Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Języki regularne indukujące rozpoznawalne i bezgwiazdkowe języki śladów

rozprawa doktorska

Krystyna Stawikowska

Uniwersytet Mikołaja Kopernika w Toruniu
Wydział Matematyki i Informatyki

Promotor rozprawy
dr hab. Edward Ochmański, prof. UMK
Uniwersytet Mikołaja Kopernika w Toruniu
Wydział Matematyki i Informatyki

Toruń, maj 2007

Oświadczenie autora pracy:
Świadoma odpowiedzialności prawnej oświadczam, że niniejsza rozprawa doktorska została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

....

data *podpis autora rozprawy*

Oświadczenie promotora rozprawy:
Potwierdzam, że niniejsza rozprawa została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej do oceny przez recenzentów.

....

data *podpis promotora rozprawy*

Języki regularne indukujące rozpoznawalne i bezgwiazdkowe języki śladów[1]

Słowa kluczowe:
automaty, języki bezgwiazdkowe, języki śladów, współbieżność

AMS Mathematical Subject Classification 2000:
68Q45 Formal languages and automata

Streszczenie

Teoria śladów stanowi ważny model semantyki systemów współbieżnych. W pracy badane są związki między językami słów i językami śladów, przede wszystkim rozpoznawalnymi i bezgwiazdkowymi.

Wiadomo, że iteracyjnie spójne języki słów indukują rozpoznawalne języki śladów. W pierwszej części rozprawy przedstawiono kilka nowych wyników o tych językach, z których najważniejszym jest fakt, że każdy iteracyjnie spójny język słów ma skończony stopień rozproszenia. Podano też przykład pokazujący, że klasa ta, w odróżnieniu od jej odpowiednika śladowego, nie jest zamknięta względem różnicy teoriomnogościowej.

Główna część rozprawy poświęcona jest badaniu bezgwiazdkowych języków słów i ich związków z bezgwiazdkowymi językami śladów. Podstawowym narzędziem tej części pracy jest operacja bezgwiazdkowej gwiazdki i uzyskana z jej pomocą nowa charakteryzacja bezgwiazdkowych języków słów. Pozwoliła ona uprościć i uzupełnić dowody już istniejących twierdzeń o bezgwiazdkowych językach śladów (aperiodyczność i definiowalność w logice 1-go rzędu), oraz pokazać nowe, z których najważniejszymi są: twierdzenie, że język śladów jest bezgwiazdkowy wtedy i tylko wtedy gdy jego spłaszczenie jest bezgwiazdkowe, twierdzenie, że leksykograficzne bezgwiazdkowe języki słów indukują wszystkie bezgwiazdkowe języki śladów oraz twierdzenie, że bezgwiazdkowa gwiazdka, wraz z sumą i złożeniem, wystarcza do zbudowania wszystkich bezgwiazdkowych języków śladów.

[1]Praca współfinansowana przez Ministerstwo Nauki i Szkolnictwa Wyższego z grantu promotorskiego N206 023 31/3744 oraz stypendium INNOREG nr Z/2.04/II/2.6/7/05.

Regular languages inducing recognizable and star-free trace languages[2]

Keywords:
automata, star-free languages, trace languages, concurrency

AMS Mathematical Subject Classification 2000:
68Q45 Formal languages and automata

Abstract

Trace theory is commonly regarded as one of the most important model of concurrency. This thesis deals with relations between word languages and trace languages, mainly the recognizable and star-free ones.

It is known that star-connected word languages induce recognizable trace languages. In the first part of the thesis, several new facts about star-connected word languages are presented. The most important result asserts that a star-connected word language has a finite rank. Moreover, it is shown that the class of star-free word languages is not closed under complement, unlike its trace-counterpart.

The main part deals with star-free word languages and their relations to star-free trace languages. The basic tools are: a new operation, named star-free star, and a new characterization of star-free word languages, obtained with the star-free star. It has allowed to simplify and supply the proofs of the most important results in this area (aperiodicity and 1-order definable). Also new results have been proved; the main ones are: flattenings of a star-free trace languages are star-free, lexicographic star-free word languages induce star-free trace languages, and the class of trace languages built form atoms using product, union and star-free star is equal to the class of star-free trace languages.

