λ, μ'),* *kde množina akceptačných stavov je definovaná nasledovne*

$$F' = \{q'[f] \in Q' \mid (\exists w \in L(A))\ (q'[0], w) \vdash^*_{A'} (q'[f], \varepsilon)\}$$

platí, že $L(A') = L(A)$.

Lema 4. *Nech L je unárny jazyk. Nech UDFA A_1 veľkosti (λ_1, μ_1) pre nejaké $\lambda_1, \mu_1 \in \mathbb{N}$ je minimálny automat akceptujúci L. Nech UDFA A_2 veľkosti (λ_2, μ_2) pre nejaké $\lambda_2, \mu_2 \in \mathbb{N}$ je iný automat akceptujúci L. Potom platí λ_1 / λ_2.*

Dôkaz. Nech L je unárny jazyk. Nech UDFA A'_1 štandardného tvaru (Značenie 1) veľkosti (λ_1, μ_1) pre nejaké λ_1, μ_1 z $\mathbb{N}$ je minimálny automat akceptujúci L. Nech UDFA A_2 štandardného tvaru (Značenie 1) veľkosti (λ_2, μ_2) pre nejaké λ_2, μ_2 z $\mathbb{N}$ je iný automat akceptujúci L. Na základe charakterizácie minimálneho UDFA (4) je ľahké nahliadnuť, že $\lambda_1 \leq \lambda_2$ a $\mu_1 \leq \mu_2$. Ak platí $\lambda_1 = \lambda_2$, tak je tvrdenie splnené.

Teraz predpokladajme, že $\lambda_1 < \lambda_2$. S využitím odrolovacej lemy 3 zostrojme UDFA A_1 štandardného tvaru (Značenie 1) veľkosti (λ_1, μ_2), ktorý akceptuje jazyk L. Ak sú všetky stavy v cykle automatu A_1 akceptačné, tak keďže A'_1, ktorý je minimálny UDFA akceptujúci L má rovnaký cyklus (iba sa do neho príde v inom stave), tak platí, že $\lambda_1 = 1$. Potom je tvrdenie triviálne splnené. Obdobná situácia nastáva ak sú všetky stavy v cykle A_1 neakceptačné. Preto môžeme predpokladať, že v cykle automatu A_1 existuje akceptačný stav $q_1[m + \mu_2]$ pre nejaké m zo $\mathbb{Z}_{\lambda_1}$ a tiež neakceptačný stav $q_1[n + \mu_2]$ pre nejaké n zo $\mathbb{Z}_{\lambda_1}$.

Sporom predpokladajme, že λ_1 nedelí λ_2. Výpočet A_1 na slove $w = a^{m+\mu_2}$ končí v stave $q_1[m + \mu_2]$. Ten je akceptačný v A_1, a teda slovo w patrí do L. Výpočet A_2 na slove w končí v stave $q_2[(m\ mod\ \lambda_2) + \mu_2]$. Keďže $m < \lambda_1 < \lambda_2$, tak končí v stave $q_2[m+\mu_2]$. A_2 akceptuje jazyk L a slovo $w = a^{m+\mu_2}$ patrí do L, a teda stav $q_2[m+\mu_2]$ je akceptačný v A_2. Výpočet A_1 na slove $v = a^{n+\mu_2}$ končí v stave $q_1[n + \mu_2]$. Ten je neakceptačný v A_1, a teda slovo v nepatrí do L. Výpočet A_2 na slove v končí v stave $q_2[(n\ mod\ \lambda_2) + \mu_2]$. Keďže $n < \lambda_1 < \lambda_2$, tak končí v stave $q_2[n + \mu_2]$. A_2 akceptuje jazyk L a slovo $v = a^{n+\mu_2}$ nepatrí do L, a teda stav $q_2[n + \mu_2]$ nemôže byť akceptačný v A_2. Teda aj v cykle automatu A_2 existuje nejaký akceptačný a nejaký neakceptačný stav.

Majme systémy kongruencii $x \equiv m\ (mod\ \lambda_1)$ a $x \equiv n\ (mod\ \lambda_2)$ kde $q_1[m + \mu_2]$ je akceptačný stav v A_1 a $q_2[n + \mu_2]$ je neakceptačný stav v A_2. Ak existuje také m, n, že daný systém kongruencii má riešenie x, tak výpočet A_1 na slove $w = a^{x+\mu_2}$ skončí v stave $q_1[m + \mu_2]$, ktorý je akceptačný, teda w patrí do L. Zároveň výpočet A_2 na w skončí v stave $q_2[n + \mu_2]$, ktorý je neakceptačný, teda w nepatrí do L, čo je spor.

Daný systém kongruencii má podľa CRT (1) riešenie práve vtedy, keď $m \equiv n\ (mod\ gcd(\lambda_1, \lambda_2))$. Teda ak neexistujú také m, n, že daný systém kongruencii má riešenie, tak ak $m \equiv n\ (mod\ gcd(\lambda_1, \lambda_2))$, tak stavy $q_1[m + \mu_2]$ a $q_2[n + \mu_2]$ sú oba akceptačné alebo sú oba neakceptačné. Ak $gcd(\lambda_1, \lambda_2) = \lambda_1$, tak λ_1/λ_2 čo je spor.

Nech teda $gcd(\lambda_1, \lambda_2) < \lambda_1$, označme ho g. Nech $m \equiv n\ (mod\ g)$, kde $m < g$ potom stavy $q_1[m+\mu_2]$, $q_2[n+\mu_2]$ sú oba akceptačné alebo neakceptačné, bez ujmy na všeobecnosti nech sú akceptačné. Zároveň platí aj $m + g \equiv n\ (mod\ g)$, pričom keďže g/λ_1, $g < \lambda_1$ a $m < g$, tak $m + g < \lambda_1$. Potom stav $q_1[m + g + \mu_2]$ je tiež akceptačný v A_1. Zároveň platí, že $m \equiv m + g\ (mod\ g)$. Rozšírením tejto úvahy dostávame, že ak $x \equiv y\ (mod\ g)$, tak stavy $q_1[x+\mu_2]$ a $q_1[y+\mu_2]$ sú oba akceptačné alebo neakceptačné. Potom vieme cyklus v A_1 nahradiť cyklom dĺžky $g < \lambda_1$. Rovnakým cyklom (len do neho prídeme v inom stave) potom vieme nahradiť aj cyklus automatu A_1', čo je spor, lebo sme našli automat akceptujúci L menší než minimálny (Na túto situáciu sa môžeme pozerať aj tak, že časť chvosta, ktorú sme pri vytváraní A_1 odrolovali teraz naspäť narolujeme na cyklus). □

Teraz už môžeme sformulovať a dokázať vetu o zlepšovaní 2-rozkladov.

Veta 7 (Veta o zlepšovaní 2-rozkladov)**.** *Nech L je 2-rozložiteľný prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Nech UDFA A je minimálny automat akceptujúci L. Potom pre každý 2-rozklad $[A_1, B_1]$ automatu A, kde automaty A_1 a B_1 sú veľkostí (λ_{a1}, μ_{a1}) a (λ_{b1}, μ_{b1}) existuje 2-rozklad $[A_e, B_e]$ automatu A, kde automaty A_e a B_e sú veľkostí $(\lambda_{ae}, 0)$ a $(\lambda_{be}, 0)$ a navyše platí, že $lcm(\lambda_{ae}, \lambda_{be}) = \lambda$, $\lambda_{ae} = \lambda_{a1}/\alpha_a$ a $\lambda_{be} = \lambda_{b1}/\alpha_b$ pre nejaké $\alpha_a, \alpha_b \in \mathbb{N}$.*

Dôkaz. Nech L je 2-rozložiteľný prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech UDFA A je minimálny automat akceptujúci L, teda je veľkosti $(\lambda, 0)$. Nech $[A_1, B_1]$ je 2-rozklad automatu A, kde automaty A_1 a B_1 sú veľkostí (λ_{a1}, μ_{a1}) a (λ_{b1}, μ_{b1}). Postupne na viac krokov zostrojíme automaty A_e, B_e veľkostí (λ_{ae}, μ_{be}), (λ_{be}, μ_{be}), ktoré tvoria 2-rozklad A a spĺňajú požadované podmienky.

Označme $L_{a1} = L(A_1)$ a $L_{b1} = L(B_1)$. Nech UDFA A_2 veľkosti (λ_{a2}, μ_{a2}) je minimálny automat akceptujúci jazyk L_{a1} a UDFA B_2 veľkosti (λ_{b2}, μ_{b2}) minimálny automat akceptujúci jazyk L_{b1}. Zrejme platí, že $sc(A_2) \leq sc(A_1)$ a tiež $sc(B_2) \leq sc(B_1)$, teda automaty A_2, B_2 tiež tvoria 2-rozklad automatu A. Podľa Lemy 4 potom $\lambda_{a2}/\lambda_{a1}$ a taktiež $\lambda_{b2}/\lambda_{b1}$. Teda existuje β_{a1} z $\mathbb{N}$ taká, že $\lambda_{a1} = \beta_{a1}\lambda_{a2}$. Rovnako existuje β_{b1} z $\mathbb{N}$ taká, že $\lambda_{b1} = \beta_{b1}\lambda_{b2}$.

Keďže A_2 a B_2 sú minimálne automaty akceptujúce príslušné jazyky a navyše platí, že $\mu_{a2} \geq 0$ a tiež $\mu_{b2} \geq 0$, tak dvojnásobným aplikovaním Lemy 2 dostávame, že existujú automaty A_3, B_3 veľkostí $(\lambda_{a2}, 0)$ a $(\lambda_{b2}, 0)$, ktoré tvoria 2-rozklad automatu A. Označme $L_{a3} = L(A_3)$ a $L_{b3} = L(B_3)$. Keďže automaty A_3, B_3 majú nulové dĺžky chvostov, jazyky L_{a3} a L_{b3} sú prísne λ-cyklické pre nejaké $\lambda_{a3} \leq \lambda_{a2}$ respektíve $\lambda_{b3} \leq \lambda_{b2}$.

Potom minimálne automaty A_4, B_4 akceptujúce tieto jazyky sú veľkostí $(\lambda_{a3}, 0)$ respektíve $(\lambda_{b3}, 0)$. Zrejme platí, že $sc(A_4) \leq sc(A_3)$ a tiež $sc(B_4) \leq sc(B_3)$, teda automaty A_4, B_4 takisto tvoria 2-rozklad automatu A. Podľa Lemy 4 potom $\lambda_{a3}/\lambda_{a2}$ a taktiež $\lambda_{b3}/\lambda_{b2}$. Teda existuje β_{a2} z $\mathbb{N}$ taká, že $\lambda_{a2} = \beta_{a2}\lambda_{a3}$, z čoho dostávame, že $\lambda_{a1} = \beta_{a1}\beta_{a2}\lambda_{a3}$, teda $\lambda_{a3} = \lambda_{a1}/\beta_{a1}\beta_{a2}$. Rovnako existuje β_{b2} z $\mathbb{N}$ taká, že $\lambda_{b2} = \beta_{b2}\lambda_{b3}$, z čoho dostávame, že $\lambda_{b1} = \beta_{b1}\beta_{b2}\lambda_{b3}$, teda $\lambda_{b3} = \lambda_{b1}/\beta_{b1}\beta_{b2}$.

Teraz nám už len stačí dokázať, že $lcm(\lambda_{a3}, \lambda_{b3}) = \lambda$. Keďže automaty A_4 a B_4 tvoria rozklad automatu A a sú minimálne akceptujúce príslušné jazyky, tak z Lemy 1 dostávame, že λ_{a3}/λ a tiež λ_{b3}/λ. Potom $lcm(\lambda_{a3}, \lambda_{b3}) \leq \lambda$. Ak by platilo $lcm(\lambda_{a3}, \lambda_{b3}) < \lambda$, tak podľa Vety 6 existuje automat A' veľkosti $(lcm(\lambda_{a3}, \lambda_{b3}), 0)$ akceptujúci jazyk $L_{a3} \cap L_{b3}$, teda jazyk L. To by ale existoval automat akceptúci L menší než minimálny, čo nemôže nastať a preto $lcm(\lambda_{a3}, \lambda_{b3}) = \lambda$.

Za A_e teda zoberieme A_4, za B_e zoberieme B_4. Potom $\lambda_{ae} = \lambda_{a3}$, $\lambda_{be} = \lambda_{b3}$, $\mu_{ae} = 0$, $\mu_{be} = 0$ a platí, že $lcm(\lambda_{ae}, \lambda_{be}) = \lambda$, $\lambda_{ae} = \lambda_{a1}/\alpha_a$ a $\lambda_{be} = \lambda_{b1}/\alpha_b$ pre $\alpha_a = \beta_{a1}\beta_{a2}$ a $\alpha_b = \beta_{b1}\beta_{b2}$. Tým sme našli 2-rozklad automatu A s požadovanými vlastnosťami. $\square$

Veta o zlepšovaní 2-rozkladov (7) nám hovorí, že pre každý 2-rozklad $[A_1, A_2]$ minimálneho automatu A akceptujúceho jazyk L existuje iný 2-rozklad $[B_1, B_2]$ taký, že oba jeho automaty majú nulové chvosty, teda nanajvýš tak dlhé ako chvosty pôvodných automatov. Rovnako dĺžky ich cyklov delia dĺžky cyklov automatov pôvodného rozkladu, a teda sú nanajvýš tak dlhé a ich najmenší spoločný násobok je dĺžka cyklu pôvodného automatu. Potom $sc(B_1) \leq sc(A_1)$ a tiež $sc(B_2) \leq sc(A_2)$. A teda podľa každej zmysluplnej funkcie f musí f-kvalita rozkladu vypočítaná na základe stavovej zložitosti automatov rozkladu byť pre rozklad $[B_1, B_2]$ aspoň tak dobrá ako pre rozklad $[A_1, A_2]$. Je ľahké nahliadnuť, že to splňuje aj nami používaná funkcia *sum*.

Dostávame teda, že všetky 2-rozklady A sa dajú zlepšiť na 2-rozklady určitého tvaru. Potom, keď je naším cieľom zisťovať ako kvalitné 2-rozklady pre daný automat existujú, pričom chceme nájsť tie najlepšie, dáva zmyseľ pozerať sa práve na tieto 2-rozklady, ktoré nazveme *efektívne*.

Definícia 9. Nech A je UDFA veľkosti $(\lambda, 0)$ pre nejaké $\lambda \in \mathbb{N}$. Dvojicu UDFA $[A_1, A_2]$ kde automaty A_1, A_2 sú veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$ nazývame efektívny 2-rozklad UDFA A ak $L(A) = L(A_1) \cap L(A_2)$, $\lambda_1 < \lambda$, $\lambda_2 < \lambda$ a $lcm(\lambda_1, \lambda_2) = \lambda$. Ak takýto efektívny 2-rozklad UDFA A existuje, hovoríme, že A je efektívne 2-rozložiteľný.

Definícia 10. Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$, nech UDFA A je minimálny automat akceptujúci L. Hovoríme, že L je deterministicky efektívne 2-rozložiteľný ak UDFA A je efektívne 2-rozložiteľný.

Ak prísne λ-cyklický jazyk L je 2-rozložiteľný, tak existuje nejaký jeho 2-rozklad, ktorý sa dá podľa Vety o zlepšovaní 2-rozkladov (7) zlepšiť na jeho efektívny 2-rozklad. Ten je zároveň jeho rozkladom, takže je ľahké vidieť, že efektívna 2-rozložiteľnosť a 2-rozložiteľnosť sú pre prísne λ-cyklický jazyk L ekvivalentné. Len nie všetky jeho rozklady sú efektívne. Nás, pri skúmaní kvality jeho rozkladov, budú zaujímať práve tie efektívne, keďže medzi tými ostatnými sa vyskytujú zbytočne veľké automaty so zbytočnými stavmi, a teda pozerať sa na kvalitu takýchto rozkladov nie je zaujímavé.

2.2 Sum-kvalita 2-rozkladov

Teraz sa môžeme pozrieť na *sum*-kvalitu 2-rozkladov. Najprv ukážeme, že pre každý 2-rozklad existuje nejaký efektívny 2-rozklad, ktorý má aspoň tak dobrú *sum*-kvalitu ako mal pôvodný.

Veta 8. *Nech* $[A_1, A_2]$ *je 2-rozklad minimálneho UDFA A akceptujúceho nejaký prísne* λ*-cyklický jazyk L. Potom existuje efektívny 2-rozklad* $[B_1, B_2]$ *automatu A taký, že* $sum([B_1, B_2]) \leq sum([A_1, A_2])$.

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$, nech A je minimálny UDFA akceptujúci L. Nech $[A_1, A_2]$ je nejaký 2-rozklad automatu A, kde automaty A_1, A_2 sú veľkostí $(\lambda_{a1}, \mu_{a1}), (\lambda_{a2}, \mu_{a2})$. Potom podľa Vety o zlepšovaní 2-rozkladov (7) vieme, že existuje 2-rozklad $[B_1, B_2]$ automatu A, kde automaty B_1, B_2 sú veľkostí $(\lambda_{b1}, 0), (\lambda_{b2}, 0)$, pričom platí $\lambda_{b1} = \lambda_{a1}/\alpha_1$ a $\lambda_{b2} = \lambda_{a2}/\alpha_2$ pre nejaké α_1, α_2 z $\mathbb{N}$. Keďže $\alpha_1 \geq 1$ tak $\lambda_{b1} \leq \lambda_{a1}$. Ďalej zrejme $\mu_{a1} \geq 0$. Potom $\lambda_{b1} \leq \lambda_{a1} + \mu_{a1}$, teda $sc(B_1) \leq sc(A_1)$. Analogickou úvahou dostávame, že $sc(B_2) \leq sc(A_2)$, a teda $sc(B_1) + sc(B_2) \leq sc(A_1) + sc(A_2)$. Keďže $sum([B_1, B_2]) = sc(B_1) + sc(B_2)$ a tiež $sum([A_1, A_2]) = sc(A_1) + sc(A_2)$, tak potom $sum([B_1, B_2]) \leq sum([A_1, A_2])$. $\square$

Teraz sa nám stačí pozerať už len na efektívne 2-rozklady, lebo ako sme dokázali, každý 2-rozklad sa dá zlepšiť na nejaký efektívny, ktorý má lepšiu *sum*-kvalitu. Ukážeme aká je horná a dolná hranica *sum*-kvality týchto rozkladov a ako ďaleko sa od nej možu jednotlivé rozklady pohybovať.

Lema 5. *Nech* $[A_1, A_2]$ *je efektívny 2-rozklad minimálneho automatu A pre nejaký prísne* λ*-cyklický jazyk L pre nejaké* $\lambda \in \mathbb{N}$*. Potom* $\lceil 2\sqrt{\lambda} \rceil \leq sum([A_1, A_2])$.

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech A je minimálny automat akceptujúci L. Nech $[A_1, A_2]$ je efektívny 2-rozklad A. Potom automaty A_1, A_2 sú veľkostí $(\lambda_1, 0), (\lambda_2, 0)$ a platí, že $lcm(\lambda_1, \lambda_2) = \lambda$. Zároveň platí $\lambda_1 < \lambda$, $\lambda_2 < \lambda$ a tiež λ_1/λ respektíve λ_2/λ. Označme $x = \sqrt{\lambda}$ a $g = gcd(\lambda_1, \lambda_2)$. Vieme, že

$x^2 = lcm(\lambda_1, \lambda_2)$ a teraz ukážeme, že platí $2x \leq \lambda_1 + \lambda_2$. Dostávame teda

$$\begin{aligned} \lambda_1 + \lambda_2 &\geq 2x \\ \lambda_1 + \lambda_2 - 2x &\geq 0 \\ \lambda_1 + \lambda_2 - 2\sqrt{lcm(\lambda_1, \lambda_2)} &\geq 0 \\ \lambda_1 + \lambda_2 - 2\frac{\sqrt{\lambda_1 \lambda_2}}{\sqrt{g}} &\geq 0 \\ \frac{\lambda_1\sqrt{g} - 2\sqrt{\lambda_1\lambda_2} + \lambda_2\sqrt{g}}{\sqrt{g}} &\geq 0 \end{aligned}$$

Keďže $g \geq 1$, potom aj $\sqrt{g} \geq 1$ a teda musí platiť

$$\begin{aligned} \lambda_1\sqrt{g} - 2\sqrt{\lambda_1\lambda_2} + \lambda_2\sqrt{g} &\geq 0 \\ (\sqrt{\lambda_1}\sqrt[4]{g} - \sqrt{\lambda_2}\sqrt[4]{g})^2 + 2\sqrt{\lambda_1}\sqrt{\lambda_2}(\sqrt{g} - 1) &\geq 0 \end{aligned}$$

Zrejme platí, že $(\sqrt{\lambda_1}\sqrt[4]{g} - \sqrt{\lambda_2}\sqrt[4]{g})^2 \geq 0$ a tiež $2\sqrt{\lambda_1}\sqrt{\lambda_2} > 0$ lebo $\lambda_1 > 0$ aj $\lambda_2 > 0$, keďže $lcm(\lambda_1, \lambda_2) = \lambda > 0$. Ak teda navyše platí, že $(\sqrt{g} - 1) \geq 0$, tak $2\sqrt{\lambda_1}\sqrt{\lambda_2}(\sqrt{g} - 1) \geq 0$ a nerovnica je splnená. Ale $(\sqrt{g} - 1) \geq 0$ platí lebo ako sme nahliadli $\sqrt{g} \geq 1$.

Tým sme dokázali, že $2\sqrt{\lambda} \leq \lambda_1 + \lambda_2$. Potom platí aj, že $\lceil 2\sqrt{\lambda} \rceil \leq \lambda_1 + \lambda_2$. Zároveň vieme, že $sum([A_1, A_2]) = sc(A_1) + sc(A_2) = \lambda_1 + \lambda_2$. Z toho dostávame, že $\lceil 2\sqrt{\lambda} \rceil \leq sum([A_1, A_2])$. □

Poznámka 9. Navrhnime alternatívny spôsob na dokončenie dôkazu predchádzajúcej lemy (5). Keďže $\sqrt{g} \geq 1$ a $\sqrt{\lambda_1, \lambda_2} > 0$, tak potom platí, že $\frac{\sqrt{\lambda_1\lambda_2}}{\sqrt{g}} \leq \sqrt{\lambda_1\lambda_2}$. A teda pre ľubovoľné x platí $x - \frac{\sqrt{\lambda_1\lambda_2}}{\sqrt{g}} \geq x - \sqrt{\lambda_1\lambda_2}$. Potom ak si za x dosadíme $\lambda_1 + \lambda_2$ a odčítavaný výraz ešte prenásobíme 2, tak nám na dokázanie nerovnosti v dôkaze stačí dokázať, že

$$\lambda_1 + \lambda_2 - 2\sqrt{\lambda_1, \lambda_2} \geq 0$$

No a to priamo vyplýva z AM-GM nerovnosti (3). Ukázali sme teda alternatívny spôsob dôkazu Lemy 5. V pôvodnom dôkaze sme sa však nemusili odvolávať na platnosť žiadneho ďalšieho tvrdenia.

Lema 6. *Nech $[A_1, A_2]$ je efektívny 2-rozklad minimálneho automatu A pre nejaký prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$. Potom $sum([A_1, A_2]) \leq \frac{5}{6}\lambda$.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech A je minimálny automat akceptujúci L. Nech $[A_1, A_2]$ je efektívny 2-rozklad A. Potom automaty A_1, A_2 sú veľkostí $(\lambda_1, 0), (\lambda_2, 0)$ a platí, že $lcm(\lambda_1, \lambda_2) = \lambda$. Zároveň platí $\lambda_1 < \lambda$,

$\lambda_2 < \lambda$ a tiež λ_1/λ respektíve λ_2/λ. Teda $\lambda = \alpha\lambda_1$ pre α z $\mathbb{N}$, $\alpha > 1$. Rovnako $\lambda = \beta\lambda_2$ pre β z $\mathbb{N}$, $\beta > 1$. Ak by $gcd(\alpha, \beta) > 1$, označme ho g, potom dostávame

$$\alpha\lambda_1 = \beta\lambda_2$$
$$\frac{\alpha\lambda_1}{g} = \frac{\beta\lambda_2}{g} = l$$

Pre l platí, že je z $\mathbb{N}$, $l < \lambda$ a tiež λ_1/l a λ_2/l. Teda l je spoločný násobok λ_1, λ_2 menší ako ten najmenší. Potom musí platiť, že α, β sú nesúdeliteľné, teda $gcd(\alpha, \beta) = 1$. Keďže $\alpha \geq 2$ a $gcd(\alpha, \beta) = 1$, tak najmešia možná hodnota pre β je 3, a teda $\beta \geq 3$. Z toho dostávame

$$2\lambda_1 \leq \alpha\lambda_1 = \lambda \quad \rightsquigarrow \quad 2\lambda_1 \leq \lambda \quad \rightsquigarrow \quad \lambda_1 \leq \frac{1}{2}\lambda$$

$$3\lambda_2 \leq \beta\lambda_2 = \lambda \quad \rightsquigarrow \quad 3\lambda_2 \leq \lambda \quad \rightsquigarrow \quad \lambda_2 \leq \frac{1}{3}\lambda$$

Potom platí

$$\lambda_1 + \lambda_2 \leq \frac{1}{2}\lambda + \frac{1}{3}\lambda = \left(\frac{1}{2} + \frac{1}{3}\right)\lambda = \frac{5}{6}\lambda$$

Zároveň vieme, že $sum([A_1, A_2]) = sc(A_1) + sc(A_2) = \lambda_1 + \lambda_2$. Z toho dostávame, že $sum([A_1, A_2]) \leq \frac{5}{6}\lambda$. □

Spojením týchto dvoch liem (5)(6) dostávame ohraničenie *sum*-kvality efektívnych 2-rozkladov pre prísne λ-cyklické jazyky.

Veta 9. *Nech $[A_1, A_2]$ je efektívny 2-rozklad minimálneho automatu A pre nejaký prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$. Potom $\lceil 2\sqrt{\lambda} \rceil \leq sum([A_1, A_2]) \leq \frac{5}{6}\lambda$.*

Máme teda dolný aj horný odhad pre *sum*-kvalitu efektívnych 2-rozkladov. To ale ešte nehovorí ako kvalitné efektívne 2-rozklady naozaj existujú, len, že sa ich *sum*-kvalita pohybuje medzi dokázanými hranicami. Teraz ukážeme, že nami odhadnuté hranice sú presné tak, že nájdeme jazyky a efektívne 2-rozklady ich minimálnych automatov, ktorých *sum*-kvalita sa bude rovnať práve týmto hraniciam.

Veta 10. *Existuje prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$ a efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A taký, že $sum([A_1, A_2]) = \lceil 2\sqrt{\lambda} \rceil$.*

Dôkaz. Zoberme jazyk $L = \{a^{12k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 12$ a minimálny automat akceptujúci L je UDFA A veľkosti $(12, 0)$ štandardného tvaru (Značenie 1), kde $F = \{q[0]\}$. Zoberme UDFA A_1, A_2 veľkostí $(3, 0)$, $(4, 0)$ štandardného tvaru (Značenie 1), kde $F_1 = \{q_1[0]\}$ a $F_2 = \{q_2[0]\}$. Platí, že $lcm(3, 4) = 12$. Potom pre automaty A_1, A_2 platí, že $L(A_1) \cap L(A_2) = L$ a tiež $sc(A_1) = 3 < 12$

a $sc(A_2) = 4 < 12$, teda automaty A_1, A_2 tvoria efektívny 2-rozklad automatu A, ktorý je minimálny akceptujúci L.

Platí, že $sum([A_1, A_2]) = sc(A_1) + sc(A_2) = 3 + 4 = 7$. Zároveň platí, že $\lceil 2\sqrt{12} \rceil = \lceil 6,928 \rceil = 7$. Našli sme teda prísne λ-cyklický jazyk L a efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A, kde platí $sum([A_1, A_2]) = \lceil 2\sqrt{\lambda} \rceil$. □

Veta 11. *Existuje prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$ a efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A taký, že $sum([A_1, A_2]) = \frac{5}{6}\lambda$.*

Dôkaz. Opäť zoberme jazyk $L = \{a^{12k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 12$ a minimálny automat akceptujúci L je UDFA A veľkosti $(12, 0)$ štandardného tvaru (Značenie 1), kde $F = \{q[0]\}$. Zoberme UDFA A_1, A_2 veľkostí $(6, 0)$, $(4, 0)$ štandardného tvaru (Značenie 1), kde $F_1 = \{q_1[0]\}$ a $F_2 = \{q_2[0]\}$. Platí, že $lcm(6, 4) = 12$. Potom vieme, že $L(A_1) \cap L(A_2) = L$ a tiež $sc(A_1) = 6 < 12$ a $sc(A_2) = 4 < 12$, teda automaty A_1, A_2 tvoria efektívny 2-rozklad automatu A, ktorý je minimálny akceptujúci L.

Platí, že $sum([A_1, A_2]) = sc(A_1) + sc(A_2) = 6 + 4 = 10$. Zároveň platí, že $\frac{5}{6}12 = 10$. Našli sme teda prísne λ-cyklický jazyk L a efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A, kde platí $sum([A_1, A_2]) = \frac{5}{6}\lambda$. □

Napriek tomu, že sú naše odhady sum-kvality presné, ukážeme, že existujú jazyky, ktorých aj najkvalitnejšie efektívne 2-rozklady sú v porovnaní s dolným odhadom veľmi zlé. Dokonca sa nám podarí ukázať, že rozdiel medzi dolným odhadom sum-kvality pre efektívne 2-rozklady a najkvalitnejším efektívnym 2-rozkladom môže byť ľubovoľne veľký.

Veta 12. *Pre každé $\delta \in \mathbb{N}$ existuje 2-rozložiteľný prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$ taký, že pre každý efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A platí, že $sum([A_1, A_1]) - \lceil 2\sqrt{\lambda} \rceil > \delta$.*

Dôkaz. Nech δ patrí do $\mathbb{N}$. Nech $L_p = \{a^{2pk} \mid k \in \mathbb{N}\}$, kde p je nejaké prvočíslo, $p > 2$. L_p je prísne λ-cyklický jazyk pre $\lambda = 2p$. Minimálny automat akceptujúci L_p je UDFA A_p veľkosti $(2p, 0)$ štandardného tvaru (Značenie 1), kde $F_p = \{q_p[0]\}$.

Ak $[A_1, A_2]$ je efektívny 2-rozklad A_p, tak musí platiť, že A_1, A_2 sú UDFA veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$, $lcm(\lambda_1, \lambda_2) = \lambda$, $\lambda_1 < \lambda$, $\lambda_2 < \lambda$ a $L(A_1) \cap L(A_2) = L$. Potom taktiež platí, že λ_1/λ a aj λ_2/λ. Keďže $\lambda = 2p$, kde 2 aj p sú prvočísla, tak λ_1 aj λ_2 môžu nadobúdať iba hodnoty $1, 2, p, 2p$. Ale ak $\lambda_i = 2p$ pre nejaké i z $\{1, 2\}$, tak potom $\lambda_i = \lambda$, čo nemôže nastať. Taktiež ak $\lambda_i = 1$ pre nejaké i z $\{1, 2\}$, tak potom aby platilo $lcm(\lambda_1, \lambda_2) = \lambda$, tak λ_j pre $j \neq i$ sa musí rovnať $2p$, čo nemôže nastať. Teda λ_1, λ_2 môžu nadobudnúť iba hodnoty 2 a p. Zároveň sa ale nesmú rovnať, aby platilo

$lcm(\lambda_1, \lambda_2) = \lambda = 2p$. Potom jediné prípustné hodnoty, až na poradie, sú $\lambda_1 = 2$ a $\lambda_2 = p$.

Zároveň vieme, že pre UDFA B_1, B_2 veľkostí $(2,0)$, $(p,0)$ štandardného tvaru (Značenie 1), kde $F_1 = \{q_1[0]\}$ a $F_2 = \{q_2[0]\}$ platí, že $L(B_1) \cap L(B_2) = L_p$, a teda tvoria efektívny 2-rozklad A_p. A_p je teda efektívne 2-rozložiteľný a pre každý jeho efektívny 2-rozklad $[A_1, A_2]$ platí, že A_1, A_2 sú veľkostí $(2,0)$ respektíve $(p,0)$. Teda $sc(A_1) = 2$ a $sc(A_2) = p$, z čoho dostávame, že $sum([A_1, A_2]) = sc(A_1) + sc(A_2) = p + 2$.

Ak chceme, aby platilo $p + 2 - \lceil 2\sqrt{2p} \rceil > \delta$, už potrebujeme len zvoliť vhodné prvočíslo p. Vo všeobecnosti platí, že $2\sqrt{2p} + 1 > \lceil 2\sqrt{2p} \rceil$, potom $p + 2 - \lceil 2\sqrt{2p} \rceil > p + 2 - (2\sqrt{2p} + 1)$. Stačí nám teda ukázať, že $p + 2 - 2\sqrt{2p} - 1 > \delta$. Dostávame teda

$$\begin{aligned}
p + 2 - 2\sqrt{2p} - 1 &> \delta \\
p + 2 - 2\sqrt{2p} &> \delta + 1 \\
(\sqrt{p} - \sqrt{2})^2 &> \delta + 1 \\
\sqrt{p} - \sqrt{2} &> \sqrt{\delta + 1} \\
\sqrt{p} &> \sqrt{\delta + 1} + \sqrt{2} \\
p &> \delta + 1 + 2\sqrt{2(\delta + 1)} + 2 \\
p &> \delta + 3 + 2\sqrt{2\delta + 2}
\end{aligned}$$

Potom ak $p > \delta + 3 + 2\sqrt{2\delta + 2}$, tak L_p je nami hľadaný jazyk. Pričom takéto p určite existuje pre každé δ z $\mathbb{N}$, lebo podľa Vety 2 je prvočísel nekonečne veľa. Dostávame teda, že pre ľubovoľné δ z $\mathbb{N}$ existuje 2-rozložiteľný prísne λ-cyklický jazyk taký, že pre každý efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu platí, že $sum([A_1, A_1]) - \lceil 2\sqrt{\lambda} \rceil > \delta$. $\square$

Kapitola 3

3-rozložiteľnosť

V tejto kapitole zavedieme rozklad jazykov a automatov na tri nové jazyky respektíve automaty v prípade DFA s cieľom zlepšiť kvalitu rozkladov. Obdobne ako pri rozkladoch DFA na dva nové automaty definujeme efektívne rozklady na tri nové automaty a takto rozložiteľné jazyky následne charakterizujeme.

Vždy je zaujímavé skúmať, či nám pridanie nových možností umožní riešiť viac problémov, ako napríklad pri prechode z konečných automatov na zásobníkové, alebo nám umožní riešiť problémy efektívnejšie, ako napríklad pri prechode z jednopáskového turingovho stroja na viacpáskový v prípade časovej zložitosti. Preto sa teraz pozrieme na možnosť pridania druhej rady. Pre náš problém, regulárny jazyk $L \in \mathcal{R}$, budeme mať dve rady, regulárne jazyky $L_{adv1}, L_{adv2} \in \mathcal{R}$ a bude nás zaujímať či vieme nájsť nový problém $L_{new} \in \mathcal{R}$ taký, že spolu jednoznačne určia riešenie pôvodného problému, teda $L = L_{adv1} \cap L_{adv2} \cap L_{new}$. Za zložitosť riešenia A opäť považujeme stavovú zložitosť daného automatu ($sc(A)$). Rovnako za zložitosť problému L berieme jeho deterministickú stavovú zložitosť ($sc(L)$). Znovu sa na túto situáciu budeme pozerať ako na rozklad minimálneho automatu A_{min} akceptujúceho L na tri nové automaty $A_{adv1}, A_{adv2}, A_{new}$ akceptujúce jazyky $L_{adv1}, L_{adv2}, L_{new}$. Rovnako opäť požadujeme aby boli rady rozumné, teda $sc(A_{adv1}) < sc(A_{min})$ a $sc(A_{adv2}) < sc(A_{min})$ a nový problém jednoduchší než pôvodný, teda $sc(A_{new}) < sc(A_{min})$.