[2]This PhD thesis has been partially supported by Ministry of Science and Higher Education of Poland, grant N206023 31/3744 and Scholarship INNOREG nr Z/2.04/II/2.6/7/05.

Spis treści

Rozdział 1

Wstęp

Tematyka rozprawy na tle historycznym

Klasyczna teoria języków formalnych, zwana też lingwistyką matematyczną, to teoria monoidów wolnych skończenie generowanych. Narodziła się ona w latach 50-tych z potrzeby formalnego opisu zachowania programów komputerowych, w tamtych czasach głównie sekwencyjnych.[1]

Rozwój technik komputerowych – pojawienie się maszyn wieloprocesorowych i programów współbieżnych – zrodził potrzebę matematycznych modeli systemów współbieżnych, z których najważniejszym (i najpopularniejszym) są dziś sieci Petriego (1962). Jako model opisu zachowań tych sieci, Mazurkiewicz zaproponował w [20] w roku 1977 ślady (*traces*), czyli elementy monoidu ilorazowego – nazwanego monoidem śladów (*trace monoid*) – otrzymanego jako iloraz monoidu wolnego przez kongruencję, opartą na relacji niezależności (współbieżności) akcji systemu obliczeniowego.

Monoidy śladów znalazły zastosowanie nie tylko praktyczne. Ich niezwykle ciekawe, często zaskakujące, własności matematyczne i szereg problemów, często bardzo trudnych, wywołały duże zainteresowanie ich teorią, dziś znaną jako teoria śladów (*trace theory*). Teoria ta, dobrze już opisana i ustabilizowana, jest nadal aktualna i stale rozwijana. Szerokie spektrum teorii śladów przedstawiono w książkach „Combinatorics on Traces" Diekerta ([5], 1990) i pracy zbiorowej „Book of Traces" ([7], 1995) oraz w „Handbook of Formal Languages", vol. 3, chapter 8 ([6], 1997).

Jednym z głównych działów klasycznej teorii języków formalnych jest teoria języków regularnych, z podstawowym twierdzeniem Kleene'go mówiącym, że w monoidach wolnych skończenie generowanych klasy języków rozpoznawanych przez automaty skończone i języków definiowanych przez wyrażenia racjonalne są równe. W monoidach śladów klasa języków rozpoznawalnych jest właściwą podklasą klasy języków racjonalnych.

Języki rozpoznawalne są bardzo ważne z praktycznego punktu widzenia, gdyż opisują one zachowania systemów współbieżnych o skończonej liczbie

[1] Ważną motywacją, szczególnie prac Noama Chomsky'ego, były również badania struktury języków naturalnych.

stanów. Z drugiej strony, wyrażenia racjonalne prosto opisują, jak język jest zbudowany, czego nie można powiedzieć o automatach, które jedynie opisują jak język budować.

Stąd jednym z centralnych tematów teorii śladów są języki racjonalne, rozpoznawalne i związki między nimi. Znanym wynikiem jest sposób opisu rozpoznawalnych języków śladów za pomocą tzw. wyrażeń iteracyjnie spójnych. Rozdział 4 rozprawy poświęcony jest iteracyjnie spójnym językom słów, które w odróżnieniu od ich śladowych odpowiedników nie były dotychczas badane.

Języki bezgwiazdkowe, czyli języki opisane przez wyrażenia podobne do wyrażeń racjonalnych, ale z dopełnieniem zastępującym gwiazdkę, odgrywają ważną rolę w teorii języków słów. Najważniejsze wyniki to twierdzenie Schützenbergera ([34], 1965) o aperiodyczności i twierdzenie McNaughtona i Paperta ([22], 1971) o definiowalności w logice 1-go rzędu. Wyniki te przenoszą się na bezgwiazdkowe języki śladów, jednak ich dowody dla śladów są znacznie bardziej skomplikowane. Tym zagadnieniom poświęcony jest rozdział 6. Podstawowym narzędziem jest tu operacja bezgwiazdkowej gwiazdki, wprowadzona w [26], która okazała się bardzo skuteczna w dowodach. Pozwoliła ona uprościć i uzupełnić dowody już istniejących twierdzeń o bezgwiazdkowych językach śladów, oraz pokazać nowe, z których najważniejszym są twierdzenie, że bezgwiazdkowa gwiazdka (wraz z sumą i złożeniem) wystarcza do zbudowania wszystkich bezgwiazdkowych języków śladów.