Na rozdiel od 2-rozkladu automatu A potrebujeme pri *3-rozklade* ešte nejaké dodatočné podmienky na nové automaty A_1, A_2, A_3. Uveďme ilustračný príklad, z ktorého vyplynie akú ďalšiu podmienku budeme požadovať.

Príklad 2. Zoberme jazyk $L = \{a^{6k} \mid k \in \mathbb{N}\}$. Minimálny automat A akceptujúci L bude UDFA veľkosti $(6, 0)$ štandardného tvaru (Značenie 1), kde $F = \{q[0]\}$. Zostrojme UDFA A_1, A_2, A_3 štandardného tvaru (Značenie 1), kde $F_i = \{q_i[0]\}$ pre každé i z $\{1, 2, 3\}$, veľkostí $(3, 0)$, $(2, 0)$ respektíve $(1, 0)$. Takto zostrojené automaty akceptujú jazyky $L(A_1) = \{a^{3k} \mid k \in \mathbb{N}\}$, $L(A_2) = \{a^{2k} \mid k \in \mathbb{N}\}$ $L(A_3) = \{a^*\}$. Pre tieto automaty síce platí, že $sc(A_i) < sc(A)$ pre každé i z $\{1, 2, 3\}$ a tiež

$L = L(A_1) \cap L(A_2) \cap L(A_3)$, keďže $lcm(3, 2, 1) = 6$, ale platí aj $L = L(A_1) \cap L(A_2)$, keďže teiž $lcm(2, 3) = 6$. Automat A_3 akceptuje $\{a\}^*$, teda všetky slová nad abecedou Σ jazyka L a preto je v tomto rozklade úplne zbytočný. Ak by sme jazyk $L(A_3)$ považovali za radu, tak by nám takáto rada žiadnu novú informáciu nepridala, ak by sme ho považovali za nový problém, tak by bol triviálny, presne čomu sme sa pri 2-rozklade potrebovali vyhnúť zavedením podmienky na stavovú zložitosť nových automatov. Preto tento prípad nebudeme považovať za 3-rozklad.

Je ľahké nahliadnuť, že podobná situácia so zbytočným automatom v rozklade nastane nielen vtedy, keď jeden z automatov akceptuje všetky slová nad danou abecedou, ale vždy, keď jeden z automatov A_i akceptuje ľubovoľnú nadmnožinu prieniku jazykov akceptovaných automatmi A_j, A_l, teda $L(A_i) \supseteq L(A_j) \cap L(A_l)$ pre $i \neq j \neq l$ a zároveň sa tento prienik už rovná jazyku akceptovanému pôvodným automatom A, teda $L(A) = L(A_j) \cap L(A_l)$. Potom jazyk $L(A_i)$ neprispieva nijakou užitočnou informáciou do tvorby rozkladu. Teraz už môžeme obdobne ako pri 2-rozložiteľnosti pomocou dvoch definícii formálne sformulovať 3-rozložiteľnosť automatu A a následne jazyka L.

Definícia 11. Nech A je DFA. Trojicu DFA $[A_1, A_2, A_3]$ nazývame 3-rozklad DFA A ak $L(A) = L(A_1) \cap L(A_2) \cap L(A_3)$, $sc(A_1) < sc(A)$, $sc(A_2) < sc(A)$, $sc(A_3) < sc(A)$ a pre každé $i, j \in \{1, 2, 3\},\ i \neq j$ platí, že $L(A_i) \cap L(A_j) \neq L(A)$. Ak takýto 3-rozklad DFA A existuje, hovoríme, že A je 3-rozložiteľný.

Definícia 12. Nech $L \in \mathcal{R}$. Hovoríme, že L je deterministicky 3-rozložiteľný ak minimálny DFA akceptujúci L je 3-rozložiteľný.

3.1 Efektívne 3-rozklady λ-cyklických jazykov

Je prirodzené, že pri skúmaní 3-rozkladu prísne λ-cyklických jazykov vyjdeme z ich 2-rozkladu. Keďže motivácia za zavedením 3-rozkladu bola zlepšiť kvalitu samotného rozkladu, už v definícii sme vypustili potenciálne rozklady, ktoré by boli len 2-rozkladmi obohatenými o zbytočný jazyk, ktorý nijako neovplyvný ich spoločný prienik. Avšak sa ukázalo, že podľa tejto definície stále existujú 3-rozklady určitých prísne λ-cyklických jazykov, ktoré sú inherentne horšie ako niektoré ich 2-rozklady. Takéto rozklady môžeme zostrojiť tak, že zoberieme nejaký 2-rozklad, ktorý pokazíme pridaním zbytočných akceptačných stavov do príslušných automatov a následne pridáme tretí automat, ktorý bude tieto novo pridané zlé slová filtrovať. Existujú prísne λ-cyklické jazyky, pre ktoré vieme takéto automaty zostrojiť tak, že splnia definíciu 3-rozkladu.

Príklad 3. Zoberme jazyk $L = \{a^{12k+2} \mid k \in \mathbb{N}\}$. Dá sa ukázať, že minimálny automat akceptujúci L je UDFA A veľkosti $(12, 0)$. Zostrojme UDFA A_1, A_2, A_3 štandardného tvaru (Značenie 1) veľkostí $(3, 0), (4, 0), (5, 0)$, kde $F_1 = \{q_1[1], q_1[2]\}$, $F_2 = \{q_2[1], q_2[2]\}$ a $F_3 = \{q_3[0], q_3[2]\}$. Dá sa ukázať, že $L(A_1) = \{a^{3k+1}, a^{3k+2} \mid k \in \mathbb{N}\}$. Rovnako sa dá ukázať, že $L(A_2) = \{a^{4k+1}, a^{4k+2} \mid k \in \mathbb{N}\}$ a $L(A_3) = \{a^{6k}, a^{6k+2} \mid k \in \mathbb{N}\}$. Potom prienik $L(A_1) \cap L(A_2) = \{a^{12k+1}, a^{12k+2}, a^{12k+5}, a^{12k+10} \mid k \in \mathbb{N}\}$. Ďalej prienik $L(A_1) \cap L(A_3) = \{a^{12k+2}, a^{12k+8} \mid k \in \mathbb{N}\}$ a prienik $L(A_2) \cap L(A_3) = \{a^{12k+2}, a^{12k+6} \mid k \in \mathbb{N}\}$. Skutočne prienik $L(A_1) \cap L(A_2) \cap L(A_3) = L$ a pre každú dvojicu automatov A_i, A_j, kde i, j sú z $\{1, 2, 3\}$ platí, že prienik jazykov, ktoré akceptujú, sa nerovná L. A_1, A_2, A_3 teda tvoria 3-rozklad A. Ale rovako sa dá ukázať, že automat A sa dá rozložiť na automaty B_1, B_2 štandardného tvaru (Značenie 1) veľkostí $(3, 0), (4, 0)$, kde $F_1 = \{q_1[2]\}$ a $F_2 = \{q_2[2]\}$. V 3-rozklade je teda automat A_3 vlastne zbytočný, keďže len zachraňuje to, že dvojica automatov $[A_1, A_2]$ je vlastne len pokazením rozkladu $[B_1, B_2]$ (Vznikla pridaním zbytočných akceptačných stavov $q_1[1], q_2[1]$).

Podobne ako nás takéto vlastne pokazené rozklady nezujímali pri skúmaní kvality 2-rozkladov, nie sú pre nás z pohľadu kvality zaujímavé ani takéto 3-rozklady. Obdobne ako pri 2-rozložiteľnosti môžeme teda zadefinovať efektívne 3-rozklady, kde automaty takéhoto rozkladu budú mať nulové chvosty a najmenší spoločný násobok dĺžok ich cyklov bude dĺžka cyklu minimálneho automatu akceptujúceho daný jazyk L. Avšak ako ukazuje Príklad 3, tak to nestačí, lebo stále máme rozklady, ktoré síce nie sú pokazením iného 3-rozkladu, ale pokazením nejakého 2-rozkladu pre daný jazyk L. Všetky takéto 3-rozklady majú spoločnú vlastnosť, že pre dva automaty z daného 3-rozkladu A_i, A_j, kde $i \neq j$, veľkostí $(\lambda_i, 0), (\lambda_j, 0)$ platí, že $lcm(\lambda_1, \lambda_2) \geq \lambda$. Určite to platí práve pre tie dva automaty, ktoré sú pokazením nejakého 2-rozkladu. Teda pri skúmaní 3-rozkladov, keďže pôvodná motivácia bola zlepšiť kvalitu rozkladov oproti 2-rozkladom, nás skutočne môžu zaujímať iba rozklady na automaty A_1, A_2, A_3 veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$, kde $lcm(\lambda_i, \lambda_j) < \lambda$ pre každé i, j z $\{1, 2, 3\}$, $i \neq j$. Obdobne ako pri 2-rozložiteľnosti pre prísne λ-cyklické jazyky definujeme *efektívnu* 3-rozložiteľnosť s danými prísnejšími podmienkami a práve jej skúmaniu sa budeme v tejto kapitole venovať.

Definícia 13. Nech A je UDFA veľkosti $(\lambda, 0)$ pre nejaké $\lambda \in \mathbb{N}$. Trojicu UDFA $[A_1, A_2, A_3]$ kde automaty A_1, A_2, A_3 sú veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$ nazývame efektívny 3-rozklad UDFA A ak $L(A) = L(A_1) \cap L(A_2) \cap L(A_3)$, $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé $i, j \in \{1, 2, 3\}$, $i \neq j$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. Ak takýto efektívny 3-rozklad UDFA A existuje, hovoríme, že A je efektívne 3-rozložiteľný.

Poznámka 10. Všimnimne si, že v definícii efektívneho 3-rozkladu nie je priamo uvedená podmienka, aby pre automat A_i veľkosti $(\lambda_i, 0)$ z rozkladu platilo, že $\lambda_i < \lambda$.

Teda, že tento automat je menší ako pôvodný automat A. Táto vlastnosť priamo vyplynie z podmienky, že $lcm(\lambda_i, \lambda_j) < \lambda$, kde $(\lambda_j, 0)$ je veľkosť ďalšieho automatu A_j z rozkladu pre $i \neq j$, keďže očividne platí, že $\lambda_i \leq lcm(\lambda_i, \lambda_j)$.

Definícia 14. Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$, nech UDFA A je minimálny automat akceptujúci L. Hovoríme, že L je deterministicky efektívne 3-rozložiteľný ak UDFA A je efektívne 3-rozložiteľný.

Teraz dokážeme, že efektívne 3-rozložiteľné jazyky sú skutočne všetky 3-rozložiteľné a teda naša nová definícia je len zúžením definície 3-rozložiteľnosti pre prísne λ-cyklické jazyky, aby sme odfiltrovali z pohľadu kvality pre nás nezaujímavé 3-rozklady. Na rozdiel od efektívnej 2-rozložiteľnosti 3-rozložiteľnosť a efektívna 3-rozložiteľnosť nie sú ekvivalentné a existujú 3-rozložiteľné jazyky, ktoré nie sú efektívne 3-rozložiteľné. Príkladom takého jazyka je práve jazyk z Príkladu 3. Teda platí len jedna z dvoch implikácii, ktorú teraz dokážeme.

Veta 13. *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Ak je L deterministicky efektívne 3-rozložiteľný, tak je aj deterministicky 3-rozložiteľný.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech L je deterministicky efektívne 3-rozložiteľný a nech A je minimálny UDFA akceptujúci L. Potom A je efektívne 3-rozložiteľný. Nech UDFA A_1, A_2, A_3 veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$ tvoria efektívny 3-rozklad UDFA A. Teda platí $L = L(A_1) \cap L(A_2) \cap L(A_3)$, $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z $\{1, 2, 3\}$, kde $i \neq j$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. Označme množinu $\{1, 2, 3\} = I$. Ukážeme, že automaty A_1, A_2, A_3 tvoria 3-rozklad automatu A.

Pre každé a, b z $\mathbb{N}$ platí, že $a/lcm(a, b)$ a tiež $b/lcm(a, b)$. Potom platí $a \leq lcm(a, b)$ a $b \leq lcm(a, b)$. Teda platí aj $\lambda_i \leq lcm(\lambda_i, \lambda_j)$ a $\lambda_j \leq lcm(\lambda_i, \lambda_j)$ a tiež vieme, že $lcm(\lambda_i, \lambda_j) < lcm(\lambda_1, \lambda_2, \lambda_3)$ pre každé i, j z I, kde $i \neq j$. Z toho dostávame, že pre každé i z I platí $\lambda_i < lcm(\lambda_1, \lambda_2, \lambda_3)$, teda platí $\lambda_i < \lambda$. Taktiež vieme, že pre každé UDFA B veľkosti (λ_b, μ_b) platí $sc(B) = \lambda_b + \mu_b$. Teda platí aj $sc(A_i) = \lambda_i$ pre každé i z I a $sc(A) = \lambda$. Čo znamená, že pre každé i z I platí, že $sc(A_i) < sc(A)$.

Teraz už potrebujeme len dokázať, že pre každé i, j z I, kde $i \neq j$ platí $L(A_i) \cap L(A_j) \neq L$. Sporom predpokladajme, že existujú i, j z I, kde $i \neq j$ také, že $L(A_i) \cap L(A_j) = L$. Bez ujmy na všeobecnosti nech $i = 1$ a $j = 2$. Platí teda $L(A_1) \cap L(A_2) = L$, pričom A_1 je veľkosti $(\lambda_1, 0)$ a A_2 je veľkosti $(\lambda_2, 0)$. Podľa Vety 6 potom existuje automat A' veľkosti $(lcm(\lambda_1, \lambda_2), 0)$ akceptujúci jazyk $L(A_1) \cap L(A_2)$, teda jazyk L. Zároveň platí, že $lcm(\lambda_1, \lambda_2) < \lambda$ a tiež, že automat A veľkosti $(\lambda, 0)$ je minimálny automat akceptujúci L. Ďalej platí, že $sc(A) = \lambda$ a $sc(A') = lcm(\lambda_1, \lambda_2)$. Čím dostávame spor, lebo sme našli automat A' akceptujúci jazyk L, ktorý je menší než minimálny automat akceptujúci daný jazyk, keďže $sc(A') < sc(A)$. Potom pre každé i, j z I, kde $i \neq j$ musí platiť $L(A_i) \cap L(A_j) \neq L$.

Z toho dostávame, že automaty A_1, A_2, A_3 tvoria 3-rozklad automatu A. Teda UDFA A je 3-rozložiteľný a potom L je deterministicky 3-rozložiteľný. □

Pri charakterizovaní 2-rozložiteľných prísne λ-cyklických jazykov využívame bipartitný, teda vrcholovo dva-zafarbiteľný graf a zovšeobecnenie čínskej zvyškovej vety (1). Daný prísne λ-cyklický jazyk L je 2-rozložiteľný práve vtedy, keď je aj efektívne 2-rozložiteľný. A práve jeho efektívny 2-rozklad je použitý pri dôkaze charakterizácie 2-rozložiteľnosti (5). Ukáže sa, že obdobne využijeme tri-zafarbiteľný graf a zovšeobecnenie čínskej zvyškovej vety (1) aj pri charakterizácii efektívnej 3-rozložiteľnosti. Konštrukcia tri-zafarbiteľného grafu bude zovšeobecnením konštrukcie pre 2-rozložiteľnosť, len budeme musieť ešte doriešiť niektoré problémy, ktoré pri rozšírení rozkladu nastali.

3.2 Graf indukovaný jazykom

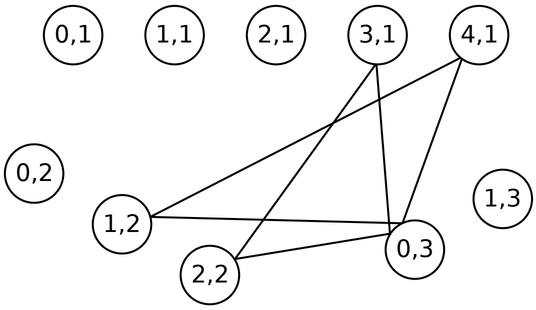
Definícia 15. Nech L je prísne λ-cyklický jazyk pre $\lambda \in \mathbb{N}$, nech $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$. Graf indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ je 3-zafarbiteľný graf $G = (V, E)$, kde
$V = V_1 \cup V_2 \cup V_3$, kde pre každé $i \in \{1,2,3\}$ $V_i = \{[r,i] \mid r \in \mathbb{Z}_{\lambda_i}\}$
$E = \{([r,i],[p,j]) \in V \times V \mid (\exists [s,k] \in V)\ i \neq j \neq k,\ (\exists m \in \mathbb{N})\ m \equiv r\ (mod\ \lambda_i) \wedge m \equiv p\ (mod\ \lambda_j)\ \wedge\ m \equiv s\ (mod\ \lambda_k)\ \wedge\ a^m \in L\}$

Intuitívne vrcholy grafu sú rozdelené do troch množín, respektíve zafarbené tromi farbami, pričom každá farba prislúcha nejakému i z $\{1,2,3\}$. Vrcholy tejto farby predstavujú prvky zo $\mathbb{Z}_{\lambda_i}$. Pre každé slovo $w = a^m$ z jazyka L sa v grafe nachádza trojuholník (kružnica dĺžky 3) s každým vrcholom inej farby, kde tieto vrcholy prislúchjú prvkom zo $\mathbb{Z}_{\lambda_i}$ kongruentným s m modulo príslušné λ_i. Uvedomme si, že presne toto hovorí podmienka na existenciu hrany medzi dvomi vrcholmi. Vrcholy r, p spája hrana, ak existuje vrchol s taký, že každý z tejto trojice vrcholov je inej farby a existuje prirodzené číslo m také, že je kongruentné s prvkom zo $\mathbb{Z}_{\lambda_i}$ prislúchajúcemu vrcholu zafarmenému farbou i modulo λ_i a tiež a^m leží v L. Potom hrana spája aj vrcholy r, s a p, s lebo pre ne taký tretí vrchol tiež existuje, práve p respektíve r, a tiež pre ne existuje také prirodzené číslo, práve m. Zároveň pre všetky prirodzené čísla m, λ existuje také $t \in \mathbb{Z}_\lambda$, ktoré je kongruentné s m modulo dané λ, čiže pre každé slovo z jazyka L existuje trojica vrcholov, ktorá spĺňa danú podmienku a tvorí v indukovanom grafe trojuholník.