Zawartość rozprawy, najważniejsze wyniki

Rozprawa składa się z siedmiu rozdziałów. Niniejszy rozdział wstępny zawiera ogólne omówienie pracy i streszczenie jej wyników. W rozdziałach 2 i 3 przedstawiam podstawowe pojęcia i fakty, wykorzystywane w pracy, dotyczące monoidów, w szczególności wolnych (rozdział 2) i monoidów śladów (rozdział 3). Zasadniczą część rozprawy stanowią rozdziały 4-6, pracę kończy podsumowanie.

Rozdział 4 poświęcony jest językom słów indukującym rozpoznawalne języki śladów. Dokładniej badam dwie klasy takich języków – języki iteracyjnie spójne i języki o skończonym stopniu rozproszenia. Głównym wynikiem tego rozdziału jest

Twierdzenie 4.15. Każdy język iteracyjnie spójny
ma skończony stopień rozproszenia,

oraz intuicyjnie nieoczekiwany przykład 4.19, pokazujący, że klasa iteracyjnie spójnych języków słów nie jest zamknięta względem różnicy teoriomnogościowej. Fakt ten zaskakuje, gdyż wiadomo, że klasa iteracyjnie spójnych języków śladów jest zamknięta względem podstawowych operacji teoriomnogościowych.

Tematem rozdziałów 5 i 6 są języki bezgwiazdkowe. Podzbiór dowolnego monoidu M nazywamy bezgwiazdkowym, jeśli można go zbudować z atomów ($\emptyset$

i $\{m\}$ dla $m \in M$) za pomocą operacji sumy mnogościowej, złożenia i dopełnienia.

W rozdziale 5 omawiam bezgwiazdkowe języki słów. Przypominam najważniejsze definicje i fakty, takie jak twierdzenie Schützenbergera (1965, język słów jest bezgwiazdkowy wtw jest on aperiodyczny) i twierdzenie McNaughtona i Paperta (1971, język słów jest bezgwiazdkowy wtw jest on definiowalny w logice 1-go rzędu).

W tym rozdziale przedstawiam główny pomysł i podstawowe narzędzie całej rozprawy – operację bezgwiazdkowej gwiazdki. Jest to klasyczna gwiazdka Kleene'go, ale stosowana jedynie, gdy wynik tej operacji jest językiem bezgwiazdkowym, i nieokreślona w przeciwnym przypadku. Okazuje się, że operacja ta może skutecznie zastąpić operację dopełnienia w konstrukcji bezgwiazdkowych języków słów:

Twierdzenie 5.19. Język słów jest bezgwiazdkowy wtw jest on konstruowalny z atomów za pomocą operacji sumy mnogościowej, złożenia i bezgwiazdkowej gwiazdki.

Dowód tej charakteryzacji wykorzystuje twierdzenie Schützenbergera oraz klasyczną konstrukcję McNaughtona i Yamady ([21], 1960) wyrażeń regularnych dla języków rozpoznawalnych przez automaty skończone.

Siłę i skuteczność tej operacji w pełni pokazuje rozdział 6 o bezgwiazdkowych językach śladów. Podstawowym wynikiem tego rozdziału, dalej intensywnie stosowanym w dowodach, jest lemat o domknięciu złożenia domkniętych języków bezgwiazdkowych:

Lemat 6.7. Domknięcie złożenia domkniętych języków bezgwiazdkowych jest językiem bezgwiazdkowym.

Jego dowód w istotny sposób wykorzystuje udowodnioną w poprzednim rozdziale charakteryzację bezgwiazdkowych języków słów za pomocą bezgwiazdkowej gwiazdki.

Wnioskiem z lematu 6.7 jest twierdzenie o spłaszczeniu dla bezgwiazdkowych języków śladów, istotnie wykorzystywane w kolejnych dowodach:

Wniosek 6.11. Język śladów jest bezgwiazdkowy wtw jego spłaszczenie jest bezgwiazdkowym językiem słów.

Lemat 6.7 pozwolił też znacznie uprościć dowód znanego twierdzenia Guaiany, Restivo i Salemi ([14], 1992) o aperiodyczności bezgwiazdkowych języków śladów.

Języki leksykograficzne, czyli zbiory słów leksykograficznie minimalnych w swoich śladach, odgrywają ważną rolę w teorii rozpoznawalnych języków śladów. Wiadomo, że klasa języków indukowanych przez regularne języki leksykograficzne to dokładnie klasa rozpoznawalnych języków śladów. Analogiczne twierdzenie zachodzi również dla języków bezgwiazdkowych w dowolnym monoidzie śladów:

Twierdzenie 6.34 + Twierdzenie 6.35.
Język śladów jest bezgwiazdkowy
wtw
jego leksykograficzna reprezentacja jest bezgwiazdkowym językiem słów
wtw
jest on definiowalny w logice 1-go rzędu.

Dowód tego faktu w przypadku monoidów przechodnio-zorientowanych (pierwsza równoważność, twierdzenie 6.29) wykorzystuje metody teorii automatów i rozumowania kombinatoryczne. Dowód ogólny, dla dowolnych monoidów śladów (twierdzenie 6.35), poprowadzony został z wykorzystaniem technik logiki 1-go rzędu dla śladów (Ebinger i Muscholl [10], 1996), klasycznego twierdzenia McNaughtona i Paperta (1971) i wcześniej uzyskanych wyników rozprawy.

Podsumowując wyżej omówione wyniki, możemy sformułować ogólną wszechstronną charakteryzację podzbiorów bezgwiazdkowych w dowolnych monoidach śladów:

T jest bezgwiazdkowy
wtw
$\bigcup T$ jest bezgwiazdkowy
wtw
$Lex(T)$ jest bezgwiazdkowy
wtw
T jest aperiodyczny
wtw
T jest definiowalny w logice 1-go rzędu.

Teraz, wykorzystując powyższą charakteryzację, pokazuję, że twierdzenie 5.19 (dla monoidów wolnych) jest prawdziwe w dowolnym monoidzie śladów:

Twierdzenie 6.39. Język śladów jest bezgwiazdkowy
wtw
jest on konstruowalny z atomów za pomocą operacji
sumy mnogościowej, złożenia i bezgwiazdkowej gwiazdki.

W ostatnim rozdziale formułuję kilka problemów otwartych, bezpośrednio związanych z tematyką pracy i uzyskanymi wynikami.

Większość wyników niniejszej rozprawy została opublikowana w pracach [19, 26, 27, 28, 35].

Podziękowania

Serdecznie dziękuję mojemu promotorowi Edwardowi Ochmańskiemu, za naukową opiekę, pomoc i poświęcony czas, Barbarze Klunder za współpracę i cenne wskazówki oraz pozostałym koleżankom i kolegom z Torunia.

Rozdział 2

Wprowadzenie – podstawowe pojęcia i fakty

Na początku przypomnijmy podstawowe pojęcia - monoid, kongruencja, morfizm, podzbiór racjonalny i rozpoznawalny, problem decyzyjny. Za zbiór liczb **naturalnych** przyjmujemy zbiór $\{0, 1, 2, \ldots\}$ i oznaczamy przez $\mathbb{N}$.

2.1 Zbiory i operacje na zbiorach

Zbiory będziemy oznaczać wielkimi literami X, Y, ..., a ich elementy małymi $x \in X$. Zawieranie zbiorów będziemy oznaczać przez $\subseteq$, a właściwe zawieranie symbolem $\subset$. Niech X, Y będą dwoma podzbiorami ustalonego zbioru Z. Zbiór $\{x \in Z \mid x \in X \vee x \in Y\}$ nazywamy **sumą zbiorów** X i Y i oznaczamy przez $X \cup Y$. Zbiór $\{x \in Z \mid x \in X \wedge x \in Y\}$ nazywamy **częścią wspólną** lub **iloczynem zbiorów** X, Y i oznaczamy przez $X \cap Y$. Zbiór $\{x \in X \mid x \notin Y\}$ nazywamy **różnicą zbiorów** X i Y i oznaczamy przez $X \setminus Y$, a **dopełnienie zbioru** X, zbiór $\{x \in Z \mid x \notin X\}$ oznaczamy przez X'. Zbiory jednoelementowe $\{x\}$ nazywamy **singletonami**. **Zbiorem potęgowym** zbioru X nazywamy zbiór $\{Y \mid Y \subseteq X\}$ podzbiorów X i oznaczamy przez 2^X.