Príklad 4. Majme jazyk $L = \{a^{30k+4}, a^{30k+8} \mid k \in \mathbb{N}\}$. Dá sa ukázať, že minimálny automat A akceptujúci tento jazyk je UDFA veľkosti $(30, 0)$, teda L je prísne λ-cyklický jazyk pre $\lambda = 30$. Zvolme $\lambda_1 = 5,\ \lambda_2 = 3,\ \lambda_3 = 2$. Zostrojme tri-zafarbiteľný graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ podľa definície (Obrázok 3.1).

$V_1 = \{[0,1],[1,1],[2,1],[3,1],[4,1]\}$
$V_2 = \{[0,2],[1,2],[2,2]\}$
$V_1 = \{[0,3],[1,3]\}$

Trojica vrcholov $[4,1],[1,2],[0,3]$ tvorí príslušný trojuholník pre slová tvaru a^m, kde $m = 30k+4$ pre nejaké k z $\mathbb{N}$, keďže pre ľubovoľné dva z nich existuje vrchol, ten tretí, taký, že sú zafarbené rôznymi farbami a platí, že $m \equiv 4\ (mod\ 5)$, $m \equiv 1\ (mod\ 3)$, $m \equiv 0\ (mod\ 2)$ a a^m leží v jazyku L. Obdobne pre slová tvaru a^m, kde $m = 30k+8$ pre nejaké k z $\mathbb{N}$, máme v grafe trojuholník z vrcholov $[3,1],[2,2],[0,3]$. Žiadne iné slová nie sú v jazyku a preto ani v grafe G nemôžu byť ďalšie hrany.



Obr. 3.1: Graf G indukovaný $L = \{a^{30k+4}, a^{30k+8} \mid k \in \mathbb{N}\}, \lambda_1, \lambda_2, \lambda_3$, kde $\lambda_1 = 5$, $\lambda_2 = 3$ a $\lambda_3 = 2$

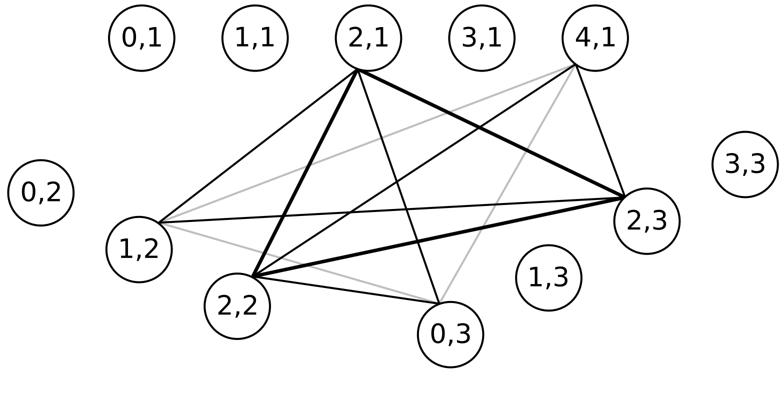
Definícia 16. Nech L je prísne λ-cyklický jazyk pre $\lambda \in \mathbb{N}$, nech $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$. Nech G je graf indukovaný $L, \lambda_1, \lambda_2, \lambda_3$, nech pre všetky $i \in \{1,2,3\}$ $V_i' = \{r \mid r \in V_i, d_G(r) > 0\}$, teda V_i' vznikne z V_i odstránením všetkých vrcholov nulového stupňa. Hovoríme, že graf G rozkladá L práve vtedy, keď pre všetky trojice $([r,1],[p,2],[s,3]) \in V_1' \times V_2' \times V_3'$ a pre všetky $m \in \mathbb{N}$ platí, že ak $m \equiv r\ (mod\ \lambda_1)\ \wedge\ m \equiv p\ (mod\ \lambda_2)\ \wedge\ m \equiv s\ (mod\ \lambda_3)$, tak potom $a^m \in L$.

Intuitívne graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá jazyk L, ak po zanedbaní všetkých vrcholov stupňa nula, pre každú trojicu vrcholov rôznej farby platí, že buď neexistuje m kongruentné s príslušnými tromi vrcholmi modulo príslušné λ_i alebo pre každé m, ktoré spĺňa danú kongruenciu slovo a^m patrí do jazyka L.

Tým hovoríme, že medzi vrcholy s nenulovým stupňom rôznych farieb v grafe G už nevieme pridať ďalšie hrany podľa podmienky z konštrukcie grafu ani keby sme nevyžadovali, že musí platiť záver tejto podmienky, teda, že a^m patrí do jazyka L, ale stačila by nám iba existencia m kongruentného s danými vrcholmi modulo príslušné λ_i.

Takisto každý trojuholník v grafe G prislúcha nejakým slovám z jazyka, čiže sme nevytvori nijaký trojuholník takpovediac nechtiac. Takáto situácia môže nastať ak do grafu pridáme tri trojuholníky, pre ktoré platí, že každá dvojica z nich má spoločný jeden vrchol, ale všetky tri nemajú spoločný žiadny vrchol. Vtedy dostávame tri vrcholy $[p,1],[r,2],[s,3]$ a tri prirodzené čísla m_1, m_2, m_3, kde platí $p \equiv m_1 \ (mod\ \lambda_1)$ a $r \equiv m_1 \ (mod\ \lambda_2)$, ďalej $r \equiv m_2 \ (mod\ \lambda_2)$ a $s \equiv m_2 \ (mod\ \lambda_3)$ a taktiež $p \equiv m_3 \ (mod\ \lambda_1)$ a $s \equiv m_3 \ (mod\ \lambda_3)$. Podľa zovšeobecnenia čínskej zvyškovej vety (1) potom existuje jedno m kongruentné s $p\ mod\ \lambda_1$, $r\ mod\ \lambda_2$, $s\ mod\ \lambda_3$. Preto aby bola splnená podmienka z definície grafu rozkladajúceho jazyk L, musia aj všetky slová prislúchajúce tomuto trojuholníku patriť do jazyka L, a teda naozaj každý trojuholník v grafe prislúcha nejakým slovám z jazyka.

Príklad 5. Uveďme príklad jazyka, kde graf indukovaný L a príslušnými λ_i obsahuje práve takýto nechtiac vytvorený trojuholník a teda nerozkladá jazyk L. Majme $L = \{a^{60k+4}, a^{60k+14}, a^{60k+22}, a^{60k+32}, a^{60k+34}, a^{60k+44}, a^{60k+52} \mid k \in \mathbb{N}\}$. Dá sa ukázať, že minimálny automat akceptujúci tento jazyk je UDFA A veľkosti $(60, 0)$, teda L je prísne λ-cyklický jazyk pre $\lambda = 60$. Zvolme $\lambda_1 = 5,\ \lambda_2 = 3,\ \lambda_3 = 4$ a zostrojme príslušný indukovaný graf G (Obrázok 3.2). Špeciálne sa pozrime na tri trojuholníky, ktoré vytvoria ten nechcený. Slovám tvaru a^{60k+32} prislúcha trojuholník s vrcholmi $[2,1],[2,2],[0,3]$. Slovám tvaru a^{60k+14} prislúcha trojuholník s vrcholmi $[4,1],[2,2],[2,3]$. Slovám tvaru a^{60k+22} prislúcha trojuholník s vrcholmi $[2,1],[1,2],[2,3]$. Týmto sme v grafe vytvorili aj trojuholník z vrcholov $[2,1],[2,2],[2,3]$, ktorý by prislúchal slovám tvaru a^{60k+2}, keďže platí $60k+2 \equiv 2 \ (mod\ 5)$, $60k+2 \equiv 2 \ (mod\ 3)$ a $60k+2 \equiv 2 \ (mod\ 4)$ pre každé k z $\mathbb{N}$, avšak takéto slová neležia v jazyku L. Keďže sme našli trojicu vrcholov nenulového stupňa rôznej farby a $m = 60k+2$ pre nejaké k z $\mathbb{N}$, kongruenté s danými vrcholmi modulo príslušné λ_i také, že a^m neleží v jazyku, tak G nerozkladá L.



Obr. 3.2: Graf G indukovaný $L = \{a^{60k+4}, a^{60k+14}, a^{60k+22}, a^{60k+32}, a^{60k+34}, a^{60k+44}, a^{60k+52} \mid k \in \mathbb{N}\}, \lambda_1, \lambda_2, \lambda_3$, kde $\lambda_1 = 5$, $\lambda_2 = 3$ a $\lambda_3 = 4$

legenda: čierna tenká - trojuholníky tvoriace nechcený; čierna hrubá - nechcene vytvorený trojuholník; šedá - zvyšné hrany grafu

Poznámka 11. Všimnime si, že ak by sme podmienku kedy graf G rozkladá jazyk L formulovali ako pri 2-rozložiteľnosti, teda nasledovne:

Hovoríme, že graf G rozkladá L práve vtedy, keď pre všetky dvojice $([r,1],[p,2],[s,3]) \in V_1' \times V_2' \times V_3'$ *platí, že ak existuje* $m \in \mathbb{N}$ *také, že* $m \equiv r \ (mod\ \lambda_1) \ \wedge \ m \equiv p \ (mod\ \lambda_2) \ \wedge \ m \equiv s \ (mod\ \lambda_3)$, *tak potom* $([r,1],[p,2]),([r,1],[s,3])([p,2],[s,3]) \in E$.

Tak potom by podľa tejto podmienky graf z Príkladu 5 rozkladal L a automaty zostrojené podľa tohto grafu by akceptovali aj zlé slová tvaru a^{60k+2}.

Uvedomme si, že ak navyše $\lambda_1, \lambda_2, \lambda_3$ spĺňajú podmienky z defície efektívnej 3-rozložiteľnosti (13), tak graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$, kde L je nejaký prísne λ-cyklický jazyk, ktorý navyše rozkladá L, určuje efektívny 3-rozklad minimálneho automatu A akceptujúceho jazyk L. Vrcholy grafu zafarbené jednou farbou predstavujú stavy nového automatu, tie ktoré sú nenulového stupňa predstavujú akceptačné. Pri úvahe či skutočne prenik jazykov akceptovaných takto zostrojenými automatmi sa rovná jazyku L, sa stačí pozerať len na slová tvaru a^m, kde $m < \lambda$, lebo keďže $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$, tak výpočty nových automatov na všetkých slovách tvaru $a^{k\lambda+n}$, kde k je z $\mathbb{N}$ a $n < \lambda$, všetky skončia v rovnakých stavoch, rovnako ako aj výpočty automatu A. Čiže sa nám stačí pozerať len slová kratšie ako λ.

Výpočty takto zostrojených nových automatov na vstupnom slove $w = a^m$ pre nejaké m z $\mathbb{N}$ skončia všetky v akceptačných stavoch len ak je m kongruentné s prvkami zo $\mathbb{Z}_{\lambda_i}$ prislúchajúcimi daným stavom modulo príslušné λ_i. Keďže graf G rozkladá L, potom w patrí do jazyka L.

Rovnako keď vstupné slovo w patrí do L, tak mu v grafe G podľa toho ako bol skonštruovaný prislúcha nejaký trojuholník, ktorého vrcholy sú práve stavy nových automatov, v ktorých skončia ich výpočty. Keďže tieto vrcholy sú nenulového stupňa, tak budú tieto stavy akceptačné a nové automaty budú všetky akceptovať vstupné slovo w. Na základe tohto môžeme teda sformulovať postačujúcu podmienku efektívnej 3-rozložiteľnosti pre prísne λ-cyklické jazyky. Ukáže sa, že táto podmienka je zároveň aj nutnou.

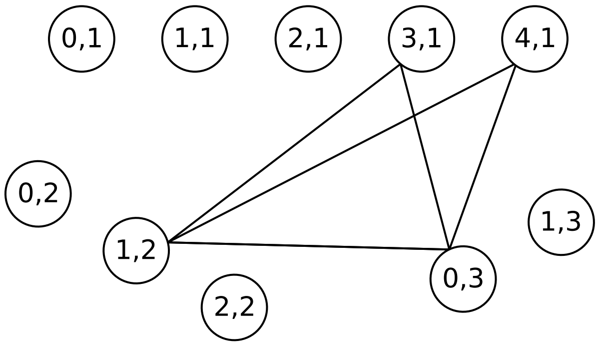
Teraz uveďme niekoľko príkladov prísne λ-cyklických jazykov s danými $\lambda_1, \lambda_2, \lambda_3$, pre ktoré platí $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z $\{1, 2, 3\}$, kde $i \neq j$ $lcm(\lambda_i, \lambda_j) < \lambda$, a príslušnými indukovanými grafmi, aby sme lepšie ukázali, kedy príslušný graf rozkladá daný jazyk a zároveň ako budú vyzerať automaty tvoriace efektívny 3-rozklad minimálneho automatu akceptujúceho daný jazyk zostrojené podľa príslušného indukovaného grafu.

Príklad 6. Zoberme jazyk $L = \{a^{30k+4}, a^{30k+8} \mid k \in \mathbb{N}\}$ a $\lambda_1, \lambda_2, \lambda_3$ z Príkladu 4. Zostrojme graf indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ (Obrázok 3.1). V tomto prípade je ľahké nahliadnuť, že graf G nerozkladá L. $\lambda_1, \lambda_2, \lambda_3$ sú po dvoch nesúdeliteľné a preto podľa CRT (1) systém kongruencii $x \equiv p \ (mod\ \lambda_1)$, $x \equiv r \ (mod\ \lambda_2)$, $x \equiv s \ (mod\ \lambda_3)$ má riešenie pre ľubovoľné p, r, s z $\mathbb{Z}$. Teda aby graf G rozkladal L, pre ľubovoľnú trojicu vrcholov nenulového stupňa rôznych farieb musia slová tvaru $a^{\lambda k+x}$ ležať v jazyku, kde x je riešením príslušného systému kongruencii pre dané vrcholy a k je z $\mathbb{N}$. V tomto prípade hneď vidíme, že táto podmienka nie je splnená, lebo podľa konštrukcie grafu G by musela ľubovoľná trojica vrcholov rôznych farieb a nenulového stupňa tvoriť trojuholník, čo neplatí napríklad pre vrcholy $[3,1],[1,2],[0,3]$. (V Príklade 5 každá trojica vrcholov nenulového stupňa a rôznych farieb tvorí trojuholník a preto je tažšie nahliadnuť, že daný graf nerozkladá daný jazyk.) Pre tieto tri vrcholy je riešením daného systému kongruencii zo $\mathbb{Z}_\lambda$ 28 a napríklad aj pre tieto hodnoty nie je splnená podmienka, aby graf rozkladal L. Potom graf G nerozkladá L. V tomto prípade teda nevieme zostrojiť efektívny 3-rozklad L podľa grafu G a keďže neskôr ukážeme, že existencia indukované grafu, ktorý rozkladá L, pričom $\lambda_1, \lambda_2, \lambda_3$ spĺňajú podmienky vyžadované v definícii efektívnej 3-rozložiteľnosti (13), je charakterizáciou efektívnej 3-rozložiteľnosti pre prísne λ-cyklické jazyky, vieme povedať, že jazyk L nie je efektívne 3-rozložiteľný.

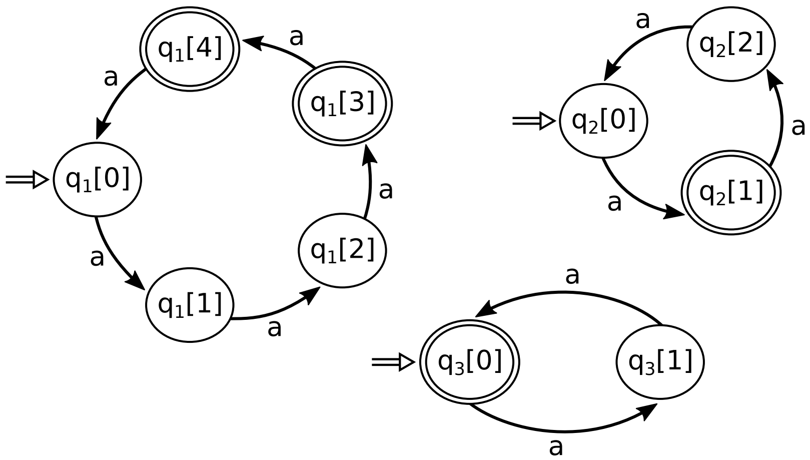
Príklad 7. Zoberme jazyk $L = \{a^{30k+4}, a^{30k+28} \mid k \in \mathbb{N}\}$. Dá sa ukázať, že minimálny automat akceptujúci tento jazyk je UDFA A veľkosti $(30,0)$, teda L je prísne λ-cyklický jazyk pre $\lambda = 30$. Zvolme $\lambda_1 = 5$, $\lambda_2 = 3$, $\lambda_3 = 2$. Zostrojme graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ (Obrázok 3.3). $\lambda_1, \lambda_2, \lambda_3$ sú po dvoch nesúdeliteľné, teda podľa CRT (1) systém kongruencii $x \equiv p\ (mod\ \lambda_1)$, $x \equiv r\ (mod\ \lambda_2)$, $x \equiv s\ (mod\ \lambda_3)$ má riešenie pre ľubovoľné p, r, s z $\mathbb{Z}$. Potom, aby graf G rozkladal L, tak pre každú trojicu vrcholov nenulového stupňa rôznych farieb a pre každé riešenie daného systému kongruenii m s príslušnými vrcholmi modulo príslušné λ_i, musí slovo a^m patriť do jazyka L. Pre trojicu vrcholov $[3,1],[1,2],[0,3]$ je riešením 28. Ďalšie riešenia sú s ním podľa CRT (1) kongruentné modulo λ a slová tvaru $a^{\lambda k+28}$ ležia v L. Pre trojicu $[4,1],[1,2],[0,3]$ je riešením 4, ostatné sú s ním kongruentné modulo λ a slová tvaru $a^{\lambda k+4}$ taktiež ležia v L. Iné trojice takýchto vrcholov v grafe nemáme, a teda podmienka je splnená, čiže G rozkladá L.