Niech X będzie zbiorem. **Relacją binarną** na zbiorze X nazywamy podzbiór $R \subseteq X \times X$. Dwa elementy $x, y \in X$ są w relacji R, jeśli $(x, y) \in R$, co tradycyjnie zapisujemy xRy. Relacja R jest relacją **równoważności**, jeśli jest:

- **zwrotna** – dowolny element $x \in X$ jest w relacji z sobą, xRx,
- **symetryczna** – dla dowolnych $x, y \in X$ jeśli xRy, to yRx,
- **przechodnia** – dla dowolnych $x, y, z \in X$ jeśli xRy oraz yRz, to xRz.

Jeśli R jest relacją równoważności na zbiorze X, to zbiory $[x]_R = \{y \in X \mid xRy\}$ nazywamy **klasami abstrakcji** relacji R. Każde dwie klasy abstrakcji są rozłączne lub równe. Jeśli relacja R będzie ustalona, to przeważnie indeks R będziemy pomijać. Zbiór klas abstrakcji nazywamy **zbiorem ilorazowym** i oznaczamy przez X/R. **Indeksem** relacji równoważności R nazywamy liczbę klas abstrakcji tej relacji.

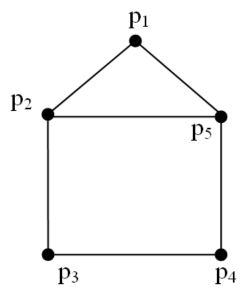
Niech $\mathcal{X}$ będzie rodziną zbiorów. Mówimy, że $\mathcal{X}$ jest **algebrą Boole'a**, jeśli jest zamknięta na sumę zbiorów, dopełnienie i część wspólną.

2.2 Grafy

Grafem niezorientowanym G nazywamy parę (V, E), gdzie V jest skończonym zbiorem **wierzchołków**, a $E \subseteq \{\{x, y\} \mid x, y, \in V\}$ zbiorem **krawędzi** grafu G.

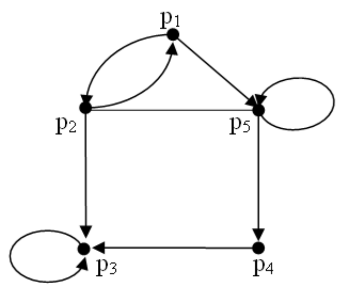
Grafem zorientowanym G nazywamy parę (V, E), gdzie V jest skończonym zbiorem **wierzchołków**, a $E \subseteq V \times V$ zbiorem **krawędzi** grafu G.

Przykład 2.1 (Graf niezorientowany). Niech $G = (V, E)$, gdzie zbiór wierzchołków jest równy $V = \{p_1, p_2, p_3, p_4, p_5\}$ oraz zbiór krawędzi $E = \{\{p_1, p_2\}, \{p_1, p_5\}, \{p_2, p_5\}, \{p_2, p_3\}, \{p_3, p_4\}, \{p_4, p_5\}\}$. Rysunek 2.1 ilustruje graf G.



Rysunek 2.1: Graf niezorientowany

Przykład 2.2 (Graf zorientowany). Niech $G_1 = (V, E_1)$, gdzie zbiór wierzchołków to $V = \{p_1, p_2, p_3, p_4, p_5\}$ oraz zbiór krawędzi to $E =_1 \{(p_1, p_2), (p_2, p_1), (p_1, p_5), (p_2, p_3), (p_5, p_5), (p_4, p_3), (p_5, p_4), (p_3, p_3)\}$. Rysunek 2.2 ilustruje graf G_1.



Rysunek 2.2: Graf zorientowany

Niech $G = (V, E)$ będzie grafem niezorientowanym (zorientowanym). **Ścieżką** o początku w wierzchołku $w \in V$ i końcu w $v \in V$ w grafie nazywamy ciąg krawędzi $\{w, v_1\}, \{v_1, v_2\}, \ldots, \{v_{n-2}, v_{n-1}\}, \{v_{n-1}, v\}$ (odpowiednio (w, v_1), (v_1, v_2), $\ldots$, (v_{n-2}, v_{n-1}), (v_{n-1}, v)). **Cyklem** nazywamy ścieżkę, w której $w = v$ (wierzchołek początkowy jest równy końcowemu).