Zároveň pre $\lambda_1, \lambda_2, \lambda_3$ platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z $\{1,2,3\}$, kde $i \neq j$ platí $lcm(\lambda_i, \lambda_j) < \lambda$. Potom vieme podľa grafu G uvedeným spôsobom zostrojiť automaty A_1, A_2, A_3 (Obrázok 3.4) veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$, $(\lambda_3, 0)$, ktoré tvoria efektívny 3-rozklad automatu A. Keďže sme našli takýto efektívny 3-rozklad A, tak potom L je deterministicky efektívne 3-rozložiteľný.

Príklad 8. Teraz zoberme jazyk $L = \{a^{60k+11}, a^{60k+12}, a^{60k+36}, a^{60k+47} \mid k \in \mathbb{N}\}$. Dá sa ukázať, že minimálny automat akceptujúci tento jazyk je UDFA A veľkosti $(60,0)$, teda L je prísne λ-cyklický jazyk pre $\lambda = 60$. Zvolme $\lambda_1 = 6$, $\lambda_2 = 4$, $\lambda_3 = 5$. Zostrojme graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ (Obrázok 3.5). Rovnakým spôsobom ako v Príklade 7 sa dá ukázať, že pre každú trojicu vrcholov nenulového stupňa rôznej

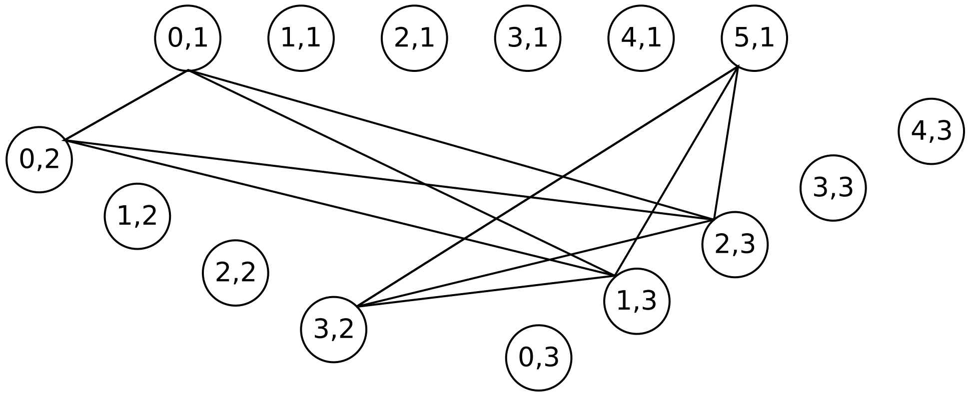


Obr. 3.3: Graf G indukovaný $L = \{a^{30k+4}, a^{30k+28} \mid k \in \mathbb{N}\}, \lambda_1, \lambda_2, \lambda_3$, kde $\lambda_1 = 5$, $\lambda_2 = 3$ a $\lambda_3 = 2$



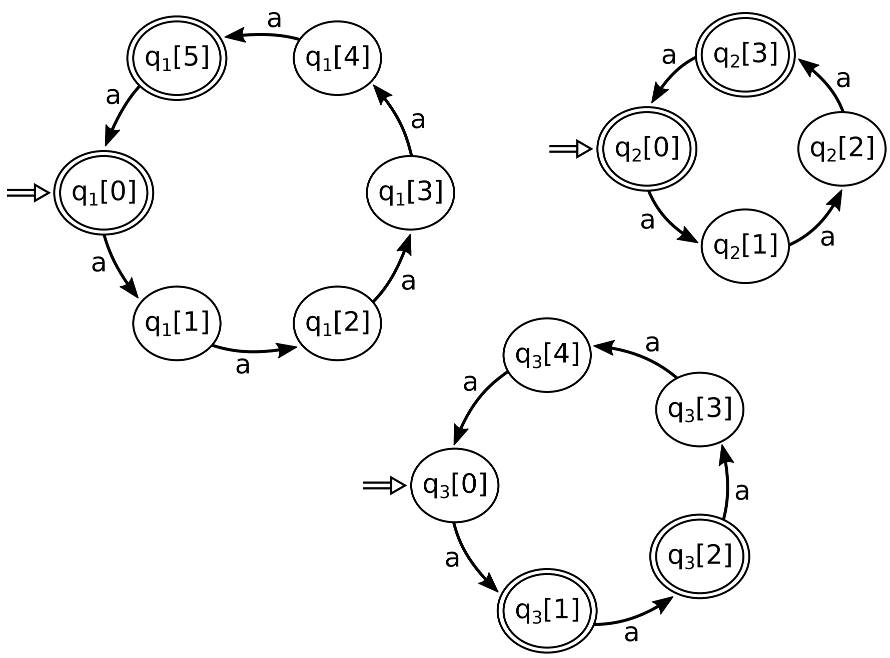
Obr. 3.4: UDFA A_1, A_2, A_3 veľkostí $(6, 0), (4, 0), (5, 0)$ tvoriace rozklad minimálneho UDFA A akceptujúceho jazyk $L = \{a^{60k+11}, a^{60k+12}, a^{60k+36}, a^{60k+47} \mid k \in \mathbb{N}\}$

farby v grafe a pre všetky m kongruentné s príslušnými vrcholmi modulo príslušné λ_i platí, že slovo a^m leží v jazyku. Sú to slová štyroch tvarov, ktoré vytvorili v grafe G štyri trojuholníky. Keď si zoberieme trojicu vrcholov nenulového stupňa rôznej farby netvoriacu trojuholník, dá sa pomocou CRT (1) ukázať, že neexistuje také m, ktoré by bolo kongruentné s danými vrcholmi modulo príslušné λ_i, a teda pre tieto trojice je podmienka triviálne splnená. Pre všetky ostatné trojice daných vrcholov príslušné slová patria do jazyka. Na ukážku zoberme vrcholy $[0, 1], [3, 2], [2, 3]$. Pozrime sa na dvojicu kongruencii $m \equiv 0 \ (mod\ 6)$, $m \equiv 3 \ (mod\ 4)$. Tá má podľa CRT (1) riešenie práve vtedy, keď platí $0 \equiv 3 \ (mod\ gcd(6, 4))$ teda $0 \equiv 3 \ (mod\ 2)$. Čo očividne neplatí, keďže 0 je párna a 3 nepárna. Potom nemôže existovať riešenie ani pre systém všetkých troch kongruencii. Obdobne je to pre ostatné trojice vrcholov nenulového stupňa rôznych farieb, ktoré netvoria trojuholník v grafe. Potom graf G rozkladá jazyk L.



Obr. 3.5: Graf G indukovaný $L = \{a^{60k+11}, a^{60k+12}, a^{60k+36}, a^{60k+47} \mid k \in \mathbb{N}\}, \lambda_1, \lambda_2, \lambda_3$, kde $\lambda_1 = 6$, $\lambda_2 = 4$ a $\lambda_3 = 5$

Zároveň pre $\lambda_1, \lambda_2, \lambda_3$ platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z $\{1, 2, 3\}$, kde $i \neq j$ platí $lcm(\lambda_i, \lambda_j) < \lambda$. Potom vieme podľa grafu G uvedeným spôsobom zostrojiť automaty A_1, A_2, A_3 (Obrázok 3.6) veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$, $(\lambda_3, 0)$, ktoré tvoria efektívny 3-rozklad automatu A. Keďže sme našli takýto efektívny 3-rozklad A, tak potom L je deterministicky efektívne 3-rozložiteľný.



Obr. 3.6: UDFA A_1, A_2, A_3 veľkostí $(6, 0), (4, 0), (5, 0)$ tvoriace rozklad minimálneho UDFA A akceptujúceho jazyk $L = \{a^{60k+11}, a^{60k+12}, a^{60k+36}, a^{60k+47} \mid k \in \mathbb{N}\}$

3.3 Charakterizácia 3-rozložiteľných jazykov

Na základe ukázaných myšlienok môžeme charakterizovať efektívne 3-rozložiteľné prísne λ-cyklické jazyky. Začneme naformulovaním a dokázaním postačujúcej podmienky pre ich efektívnu 3-rozložiteľnosť.

Lema 7. *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Ak existujú $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ také, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre všetky $i, j \in \{1, 2, 3\}$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$ a graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá L, tak L je deterministicky efektívne 3-rozložiteľný.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech UDFA $A = (Q, \{a\}, \delta, q[0], F)$ taký, že $L(A) = L$ je minimálny automat akceptujúci L, A je teda UDFA veľkosti $(\lambda, 0)$ štandardného tvaru (Značenie 1). Označme množinu $\{1, 2, 3\} = I$. Nech $\lambda_1, \lambda_2, \lambda_3$ patria do $\mathbb{N}$, pričom pre ne platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre všetky i, j z I platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. Nech graf $G = (V, E)$ indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá L. Zostrojme UDFA $A_1 = (Q_1, \{a\}, \delta_1, q_1[0], F_1), A_2 = (Q_2, \{a\}, \delta_2, q_2[0], F_2), A_3 = (Q_3, \{a\}, \delta_3, q_3[0], F_3)$ také, že $L = L(A_1) \cap L(A_2) \cap L(A_3)$. Pre každé i z I zostrojme A_i nasledovne:

$Q_i = \{q_i[j] \mid j \in \mathbb{Z}_{\lambda_i}\}$
$(\forall j \in \mathbb{Z}_{\lambda_i})\ \delta_i(q_i[j], a) = q_i[j + 1\ mod\ \lambda_i]$
$F_i = \{q_i[m\ mod\ \lambda_i] \mid m \in \mathbb{Z}_\lambda,\ q[m] \in F\} = \{q_i[n] \mid [n, i] \in V_i'\}$

Najprv dokážme, že $L \subseteq L(A_1) \cap L(A_2) \cap L(A_3)$. Nech w patrí do L, chceme dokázať, že w patrí aj do $L(A_1) \cap L(A_2) \cap L(A_3)$. Keďže w patrí do L, musí byť tvaru $w = a^n$ pre nejaké n z $\mathbb{N}$. Nech $m \equiv n\ (mod\ \lambda)$ a $m < \lambda$. Potom akceptačný výpočet A na w je tvaru $(q[0], w) \vdash_A^* (q[m], \varepsilon)$, kde $q[m]$ je akceptačný stav v A. Výpočet A_i na w je tvaru $(q_i[0], w) \vdash_{A_i}^* (q_i[n\ mod\ \lambda_i], \varepsilon)$ pre každé i z I. Keďže $\lambda = lcm(\lambda_1, \lambda_2, \lambda_3)$, tak pre každé i z I platí, že λ_i / λ. Potom podľa Tvrdenia 2 dostávame, že $n\ mod\ \lambda_i = (n\ mod\ \lambda)\ mod\ \lambda_i$ pre každé i z I. Teda pre každé i z I platí, že $q_i[n\ mod\ \lambda_i] = q_i[(n\ mod\ \lambda)\ mod\ \lambda_i] = q_i[m\ mod\ \lambda_i]$. Keďže $q[m]$ patrí do F, tak potom podľa koštrukcie automatov A_i pre každé i z I platí, že $q_i[m\ mod\ \lambda_i]$ padtrí do F_i, teda je to akceptačný stav automatu A_i. Teda výpočty automatov A_1, A_2, A_3 na slove w sú všetky akceptačné, z čoho dostávame, že w patrí do jazykov $L(A_1), L(A_2), L(A_3)$, a teda patrí aj do ich prieniku $L(A_1) \cap L(A_2) \cap L(A_3)$. Dostávame teda, že $L \subseteq L(A_1) \cap L(A_2) \cap L(A_3)$.

Teraz dokážeme, že platí aj druhá inklúzia, teda $L(A_1) \cap L(A_2) \cap L(A_3) \subseteq L$. Nech w patrí do $L(A_1) \cap L(A_2) \cap L(A_3)$, chceme dokázať, že w patrí aj do L. Keďže w patrí do $L(A_1) \cap L(A_2) \cap L(A_3)$, musí byť tvaru $w = a^n$ pre nejaké n z $\mathbb{N}$. Výpočet A_i na w je tvaru $(q_i[0], w) \vdash_{A_i}^* (q_i[n\ mod\ \lambda_i], \varepsilon)$ pre každé i z I. Keďže pre každé

i z I platí, že w patrí do $L(A_i)$, tak $q_i[n\ mod\ \lambda_i]$ je akceptačný stav automatu A_i pre každé i z I. Nech $r_i \equiv n\ (mod\ \lambda_i)$ a $r_i < \lambda_i$, teda $q_i[n\ mod\ \lambda_i] = q_i[r_i]$ čo je akceptačný stav pre každé i z I. Podľa definície automatov A_i dostávame, že pre každé i z I existuje m_i zo $\mathbb{Z}_\lambda$ také, že $m_i \equiv r_i\ (mod\ \lambda_i)$ a súčasne $q[m_i]$ patrí do F, teda je akceptačný stav automatu A. Potom pre každé i z I slovo a^{m_i} patrí do L, keďže výpočet A na a^{m_i} je tvaru $(q[0], a^{m_i}) \vdash_A^* (q[m_i], \varepsilon)$ a $q[m_i]$ patrí do F. Zoberme a^{m_1}. Nech $s_{12} \equiv m_1\ (mod\ \lambda_2)$, kde $s_{12} < \lambda_2$ a $s_{13} \equiv m_1\ (mod\ \lambda_3)$, kde $s_{13} < \lambda_3$. Ďalej vieme, že $r_1 \equiv m_1\ (mod\ \lambda_1)$ a $r_1 < \lambda_1$. Nasledujúci systém kongruencí

$$\begin{aligned} r_1 = x &\quad (mod\ \lambda_1) \\ s_{12} = x &\quad (mod\ \lambda_2) \\ s_{13} = x &\quad (mod\ \lambda_3) \end{aligned}$$

má teda riešenie, napríklad m_1. Taktiež a^{m_1} patrí do L, potom graf G musí obsahovať hrany $([r_1, 1], [s_{12}, 2])$, $([r_1, 1], [s_{13}, 3])$, $([s_{12}, 2], [s_{13}, 3])$. Analogickú úvahu môžeme uplatniť na slová a^{m_2} a a^{m_3}. Dostávame, že vrcholy $[r_1, 1], [r_2, 2], [r_3, 3]$ sú v grafe G nenulového stupňa a teda platí, že $[r_1, 1]$ patrí do V_1', $[r_2, 2]$ patrí do V_2' a $[r_3, 3]$ patrí do V_3'. Taktiež vieme, že systém kongruencii

$$\begin{aligned} r_1 = x &\quad (mod\ \lambda_1) \\ r_2 = x &\quad (mod\ \lambda_2) \\ r_3 = x &\quad (mod\ \lambda_3) \end{aligned}$$

má riešenie, jedno z jeho riešení je napríklad n. Potom, keďže G rozkladá L musí platiť, že $a^n = w$ patrí do jazyka L. Dostávame teda $L(A_1) \cap L(A_2) \cap L(A_3) \subseteq L$.

Potom $L = L(A_1) \cap L(A_2) \cap L(A_3)$. Zároveň platí, že A_1, A_2, A_3 sú UDFA veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$, $(\lambda_3, 0)$ a pre $\lambda_1, \lambda_2, \lambda_3$ platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z I, kde $i \neq j$ platá, že $lcm(\lambda_i, \lambda_j) < \lambda$. Automaty A_1, A_2, A_3 teda tvoria efektívny 3-rozklad automatu A veľkosti $(\lambda, 0)$, ktorý je minimálny automat akceptujúci jazyk L. Potom L je deterministicky efektívne 3-rozložiteľný. □

Poznámka 12. Všimnime si, že pri dôkaze prvej inklúzie, teda $L(A) \subseteq L(A_1) \cap L(A_2) \cap L(A_3)$, sme vôbec nevyužili, že graf G rozkladá L. Použili sme len vlastnosť, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Táto inklúzia teda platí vo všeobecnosti, pre ľubovoľný prísne λ-cyklický jazyk L, ak existujú $\lambda_1, \lambda_2, \lambda_3$ také, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$, tak existujú λ_i-cyklické jazyky L_i, pre každé i z $\{1, 2, 3\}$ také, že $L \subseteq L_1 \cap L_2 \cap L_3$ a tiež pre minimálny automat A_i akceptujúci jazyk L_i platí, že $sc(A_i) \leq sc(A)$, pre každé i z $\{1, 2, 3\}$, kde A je minimálny automat akceptujúci L.

Poznámka 13. Keďže platí, že ak je jazyk L efektívne 3-rozložiteľný, tak je aj 3-

rozložiteľný, potom táto podmienka je postačujúcou podmienkou aj pre 3-rozložiteľnosť vo všeobecnosti, nie len pre efektívnu. Avšak v tomto všeobecnom prípade už nie je aj nutnou podmienkou.

Teraz ukážeme, že táto podmienka je zároveň aj nutnou podmienkou efektívnej 3-rozložiteľnosti pre prísne λ-cyklické jazyky, a tým dostaneme ich charakterizáciu.

Lema 8. *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Ak L je deterministicky efektívne 3-rozložiteľný, tak existujú $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ také, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé $i, j \in \{1, 2, 3\}$, kde $i \neq j$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$ a graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá L.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Nech L je deterministicky efektívne 3-rozložiteľný a UDFA A je minimálny automat akceptujúci L, teda má veľkosť $(\lambda, 0)$. Označme množinu $\{1, 2, 3\} = I$. Potom existujú UDFA A_1, A_2, A_3 veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$ také, že $L(A_1) \cap L(A_2) \cap L(A_3) = L(A) = L$. Taktiež pre $\lambda_1, \lambda_2, \lambda_3$ platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z I, kde $i \neq j$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. Zostrojme graf $G = (V, E)$ indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ podľa definície a ukážeme, že rozkladá L.

$V = V_1 \cup V_2 \cup V_3$, kde pre všetky $i \in I$ platí $V_i = \{[r, i] \mid r \in \mathbb{Z}_{\lambda_i}\}$
$E = \{([r, i], [p, j]) \in V \times V \mid (\exists [s, k] \in V)\, i \neq j \neq k,\, (\exists m \in \mathbb{N})\, m \equiv r \ (mod\ \lambda_1) \wedge m \equiv p \ (mod\ \lambda_j) \ \wedge \ m \equiv s \ (mod\ \lambda_k) \wedge a^m \in L\}$

Sporom predpokladajme, že G nerozkladá L. Teda existujú vrcholy nenulového stupňa $[r, 1]$ z V_1', $[p, 2]$ z V_2', $[s, 3]$ z V_3' a existuje prirodzené číslo m také, že $m \equiv r \ (mod\ \lambda_1)$, $m \equiv p \ (mod\ \lambda_2)$, $m \equiv s \ (mod\ \lambda_3)$ a a^m nepatrí do jazyka L. Keďže $[r, 1]$ je vrchol nenulového stupňa, v grafe G existuje vrchol $[r_i, i]$, kde $i \neq 1$ a hrana $([r, 1], [r_i, i])$ medzi nimi. Podľa definície hranovej množiny grafu G existuje vrchol $[r_j, j]$, kde $j \neq i$ a tiež $j \neq 1$. Takisto existuje prirodzené číslo n pre ktoré platí, že $n \equiv r \ (mod\ \lambda_1)$, $n \equiv r_i \ (mod\ \lambda_i)$, $n \equiv r_j \ (mod\ \lambda_j)$ a tiež $a^n \in L$. Výpočet A_1 na a^n je tvaru $(q_1[0], a^n) \vdash_{A_1}^* (q_1[r], \varepsilon)$, lebo $m \equiv r \ (mod\ \lambda_1)$ a tiež r je zo $\mathbb{Z}_{\lambda_1}$, teda $r < \lambda_1$. Keďže a^n patrí do $L = L(A) = L(A_1) \cap L(A_2) \cap L(A_3)$, patrí aj do $L(A_1)$, a preto tento výpočet je akceptačný a $q_1[r]$ patrí do F_1, teda je akceptačný stav automatu A_1. Analogicky vieme ukázať, že aj $q_2[p]$ patrí do F_2 a $q_3[s]$ patrí do F_3, teda sú to akceptačné stavy príslušných automatov A_2, A_3.

Výpočet A_1 na slove a^m je tvaru $(q_1[0], a^m) \vdash_{A_1}^* (q_1[m \ mod\ \lambda_1], \varepsilon)$. Ale $m \equiv r \ (mod\ \lambda_1)$, kde $r < \lambda$, a teda výpočet končí v stave $q_1[r]$, čo je akceptačný stav automatu A_1. Teda A_1 akceptuje slovo a^m, čiže a^m patrí do $L(A_1)$. Analogicky vieme ukázať, že slovo a^m je akceptované aj automatmi A_2, A_3, a teda a^m patrí do $L(A_2)$ a tiež a^m patrí do $L(A_3)$. Potom a^m patrí aj do $L(A_1) \cap L(A_2) \cap L(A_3) = L(A) = L$. Čo je spor lebo a^m nepatrí do jazyka L.

Dostávame teda, že graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá L. Zároveň pre $\lambda_1, \lambda_2, \lambda_3$ platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z I, kde $i \neq j$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. □

Spojením týchto dvoch liem (7)(8) dostávame charakterizáciu deterministicky efektívne 3-rozložiteľných prísne λ-cyklických jazykov.

Veta 14. *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. L je deterministicky efektívne 3-rozložiteľný práve vtedy, keď existujú $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}$ také, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé $i, j \in \{1, 2, 3\}$, kde $i \neq j$ platí, že $lcm(\lambda_i, \lambda_j) < \lambda$ a graf G indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá L.*

Kapitola 4

Porovnanie rozkladov

V tejto kapitole ukážeme aký je vzťah medzi triedami efektívne 2-rozložiteľných a efektívne 3-rozložiteľných jazykov. Ďalej budeme skúmať kvalitu 3-rozkladov a následne ju porovnáme s kvalitou 2-rozkladov, keďže zlepšenie kvality rozkladov bol náš prvotný cieľ pri zavedení 3-rozkladov.

4.1 Vzťah 2-rozkladov a 3-rozkladov

Na to, aby sme mohli porovnávať kvalitu efektívnych 2-rozkladov a efektívnych 3-rozkladov pre prísne λ-cyklické jazyky, potrebujeme zistiť aký je vzťah medzi množinami jazykov, ktoré sú deterministicky efektívne 2-rozložiteľné, respektíve 3-rozložiteľné. Ukážeme, že ak je jazyk L efektívne 3-rozložiteľný, tak je aj efektívne 2-rozložiteľný. Teda keď existuje efektívny 3-rozklad minimálneho automatu akceptujúceho nejaký prísne λ-cyklický jazyk L, tak existuje aj jeho efektívny 2-rozklad. Potom môžeme bez problémov porovnať kvalitu jeho rozkladov. Ukáže sa, že opačná implikácia neplatí, a teda, že existuje efektívne 2-rozložieteľný jazyk, ktorý nie je efektívne 3-rozložiteľný. V tomto prípade je teda jeho efektívny 2-rozklad to najlepšie, čo môžeme dosiahnuť, keďže žiadny jeho 3-rozklad neexistuje. Prirodzene ich potom ani nemôžeme porovnávať. Teraz poďme sformulovať a dokázať uvedené myšlienky.

Začnime dôkazom tvrdenia, že každý efektívne 3-rozložiteľný prísne λ-cyklický jazyk L je aj efektívne 2-rozložiteľný. V dôkaze využijeme charakterizácie takýchto jazykov pomocou indukovaných grafov.

Veta 15. *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Potom ak L je deterministicky efektívne 3-rozložiteľný, tak je aj deterministicky efektívne 2-rozložiteľný.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech L je deterministicky efektívne 3-rozložiteľný. Potom existujú $\lambda_1, \lambda_2, \lambda_3$ z $\mathbb{N}$ také, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z $\{1, 2, 3\} = I$, kde $i \neq j$, platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. Zároveň platí, že graf $G = (V, E)$ indukovaný $L, \lambda_1, \lambda_2, \lambda_3$ rozkladá L. Označme $lcm(\lambda_1, \lambda_2) = \lambda_x$ a

$\lambda_3 = \lambda_y$. Platí, že $lcm(\lambda_x, \lambda_y) = lcm(lcm(\lambda_1, \lambda_2), \lambda_2) = lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Taktiež vieme, že $\lambda_x < \lambda$ a $\lambda_y < \lambda$. Zostrojme graf $G_1 = (V_1, E_1)$ indukovaný L, λ_x, λ_y a ukážeme, že G_1 rozkladá L.

Sporom predpokladajme, že G_1 nerozkladá L. Teda existuje dvojica vrcholov rôznej farby $[r_x, 1], [r_y, 2]$ z V_1', čo je množina vrcholov nenulového stupňa, kde r_x je z $\mathbb{Z}_{\lambda_x}$ a r_y z $\mathbb{Z}_{\lambda_y}$, pričom platí, že existuje m z $\mathbb{N}$ také, že platí $m \equiv r_x \ (mod\ \lambda_x)$ a $m \equiv r_y \ (mod\ \lambda_y)$ a tiež hrana $([r_x, 1], [r_y, 2])$ neleží v E_1 hranovej množine grafu G_1. Na základe konštrukcie E_1 vieme, že potom a^m neleží v jazyku L.

Vieme, že $m \equiv r_x \ (mod\ \lambda_x)$, teda $m \equiv r_x \ (mod\ lcm(\lambda_1, \lambda_2))$. Potom podľa Tvrdenia 1 platí aj $m \equiv r_x \ (mod\ \lambda_1)$, respektíve $m \equiv r_x \ (mod\ \lambda_2)$. Zároveň vieme, že $m \equiv r_y \ (mod\ \lambda_y)$ teda $m \equiv r_y \ (mod\ \lambda_3)$.

Nech $r_x \equiv r_1 \ (mod\ \lambda_1)$, kde r_1 patrí do $\mathbb{Z}_{\lambda_1}$. Rovnako nech $r_x \equiv r_2 \ (mod\ \lambda_2)$, kde r_2 patrí do $\mathbb{Z}_{\lambda_2}$. Označme $r_y = r_3$. Teraz zoberme trojicu vrcholov v grafe G $[r_1, 1], [r_2, 2], [r_3, 3]$. Vieme, že platia kongruencie $m \equiv r_1 \ (mod\ \lambda_1)$, $m \equiv r_2 \ (mod\ \lambda_2)$ a $m \equiv r_3 \ (mod\ \lambda_3)$, pričom m je z $\mathbb{N}$. Potom ak sú nami vybrané tri vrcholy v G nenulového stupňa, tak a^m leží v jazyku L, keďže G rozkladá L. Tým dostávame spor a teda G_1 rozkladá L.

Teraz už musíme len dokázať, že vrcholy $[r_1, 1], [r_2, 2], [r_3, 3]$ majú v grafe G nenulový stupeň. Vieme, že vrcholy $[r_x, 1], [r_y, 2]$ majú nenulový stupeň v grafe G_1, teda existujú vrcholy $[r_x^+, 2], [r_y^+, 1]$ vo V_1', teda nenulového stupňa v G_1, kde r_x^+ je zo $\mathbb{Z}_{\lambda_y}$ a r_y^+ zo $\mathbb{Z}_{\lambda_x}$ a navyše existujú hrany $([r_x, 1], [r_x^+, 2]), ([r_y^+, 1], [r_y, 2])$ v E_1 hranovej množine grafu G_1.

Keďže G_1 je indukovaný L, λ_x, λ_y a $([r_x, 1], [r_x^+, 2])$ leží v E_1, tak podľa konštrukcie G_1 vieme, že existuje n_x z $\mathbb{N}$ také, že $n_x \equiv r_x \ (mod\ \lambda_x)$ a $n_x \equiv r_x^+ \ (mod\ \lambda_y)$ a navyše a^{n_x} leží v L. Potom podľa Tvrdenia 1 platí, že $n_x \equiv r_x \ (mod\ \lambda_1)$ a tiež $n_x \equiv r_x \ (mod\ \lambda_2)$. Keďže $r_1 \equiv r_x \ (mod\ \lambda_1)$ a $r_2 \equiv r_x \ (mod\ \lambda_2)$, tak aj $n_x \equiv r_1 \ (mod\ \lambda_1)$ a $n_x \equiv r_2 \ (mod\ \lambda_2)$, kde vieme, že r_1 je zo $\mathbb{Z}_{\lambda_1}$ a r_2 zo $\mathbb{Z}_{\lambda_2}$. Ďalej vieme, že $n_x \equiv r_x^+ \ (mod\ \lambda_3)$ lebo $\lambda_y = \lambda_3$, kde r_x^+ je zo $\mathbb{Z}_{\lambda_3}$. Keďže a^{n_x} leží v L a platí $n_x \equiv r_1 \ (mod\ \lambda_1)$, $n_x \equiv r_2 \ (mod\ \lambda_2)$ a $n_x \equiv r_x^+ \ (mod\ \lambda_3)$, tak potom keďže G je graf indukovaný $L, \lambda_1, \lambda_2, \lambda_3$, tak hrany $([r_1, 1], [r_2, 2])$, $([r_1, 1], [r_x^+, 3])$ a $([r_2, 2], [r_x^+, 3])$ ležia v E hranovej množine grafu G. Teda vrcholy $[r_1, 1], [r_2, 2]$ sú v G nenulového stupňa.

Ešte potrebujeme dokázať, že aj vrchol $[r_3, 3]$ je v G nenulového stupňa. Keďže G_1 je indukovaný L, λ_x, λ_y a $([r_y^+, 1], [r_y, 2])$ leží v E_1, tak podľa konštrukcie G_1 vieme, že existuje n_y z $\mathbb{N}$ také, že $n_y \equiv r_y \ (mod\ \lambda_y)$ a $n_y \equiv r_y^+ \ (mod\ \lambda_x)$ a navyše a^{n_y} leží v L. Potom podľa Tvrdenia 1 platí, že $n_y \equiv r_y^+ \ (mod\ \lambda_1)$ a tiež $n_y \equiv r_y^+ \ (mod\ \lambda_2)$. Nech $r_y^+ \equiv r_1^+ \ (mod\ \lambda_1)$, kde r_1^+ patrí do $\mathbb{Z}_{\lambda_1}$. Rovnako nech $r_y^+ \equiv r_2^+ \ (mod\ \lambda_2)$, kde

r_2^+ patrí do $\mathbb{Z}_{\lambda_2}$. Potom platí aj, že $n_y \equiv r_1^+ \ (mod\ \lambda_1)$ a $n_y \equiv r_2^+ \ (mod\ \lambda_2)$. Ďalej vieme, že $n_y \equiv r_3 \ (mod\ \lambda_3)$ lebo $\lambda_y = \lambda_3$ a $r_y = r_3$, kde r_3 je zo $\mathbb{Z}_{\lambda_3}$. Keďže a^{n_y} leží v L a platí $n_y \equiv r_1^+ \ (mod\ \lambda_1)$, $n_y \equiv r_2^+ \ (mod\ \lambda_2)$ a $n_y \equiv r_3 \ (mod\ \lambda_3)$, tak potom keďže G je graf indukovaný $L, \lambda_1, \lambda_2, \lambda_3$, tak hrany $([r_1^+, 1], [r_2^+, 2])$, $([r_1^+, 1], [r_3, 3])$ a $([r_2^+, 2], [r_3, 3])$ ležia v E hranovej množine grafu G. Teda vrchol $[r_3, 3]$ je v grafe G takisto nenulového stupňa.

Tým sme ukázali, že G_1 rozkladá L. Keďže G_1 je graf indukovaný L, λ_x, λ_y a ďalej platí, že $lcm(\lambda_x, \lambda_y) = \lambda$ a tiež $\lambda_x < \lambda$ a $\lambda_y < \lambda$, tak L je deterministicky 2-rozložiteľný, keďže spĺňa charakterizáciu deterministickej 2-rozložiteľnosti pre prísne λ-cyklické jazyky (5). Potom je aj deterministicky efektívne 2-rozložiteľný. □

Poznámka 14. Uveďme alternatívny spôsob ako dokázať predchádzajúcu vetu (15). Ak prísne λ-cyklický jazyk L je efektívne 3-rozložiteľný, tak existuje 3-rozklad $[A_1, A_2, A_3]$ jeho minimálneho UDFA A. Pričom tieto automaty sú veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$, kde pre každé i, j z $\{1, 2, 3\}$, kde $i \neq j$, platí $lcm(\lambda_i, \lambda_j) < \lambda$ a $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Potom vieme podľa Vety 6 zostrojiť UDFA A_4 veľkosti $(lcm(\lambda_i, \lambda_j), 0)$, ktorý akceptuje prienik $L(A_i)$ a $L(A_j)$. Bez ujmy na všeobecnosti pre $i = 1$ a $j = 2$ dostávame, že $L(A_3) \cap L(A_4) = L$ a aj $lcm(\lambda_3, lcm(\lambda_1, \lambda_2)) = \lambda$, $lcm(\lambda_1, \lambda_2) < \lambda$ a $\lambda_3 < \lambda$. Teda sme našli efektívny 2-rozklad $[A_3, A_4]$ UDFA A, ktorý je minimálny akceptujúci L, a teda L je deterministicky efektívne 2-rozložiteľný.

Z alternatívneho dôkazu uvedeného v Poznámke 14 vyplýva aj další vzťah efektívnych 3-rozkladov a 2-rozkladov, ktorý zachycuje nasledujúce tvrdenie.

Veta 16. *Nech L je prísne λ-cyklický jazyk pre nejaké $\lambda \in \mathbb{N}$. Potom ak L je deterministicky efektívne 3-rozložiteľný, tak existuje efektívny 2-rozklad $[A_1, A_2]$ jeho minimálneho automatu A taký, že A_1 je znovu efektívne 2-rozložiteľný a existuje jeho efektívny 2-rozklad $[B_1, B_2]$ pre ktorý platí, že $[A_2, B_1, B_2]$ je efektívny 3-rozklad A.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech A je minimálny automat akceptujúci L, teda je veľkosti $(\lambda, 0)$. Ak L je efektívne 3-rozložiteľný, tak existuje 3-rozklad $[B_1, B_2, B_3]$ automatu A, pričom automaty B_1, B_2, B_3 sú veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$, kde pre každé i, j z $\{1, 2, 3\}$, kde $i \neq j$, platí $lcm(\lambda_i, \lambda_j) < \lambda$ a zároveň platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Podľa Vety 6 vieme zostrojiť UDFA A_1 veľkosti $(lcm(\lambda_1, \lambda_2), 0)$, ktorý akceptuje prienik $L(B_1) \cap L(B_2)$. Pre automaty A_1 a B_3 platí, že $L(A_1) \cap L(B_3) = L$ a aj $lcm(\lambda_3, lcm(\lambda_1, \lambda_2)) = lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$, $lcm(\lambda_1, \lambda_2) < \lambda$, $\lambda_3 < \lambda$, keďže aj $lcm(\lambda_1, \lambda_3) < \lambda$. Teda $[A_1, B_3]$ je efektívny 2-rozklad UDFA A.

Ak by platilo $\lambda_1 = lcm(\lambda_1, \lambda_2)$, tak potom dostávame $\lambda = lcm(\lambda_1, \lambda_2, \lambda_3) = lcm(lcm(\lambda_1, \lambda_2), \lambda_3) = lcm(\lambda_1, \lambda_3) < \lambda$. Dostávame $\lambda < \lambda$, čo nemôže nastať, a teda $\lambda_1 < lcm(\lambda_1, \lambda_2)$. Analogicky musí platiť aj, že $\lambda_2 < lcm(\lambda_1, \lambda_2)$. Potom keďže platí

$L(A_1) = L(B_1) \cap L(B_2)$ a A_1 je veľkosti $(lcm(\lambda_1, \lambda_2), 0)$, tak B_1, B_2 tvoria efektívny 2-rozklad A_1 a teda A_1 je efektívne 2-rozložiteľný.

Našli sme teda efektívny 2-rozklad $[A_1, B_3]$ automatu A, ktorý je minimálny akceptujúci L, pre ktorý platí, že A_1 je znovu efektívne 2-rozložiteľný. A našli sme aj efektívny 2-rozklad $[B_1, B_2]$ automatu A_1, pre ktorý platí, že $[B_1, B_2, B_3]$ je efektívny 3-rozklad minimálneho automatu A akceptujúceho L. $\square$

Teraz sa vrátime k porovnaniu množín efektívne 2-rozložiteľných a efektívne 3-rozložiteľných jazykov a ukážeme, že existuje efektívne 2-rozložiteľný jazyk L, ktorý nie je efektívne 3-rozložiteľný. Ako sme si mohli všimnúť, podmienky na efektívnu 3-rozložiteľnosť požadujú aby λ, teda dĺžka cyklu daného minimálneho automatu akceptujúceho L, bola dosť veľká. Pre príliš malé λ neexistujú vhodné $\lambda_1, \lambda_2, \lambda_3$, ktoré by spĺňali podmienky z definície. Práve na tejto myšlienke postavíme dôkaz nasledujúceho tvrdenia, v ktorom využijeme dobre známy príklad 2-rozložiteľného jazyka pre deliteľnosť šiestimi.

Veta 17. *Existuje prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$ taký, že L je efektívne 2-rozložiteľný, ale L nie je efektívne 3-rozložiteľný.*

Dôkaz. Zoberme jazyk $L = \{a^{6k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 6$. Minimálny automat akceptujúci L je UDFA A veľkosti $(6, 0)$ štandardného tvaru (Značenie 1) kde $F = \{q[0]\}$.

Zoberme UDFA A_1, A_2 veľkostí $(2, 0)$, $(3, 0)$ štandardného tvaru (Značenie 1) kde $F_1 = \{q_1[0]\}$ a $F_2 = \{q_2[0]\}$. Platí, že $lcm(2, 3) = 6$ a tiež $sc(A_1) = 2 < 6$ a $sc(A_2) = 3 < 6$, teda platí, že $L(A_1) \cap L(A_2) = L$. Potom A_1, A_2 tvoria efektívny 2-rozklad A, čiže A je efektívne 2-rozložiteľný. Potom teda aj L je efektívne 2-rozložiteľný.

Ak $[B_1, B_2, B_3]$ je efektívny 3-rozklad A, tak musí platiť, že B_1, B_2, B_3 sú UDFA veľkostí $(\lambda_1, 0)$, $(\lambda_2, 0)$, $(\lambda_3, 0)$, ďalej $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$ a pre každé i, j z $\{1, 2, 3\}$, kde $i \neq j$, platí, že $lcm(\lambda_i, \lambda_j) < \lambda$. Okrem toho musí samozrejme platiť aj $L(B_1) \cap L(B_2) \cap L(B_3) = L$. Potom taktiež platí, že λ_1/λ, λ_2/λ a aj λ_3/λ. Keďže $\lambda = 6 = 2 \cdot 3$, kde 2 aj 3 sú prvočísla, tak λ_1, λ_2 aj λ_3 môžu nadobúdať iba hodnoty $1, 2, 3, 6$. Ale ak $\lambda_i = 6$ pre nejaké i z $\{1, 2, 3\}$, tak potom $\lambda_i = \lambda$, čo nemôže nastať, lebo $lcm(\lambda_i, \lambda_j) < \lambda$ pre nejaké j z $\{1, 2, 3\}$, kde $j \neq i$. Taktiež ak $\lambda_i = 1$ pre nejaké i z $\{1, 2, 3\}$, tak potom $lcm(\lambda_i, \lambda_j) = \lambda_j$ pre nejaké j z $\{1, 2, 3\}$, kde $j \neq i$. Z toho dostaneme, že by malo platiť $\lambda = lcm(\lambda_1, \lambda_2, \lambda_3) = lcm(lcm(\lambda_j, \lambda_i), \lambda_k) = lcm(\lambda_j, \lambda_k) < \lambda$ pre k z $\{1, 2, 3\}$, kde $k \neq i$ a tiež $k \neq j$. Teda by malo platiť $\lambda < \lambda$, čo nemôže nastať a preto $\lambda_i \neq 1$ pre žiadne i. Teda $\lambda_1, \lambda_2, \lambda_3$ môžu nadobudnúť iba hodnoty 2 a 3.

Zároveň ak $\lambda_i = \lambda_j$ kde $i \neq j$, i, j sú z $\{1, 2, 3\}$, tak $lcm(\lambda_i, \lambda_j) = \lambda_i$. Tým sa dostávame do analogickej situácie, ktorá nemôže platiť, a teda $\lambda_i \neq \lambda_j$ pre žiadne i, j.

Potom ale hodnoty, ktoré by mohli $\lambda_1, \lambda_2, \lambda_3$ nadobúdať nemôžu existovať a teda nemôže existovať ani efektívny 3-rozklad A. Čiže L nie je efektívne 3-rozložiteľný. $\square$

4.2 Sum-kvalita 3-rozkladov

Keďže sme zaviedli efektívny 3-rozklad, aby sme získali kvalitnejšie rozklady v porovnaní s 2-rozkladmi, poďme sa teraz pozrieť ako kvalitné efektívne 3-rozklady naozaj sú. Následne ich môžeme porovnať s efektívnymi 2-rozkladmi, ktoré ako sme dokázali, vždy existujú, ak je daný jazyk efektívne 3-rozložiteľný. Opäť sa na ich kvalitu budeme pozerať prostredníctvom *sum*-kvality, teda budeme brať do úvahy súčet stavov nových automatov tvoriacich 3-rozklad. Znovu ukážeme hornú a dolnú hranicu *sum*-kvality týchto rozkladov a ako ďaleko sa od nej budú pohybovať.

Lema 9. *Nech $[A_1, A_2, A_3]$ je efektívny 3-rozklad minimálneho automatu A pre nejaký λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$. Potom $\lceil 3\sqrt[3]{\lambda} \rceil \leq sum([A_1, A_2, A_3])$.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech A je minimálny automat akceptujúci L. Nech $[A_1, A_2, A_3]$ je efektívny 3-rozklad A. Potom automaty A_1, A_2, A_3 sú veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$ a platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Zároveň platí $lcm(\lambda_1, \lambda_2) < \lambda$, $lcm(\lambda_1, \lambda_3) < \lambda$ a $lcm(\lambda_2, \lambda_3) < \lambda$. Z toho vyplýva, že λ_1/λ, λ_2/λ, λ_3/λ a zároveň $\lambda_1 < \lambda$, $\lambda_2 < \lambda$ a tiež $\lambda_3 < \lambda$. Označme $x = \sqrt[3]{\lambda}$ a $g = gcd(\lambda_1, \lambda_2, \lambda_3)$. Vieme, že $x^3 = lcm(\lambda_1, \lambda_2, \lambda_3)$. Ukážeme, že platí $3x \leq \lambda_1 + \lambda_2 + \lambda_3$. Dostávame teda

$$\begin{aligned} \lambda_1 + \lambda_2 + \lambda_3 &\geq 3x \\ \lambda_1 + \lambda_2 + \lambda_3 - 3x &\geq 0 \\ \lambda_1 + \lambda_2 + \lambda_3 - 3\sqrt[3]{lcm(\lambda_1, \lambda_2, \lambda_3)} &\geq 0 \\ \lambda_1 + \lambda_2 + \lambda_3 - 3\frac{\sqrt[3]{\lambda_1\lambda_2\lambda_3}}{\sqrt[3]{g}} &\geq 0 \end{aligned}$$

Keďže $g \geq 1$, potom aj $\sqrt[3]{g} \geq 1$. Zároveň platí $\sqrt[3]{\lambda_1\lambda_2\lambda_3} > 0$, z čoho dostávame

$$\frac{\sqrt[3]{\lambda_1\lambda_2\lambda_3}}{\sqrt[3]{g}} \leq \sqrt[3]{\lambda_1\lambda_2\lambda_3}$$

Potom zjavne

$$\lambda_1 + \lambda_2 + \lambda_3 - 3\frac{\sqrt[3]{\lambda_1\lambda_2\lambda_3}}{\sqrt[3]{g}} \geq \lambda_1 + \lambda_2 + \lambda_3 - 3\sqrt[3]{\lambda_1\lambda_2\lambda_3}$$

A teda nám stačí dokázať, že

$$\lambda_1 + \lambda_2 + \lambda_3 - 3\sqrt[3]{\lambda_1\lambda_2\lambda_3} \geq 0$$

Ale táto nerovnosť priamo vyplýva z AM-GM nerovnosti (3), keďže λ_i je z $\mathbb{N}$ pre každé i z $\{1, 2, 3\}$.

Tým dostávame, že platí $3\sqrt[3]{\lambda} \leq \lambda_1+\lambda_2+\lambda_3$. Potom platí aj $\lceil 3\sqrt[3]{\lambda}\rceil \leq \lambda_1+\lambda_2+\lambda_3$. Zároveň vieme, že $sum([A_1, A_2, A_3]) = sc(A_1) + sc(A_2) + sc(A_3) = \lambda_1 + \lambda_2 + \lambda_3$. Z toho teda dostávame, že $\lceil 3\sqrt[3]{\lambda}\rceil \leq sum([A_1, A_2, A_3])$. □

Lema 10. *Nech $[A_1, A_2, A_3]$ je efektívny 3-rozklad minimálneho automatu A pre nejaký prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$. Potom $sum([A_1, A_2, A_3]) \leq \frac{1}{3}\lambda$.*

Dôkaz. Nech L je prísne λ-cyklický jazyk pre nejaké λ z $\mathbb{N}$. Nech A je minimálny automat akceptujúci L. Nech $[A_1, A_2, A_3]$ je efektívny 3-rozklad A. Potom automaty A_1, A_2, A_3 sú veľkostí $(\lambda_1, 0), (\lambda_2, 0), (\lambda_3, 0)$ a platí, že $lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Zároveň platí $lcm(\lambda_1, \lambda_2) < \lambda$, $lcm(\lambda_1, \lambda_3) < \lambda$ a $lcm(\lambda_2, \lambda_3) < \lambda$.

Platí, že $lcm(lcm(\lambda_1, \lambda_2), lcm(\lambda_1, \lambda_3), lcm(\lambda_2, \lambda_3)) = lcm(\lambda_1, \lambda_2, \lambda_1, \lambda_3, \lambda_2, \lambda_3) = lcm(\lambda_1, \lambda_2, \lambda_3) = \lambda$. Z toho vyplýva, že $lcm(\lambda_1, \lambda_2)/\lambda$, $lcm(\lambda_2, \lambda_3)/\lambda$ a tiež $lcm(\lambda_1, \lambda_3)/\lambda$. Dostávame, že $\lambda = lcm(\lambda_1, \lambda_2)\alpha$ pre α z $\mathbb{N}$, $\alpha > 1$. Rovnako $\lambda = lcm(\lambda_2, \lambda_3)\beta$ pre β z $\mathbb{N}$, $\beta > 1$ a tiež $\lambda = lcm(\lambda_1, \lambda_3)\gamma$ pre γ z $\mathbb{N}$, $\gamma > 1$. Ak by platilo, že $gcd(\alpha, \beta, \gamma) > 1$, označme ho g, potom dostávame

$$\alpha lcm(\lambda_1, \lambda_2) = \beta lcm(\lambda_2, \lambda_3) = \gamma lcm(\lambda_1, \lambda_3)$$
$$\frac{\alpha lcm(\lambda_1, \lambda_2)}{g} = \frac{\beta lcm(\lambda_2, \lambda_3)}{g} = \frac{\gamma lcm(\lambda_1, \lambda_3)}{g} = l$$

Pre l platí, že je z $\mathbb{N}$, $l < \lambda$ a tiež λ_1/l, λ_2/l a λ_3/l. Teda l je spoločný násobok $\lambda_1, \lambda_2, \lambda_3$ menší ako ten najmenší. Potom musí platiť, že α, β, γ sú ako trojica nesúdeliteľné, teda $gcd(\alpha, \beta, \gamma) = 1$.

Zároveň zrejme platí, že $\lambda_1/lcm(\lambda_1, \lambda_2)$ aj $\lambda_1/lcm(\lambda_1, \lambda_3)$. Rovnako aj $\lambda_2/lcm(\lambda_1, \lambda_2)$, aj $\lambda_2/lcm(\lambda_2, \lambda_3)$ a tiež $\lambda_3/lcm(\lambda_1, \lambda_3)$ aj $\lambda_3/lcm(\lambda_2, \lambda_3)$. Teda $lcm(\lambda_1, \lambda_2) = \alpha_1\lambda_1$ pre α_1 z $\mathbb{N}$ a tiež $lcm(\lambda_1, \lambda_2) = \alpha_2\lambda_2$ pre α_2 z $\mathbb{N}$. Ďalej rovnako platí $lcm(\lambda_2, \lambda_3) = \beta_2\lambda_2$ pre β_2 z $\mathbb{N}$ a $lcm(\lambda_2, \lambda_3) = \beta_3\lambda_3$ pre β_3 z $\mathbb{N}$ a aj $lcm(\lambda_1, \lambda_3) = \gamma_1\lambda_1$ pre γ_1 z $\mathbb{N}$ a $lcm(\lambda_1, \lambda_3) = \gamma_3\lambda_3$ pre γ_3 z $\mathbb{N}$. Potom dostávame

$$\begin{array}{ccc} \lambda_1\alpha_1\alpha = \lambda & \lambda_2\alpha_2\alpha = \lambda & \lambda_3\gamma_3\gamma = \lambda \\ \lambda_1\gamma_1\gamma = \lambda & \lambda_2\beta_2\beta = \lambda & \lambda_3\beta_3\beta = \lambda \end{array}$$

Ak by platilo, že $lcm(\alpha,\gamma) > 1$, označme ho g_1 tak dostávame

$$\lambda_1\alpha_1\alpha = \lambda \qquad \lambda_2\alpha_2\alpha = \lambda \qquad \lambda_3\gamma_3\gamma = \lambda$$
$$\frac{lam_1\alpha_1\alpha}{g_1} = l_1 \qquad \frac{\lambda_2\alpha_2\alpha}{g_1} = l_1 \qquad \frac{\lambda_3\gamma_3\gamma}{g_1} = l_1$$

Pre l_1 platí, že je z $\mathbb{N}$, $l_1 < \lambda$ a tiež λ_1/l_1, λ_2/l_1 a λ_3/l_1. Teda l_1 je spoločný násobok $\lambda_1, \lambda_2, \lambda_3$ menší ako ten najmenší. Potom musí platiť, že α, γ sú nesúdeliteľné, teda $gcd(\alpha,\gamma) = 1$. Anologickou úvahou dospejeme k tomu, že aj α, β a sú nesúdeliteľné, teda $gcd(\alpha,\beta) = 1$ a rovnako aj β, γ sú nesúdeliteľné, teda $gcd(\beta,\gamma) = 1$. Ale platí aj

$$\alpha_1\alpha = \gamma_1\gamma \qquad \alpha_2\alpha = \beta_2\beta \qquad \gamma_3\gamma = \beta_3\beta$$

Potom keďže $gcd(\alpha,\gamma) = 1$ tak zjavne γ/α_1 a tiež α/γ_1. Tým dostávame, že platí $\lambda = \lambda_1\psi_1\gamma\alpha$ kde $\alpha_1 = \psi\gamma$ a ψ je z $\mathbb{N}$. Uplatnením analogickej úvahy dospejeme k

$$\lambda = \lambda_1\psi_1\alpha\gamma \qquad \lambda = \lambda_2\psi_2\alpha\beta \qquad \lambda = \lambda_3\psi_3\beta\gamma$$

kde vieme, že ψ_2, ψ_3 sú tiež z $\mathbb{N}$ a ďalej, že α, β, γ sú po dvoch nesúdeliteľné. Keďže $\alpha \geq 2$ a $gcd(\alpha,\beta) = 1$ tak najmešia možná hodnota pre β je 3, teda $\beta \geq 3$. Ďalej keďže $gcd(\alpha,\gamma) = 1$ a tiež $gcd(\beta,\gamma) = 1$, tak najmenšia možná hodnota pre γ je 5, teda $\gamma \geq 5$. Z toho dostávame

$$2\cdot 5\cdot\lambda_1 \leq \alpha\gamma\lambda_1 \leq \lambda \quad\rightsquigarrow\quad 2\cdot 5\cdot\lambda_1 \leq \lambda \quad\rightsquigarrow\quad \lambda_1 \leq \frac{1}{2\cdot 5}\lambda$$
$$2\cdot 3\cdot\lambda_2 \leq \alpha\beta\lambda_2 \leq \lambda \quad\rightsquigarrow\quad 2\cdot 3\cdot\lambda_2 \leq \lambda \quad\rightsquigarrow\quad \lambda_2 \leq \frac{1}{2\cdot 3}\lambda$$
$$3\cdot 5\cdot\lambda_3 \leq \beta\gamma\lambda_3 \leq \lambda \quad\rightsquigarrow\quad 3\cdot 5\cdot\lambda_3 \leq \lambda \quad\rightsquigarrow\quad \lambda_3 \leq \frac{1}{3\cdot 5}\lambda$$

Potom platí

$$\lambda_1+\lambda_2+\lambda_3 \leq \frac{1}{2\cdot 5}\lambda+\frac{1}{2\cdot 3}\lambda+\frac{1}{3\cdot 5}\lambda = \left(\frac{1}{2\cdot 5}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 5}\right)\lambda = \frac{3+5+2}{30}\lambda = \frac{1}{3}\lambda$$

Zároveň vieme, že $sum([A_1, A_2, A_3]) = sc(A_1) + sc(A_2) + sc(A_3) = \lambda_1 + \lambda_2 + \lambda_3$. Z toho dostávame, že $sum([A_1, A_2, A_3]) \leq \frac{1}{3}\lambda$. □

Poznámka 15. Všimnime si, že dôkazy dolného (18) a horného (10) odhadu *sum*-kvality efektívnych 3-rozkladov využívajú rovnaké myšlienky ako dôkazy dolného (5) a horného (6) odhadu *sum*-kvality efektívnych 2-rozkladov. Obdobné myšlienky by sa dali pre vhodne zadefinovaný efektívny n-rozklad využiť aj pri dôkaze horného a dolného odhadu jeho kvality, kde berieme n > 3.

Spojením týchto dvoch liem (18)(10) dostávame ohraničenie *sum*-kvality efektívnych 3-rozkladov pre prísne λ-cyklické jazyky.

Veta 18. *Nech* $[A_1, A_2, A_3]$ *je efektívny 3-rozklad minimálneho automatu* A *pre nejaký* λ*-cyklický jazyk* L *pre nejaké* $\lambda \in \mathbb{N}$*. Potom* $\lceil 3\sqrt[3]{\lambda} \rceil \leq sum([A_1, A_2, A_3]) \leq \frac{1}{3}\lambda$.

Podobne ako pri odhade hraníc *sum*-kvality pre efektívne 2-rozklady, aj teraz nás zaujíma ako presne sme odhadli *sum*-kvalitu efektívnych 3-rozkladov. Opäť sa nám podarí ukázať, že naše odhady sú presné tak, že nájdemne jazyky a efektívne 3-rozklady ich minimálnych automatov, ktorých *sum*-kvalita sa bude presne rovnať nami dokázaným hraniciam.

Veta 19. *Existuje prísne* λ*-cyklický jazyk* L *pre nejaké* $\lambda \in \mathbb{N}$ *a efektívny 3-rozklad* $[A_1, A_2, A_3]$ *jeho minimálneho automatu* A *taký, že* $sum([A_1, A_2, A_3]) = \lceil 3\sqrt[3]{\lambda} \rceil$.

Dôkaz. Zoberme jazyk $L = \{a^{60k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 60$ a minimálny automat akceptujúci L je UDFA A veľkosti $(60, 0)$ štandardného tvaru (Značenie 1), kde $F = \{q[0]\}$. Zoberme UDFA A_1, A_2, A_3 veľkostí $(5, 0), (3, 0)$, $(4, 0)$ štandardného tvaru (Značenie 1) kde $F_1 = \{q_1[0]\}$, $F_2 = \{q_2[0]\}$ a $F_3 = \{q_3[0]\}$. Platí, že $lcm(5, 3, 4) = 60$. Potom pre automaty A_1, A_2, A_3 platí, že $L(A_1) \cap L(A_2) \cap L(A_3) = L$ a tiež $lcm(5, 3) = 15 < 60$, $lcm(5, 4) = 20 < 60$ a $lcm(3, 4) = 12 < 60$. Teda automaty A_1, A_2, A_3 tvoria efektívny 3-rozklad automatu A, ktorý je minimálny akceptujúci L.

Platí, že $sum([A_1, A_2, A_3]) = sc(A_1) + sc(A_2) + sc(A_3) = 5 + 3 + 4 = 12$. Zároveň platí, že $\lceil 3\sqrt[3]{60} \rceil = \lceil 11,745 \rceil = 12$. Našli sme teda prísne λ-cyklický jazyk L a efektívny 3-rozklad $[A_1, A_2, A_3]$ jeho minimálneho automatu A, kde platí $sum([A_1, A_2, A_3]) = \lceil 3\sqrt[3]{\lambda} \rceil$. □

Veta 20. *Existuje prísne* λ*-cyklický jazyk* L *pre nejaké* $\lambda \in \mathbb{N}$ *a efektívny 3-rozklad* $[A_1, A_2, A_3]$ *jeho minimálneho automatu* A *taký, že* $sum([A_1, A_2, A_3]) = \frac{1}{3}\lambda$.

Dôkaz. Znovu zoberme jazyk $L = \{a^{60k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 60$ a minimálny automat akceptujúci L je UDFA A veľkosti $(60, 0)$ štandardného tvaru (Značenie 1), kde $F = \{q[0]\}$. Zoberme UDFA A_1, A_2, A_3 veľkostí $(10, 0), (6, 0)$, $(4, 0)$ štandardného tvaru (Značenie 1) kde $F_1 = \{q_1[0]\}$, $F_2 = \{q_2[0]\}$ a $F_3 = \{q_3[0]\}$. Platí, že $lcm(10, 6, 4) = 60$. Potom dostávame, že $L(A_1) \cap L(A_2) \cap L(A_3) = L$ a tiež $lcm(10, 6) = 30 < 60$, $lcm(10, 4) = 20 < 60$ a $lcm(6, 4) = 12 < 60$. Teda automaty A_1, A_2, A_3 tvoria efektívny 3-rozklad automatu A, ktorý je minimálny akceptujúci L.

Platí, že $sum([A_1, A_2, A_3]) = sc(A_1) + sc(A_2) + sc(A_3) = 10 + 6 + 4 = 20$. Zároveň platí, že $\frac{1}{3}60 = 20$. Našli sme teda prísne λ-cyklický jazyk L a efektívny 3-rozklad $[A_1, A_2, A_3]$ jeho minimálneho automatu A, kde platí $sum([A_1, A_2, A_3]) = \frac{1}{3}\lambda$. □

4.3 Porovnanie sum-kvality rozkladov

Teraz môžeme porovnať *sum*-kvalitu efektívnych 2-rozkladov a 3-rozkladov pre prísne λ-cyklické jazyky. V súlade s našimi očakávaniami sa ukáže, že 3-rozklady sú vo všeobecnosti kvalitnejšie ako 2-rozklady. Avšak neplatí to pre všetky rozklady všetkých jazykov a ukáže sa, že niektoré 2-rozklady môžu byť lepšie ako niektoré 3-rozklady.

Veta 21. *Existuje efektívne 3-rozložiteľný prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$ taký, že pre každý efektívny 3-rozklad $[A_1, A_2, A_3]$ a každý efektívny 2-rozklad $[B_1, B_2]$ jeho minimálneho automatu A platí, že $sum([A_1, A_2, A_3]) < sum([B_1, B_2])$.*

Dôkaz. Zoberme jazyk $L = \{a^{30k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 30$ a minimálny automat akceptujúci L je UDFA A veľkosti $(30, 0)$ štandardného tvaru (Značenie 1) kde $F = \{q[0]\}$. Pre každý jeho efektívny 3-rozklad $[A_1, A_2, A_3]$ platí, že $sum([A_1, A_2, A_3]) \leq \frac{1}{3}30 = 10$. Zároveň pre každý jeho efektívny 2-rozklad $[B_1, B_2]$ platí, že $sum([B_1, B_2]) \geq \lceil 2\sqrt{30} \rceil = \lceil 2 \cdot 5,477 \rceil = 11$. Teda pre každý efektívny 3-rozklad $[A_1, A_2, A_3]$ a každý efektívny 2-rozklad $[B_1, B_2]$ automatu A platí, že $sum([A_1, A_2, A_3]) < sum([B_1, B_2])$. Teraz už potrebujeme len ukázať, že L je efektívne 3-rozložiteľný.

Zoberme UDFA A_1, A_2, A_3 veľkostí $(2, 0)$, $(3, 0)$, $(5, 0)$ štandardného tvaru (Značenie 1) kde $F_1 = \{q_1[0]\}$, $F_2 = \{q_2[0]\}$ a $F_3 = \{q_3[0]\}$. Platí, že $lcm(2, 3, 5) = 30$, potom pre automaty A_1, A_2, A_3 platí, že $L(A_1) \cap L(A_2) \cap L(A_3) = L$. Tiež platí, že $lcm(2, 3) = 6 < 30$, $lcm(2, 5) = 10 < 30$ a aj $lcm(3, 5) = 15 < 30$. Teda automaty A_1, A_2, A_3 tvoria efektívny 3-rozklad automatu A, ktorý je minimálny akceptujúci L. Potom L je efektívne 3-rozložiteľný. □

Veta 22. *Existuje efektívne 3-rozložiteľný prísne λ-cyklický jazyk L pre nejaké $\lambda \in \mathbb{N}$ a efektívny 3-rozklad $[A_1, A_2, A_3]$ jeho minimálneho automatu A taký, že pre každý efektívny 2-rozklad $[B_1, B_2]$ automatu A platí, že $sum([A_1, A_2, A_3]) < sum([B_1, B_2])$ a zároveň existuje efektívny 3-rozklad $[C_1, C_2, C_3]$ automatu A a efektívny 2-rozklad $[D_1, D_2]$ automatu A, pre ktoré platí, že $sum([C_1, C_2, C_3]) > sum([D_1, D_2])$.*

Dôkaz. Zoberme jazyk $L = \{a^{60k} \mid k \in \mathbb{N}\}$. L je prísne λ-cyklický jazyk pre $\lambda = 60$ a minimálny automat akceptujúci L je UDFA A veľkosti $(60, 0)$ štandardného tvaru (Značenie 1) kde $F = \{q[0]\}$.

Zoberme UDFA A_1, A_2, A_3 veľkostí $(4, 0)$, $(3, 0)$, $(5, 0)$ štandardného tvaru (Značenie 1), kde $F_1 = \{q_1[0]\}$, $F_2 = \{q_2[0]\}$ a $F_3 = \{q_3[0]\}$. Platí, že $lcm(4, 3, 5) = 60$, potom pre automaty A_1, A_2, A_3 platí, že $L(A_1) \cap L(A_2) \cap L(A_3) = L$. Tiež platí, že $lcm(4, 3) = 12 < 60$, $lcm(4, 5) = 20 < 60$ a aj $lcm(3, 5) = 15 < 60$. Teda automaty

A_1, A_2, A_3 tvoria efektívny 3-rozklad automatu A, ktorý je minimálny akceptujúci L. Potom L je efektívne 3-rozložiteľný.

Zároveň vieme, že pre každý efektívny 2-rozklad $[B_1, B_2]$ automatu A platí, že $sum([B_1, B_2]) \geq \lceil 2\sqrt{60} \rceil = \lceil 2 \cdot 7,746 \rceil = 16$. K tomu platí, že $sum([A_1, A_2, A_3]) = sc(A_1) + sc(A_2) + sc(A_3) = 12$ Teda pre efektívny 3-rozklad $[A_1, A_2, A_3]$ a každý efektívny 2-rozklad $[B_1, B_2]$ automatu A platí, že $sum([A_1, A_2, A_3]) < sum([B_1, B_2])$.

Teraz zoberme UDFA C_1, C_2, C_3 veľkostí $(4, 0)$, $(6, 0), (10, 0)$ štandardného tvaru (Značenie 1), kde $F_1 = \{q_1[0]\}$, $F_2 = \{q_2[0]\}$ a $F_3 = \{q_3[0]\}$. Platí, že $lcm(4, 6, 10) = 60$, potom pre automaty C_1, C_2, C_3 platí, že $L(C_1) \cap L(C_2) \cap L(C_3) = L$. Tiež platí, že $lcm(4, 6) = 12 < 60$, $lcm(4, 10) = 20 < 60$ a aj $lcm(6, 10) = 30 < 60$. Teda automaty C_1, C_2, C_3 tvoria efektívny 3-rozklad automatu A a zároveň platí, že $sum([C_1, C_2, C_3]) = 20$

Teraz zoberme UDFA D_1, D_2 veľkostí $(5, 0)$, $(12, 0)$ štandardného tvaru (Značenie 1), kde $F_1 = \{q_1[0]\}$ a $F_2 = \{q_2[0]\}$. Platí, že $lcm(5, 12) = 60$, potom pre automaty D_1, D_2 platí, že $L(D_1) \cap L(D_2) = L$. Keďže $sc(D_1) = 5 < 60$ a $sc(D_2) = 12 < 60$, automaty D_1, D_2 tvoria efektívny 2-rozklad automatu A a zároveň platí, že $sum([D_1, D_2]) = 17$

Našli sme teda taký efektívny 3-rozklad $[C_1, C_2, C_3]$ a efektívny 2-rozklad $[D_1, D_2]$ automatu A, že pre ne platí $sum([D_1, D_2]) < sum([C_1, C_2, C_3])$. □

Poznámka 16. Keď sa zamyslíme, tento výsledok je vlastne celkom prirodzený, keďže intervaly, z ktorých nadobúdajú hodnoty sum-kvality efektívnych 2-rozkladov a efektívnych 3-rozkladov minimálnych automatov akceptujúcich nejaký λ-cyklický jazyk, sa prekrývajú pre väčšinu prípustných hodnôt λ. Riešením ľahkej nerovnice sa dá ukázať, že sa prekrývajú pre každé $\lambda > 36$, čo je v súlade s našimi výsledkami. Navyše jediné možné $\lambda \leq 36$ také, aby daný prísne λ-cyklický jazyk bol 3-rozložiteľný je práve hodnota 30 využitá pri dôkaze jedného z predchádzajúcich tvrdení.

Záver

V tejto práci sme nadviazali na skúmanie pojmu užitočnosti informácie, krorý formalizujeme rozkladom automatov, kde automat A považujeme za riešenie problému $L = L(A)$. A automaty tvoriace jeho rozklad za riešenia jednoduchších problémov, z ktorých jeden uvažujeme ako nový problém a ostatné ako rady, teda dodatočné užitočné informácie o vstupe. Pokračovali sme vo výskume rozkladu UDFA, kde sme sa pozerali na kvalitu rozkladov a zaviedli sme možnosť dvojnásobnej rady.

Pri 2-rozkladoch sme definovali efektívne 2-rozklady, teda roklady nejakého pekného tvaru a ukázali, že každý 2-rozklad sa dá zlepšiť na nejaký efektívny, ktorý je aspoň tak kvalitný ako bol pôvodný. Kvalitu 2-rozkladov sme merali pomocou sum-kvality, teda súčtu stavových zložitostí automatov rozkladu. Podarilo sa nám presne stanoviť hornú aj dolnú hranicu sum-kvality efektívnych 2-rozkladov a ukázať, kde sa reálne kvalita týchto rozkladov pohybuje.

Ďalej sme definovali 3-rozklady a následne sme našu definíciu zúžili na efektívne 3-rozklady, keďže cieľom rozšírenia počtu automatov rozkladu bolo získať kvalitnejšie rozklady. Charakterizovali sme efektívne 3-rozklady a ukázali, že každý jazyk, ktorý je efektívne 3-rozložiteľný, je aj efektívne 2-rozložiteľný.

Následne sme obdobne ako pri efektívnych 2-rozkladoch presne stanovili hornú aj dolnú hranicu sum-kvality efektívnych 3-rozkladov a ukázali sme, kde sa reálne kvalita týchto rozkladov pohybuje. Na záver sme porovnali sum-kvalitu efektívnych 2-rozkladov a 3-rozkladov a súlade s našimi očakávaniami sa ukázalo, že 3-rozklady sú kvalitnejšie.

Ďalej by sa dalo pokračovať v našom výskume skúmaním neefektívnych 3-rozkladov a ich kvality, rovnako ako aj kvality neefektívnych 2-rozkladov. Inými možnými rozšíreniami by bolo pridanie n-násobnej rady a pozerať sa $n + 1$-rozklady, kde n uvažujeme vačšie ako 2 alebo merať kvalitu rozkladov inak ako pomocou súčtu stavových zložitostí nových automatov. Ako sme v práci navrhli, zmysluplné miery by boli napríklad maximum alebo súčin.

Literatúra

[1] Branislav Rovan and Šimon Sádovský. On usefulness of information: framework and nfa case. In *Adventures Between Lower Bounds and Higher Altitudes*, volume 11011, pages 85–99. Springer International Publishing, 2018.

[2] John E Hopcroft, Rajeev Motwani, and Jeffrey D Ullman. *Introduction to Automata theory, languages, and computation (3rd edition)*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2006.

[3] Gareth A Jones and Josephine M Jones. *Elementary number theory*. Springer Science & Business Media, 1998.

[4] D. G. Hoffman. Packing problems and inequalities. *The Mathematical Gardner*, pages 212–225, 1981.

[5] Giovanni Pighizzini, Branislav Rovan, and Šimon Sádovský. Usefulness of information and decomposability of unary regular languages. *Information and Computation*, page 104868, 2022.

[6] Giovanni Pighizzini and Jeffrey Shallit. Unary language operations, state complexity and Jacobsthal's function. *International Journal of Foundations of Computer Science*, 13(1):145 – 159, 2002.