2.3 Monoidy

W tym podrozdziale podane zostaną podstawowe definicje monoidu i morfizmu monoidów z przykładami.

Definicja 2.3. **Monoidem** nazywamy parę $(M, \cdot)$, gdzie M jest zbiorem oraz $\cdot \colon M \times M \to M$ binarną operacją złożenia, która:

- jest łączna:
$$(\forall x, y, z \in M)\ (x \cdot y) \cdot z = x \cdot (y \cdot z),$$
- posiada element neutralny $1_M \in M$, zwany **jedynką**:
$$(\forall x \in M)\ x \cdot 1_M = x = 1_M \cdot x.$$

Przykład 2.4. Przykładem monoidu jest zbiór liczb naturalnych z dodawaniem, wówczas 0 jest elementem neutralnym lub $\mathbb{N}$ z mnożeniem, wtedy 1 jest elementem neutralnym. Podobnie zbiór liczb całkowitych $\mathbb{Z}$. W szczególności, każda grupa jest monoidem.

Przykład 2.5. Niech X będzie zbiorem. Zbiór potęgowy 2^X z sumą zbiorów i zbiorem pustym jako elementem neutralnym jest monoidem. Jeśli za działanie przyjmiemy iloczyn zbiorów, to elementem neutralnym będzie X.

Definicja 2.6. **Monoidem potęgowym** monoidu $(M, \cdot)$ nazywamy monoid $P(M) = (2^M, \cdot)$, gdzie

- 2^M jest zbiorem potęgowym,
- operacja $\cdot$ jest rozszerzeniem operacji złożenia z monoidu M do operacji na podzbiorach: $X \cdot Y = \{x \cdot y \mid x \in X \wedge y \in Y\}$
- elementem neutralnym jest singleton $\{1_M\}$.

Operacja **potęgowania** zbioru $X \subseteq M$ jest określona następująco: $X^0 = \{1_M\}$, $X^{n+1} = XX^n$ dla $n \geq 1$. Operacja **iteracji** (domknięcie Kleene'go) na podzbiorze $X \subseteq M$, nazywana dalej operacją gwiazdki lub **gwiazdką**, jest określona następująco:
$$X^* = \bigcup_{n \in \mathbb{N}} X^n.$$

Podzbiór $P \subseteq M$ nazywamy **podmonoidem** monoidu $(M, \cdot)$, o ile $1_M \in P$ oraz dla dowolnych elementów $x, y \in P$, złożenie $x \cdot y \in P$.

Podzbiór $G \subseteq M$ nazywamy **zbiorem generatorów** monoidu M o ile $G^* = M$. Monoid M jest skończenie generowany, jeśli posiada skończony zbiór generatorów.

Definicja 2.7. Niech $(M, \cdot)$ i $(N, \bullet)$ będą monoidami. Funkcję $\varphi \colon M \to N$ nazywamy **morfizmem monoidów** wtedy i tylko wtedy, gdy funkcja φ

- zachowuje działanie: $(\forall x, y \in M)\ \varphi(x \cdot y) = \varphi(x) \bullet \varphi(y)$,

- zachowuje element neutralny: $\varphi(1_M) = 1_N$.

Przykład 2.8. Weźmy monoidy liczb naturalnych $\mathbb{N}$ oraz liczb całkowitych $\mathbb{Z}$ z operacją dodawania. Włożenie $\varphi\colon \mathbb{N} \to \mathbb{Z}$, gdzie $\varphi(n) = n$ jest morfizmem monoidów.

Jeśli $\varphi\colon M \to N$, to przeciwobraz morficzny zbioru $Y \subseteq N$ oznaczmy $\varphi^{-1}(Y) = \{m \in M \mid \varphi(m) \in Y\}$.

Morfizm monoidów $\varphi\colon M \to N$ jest **izomorfizmem** o ile istnieje morfizm $\psi\colon N \to M$ taki, że $\psi \circ \varphi = id_M$ oraz $\varphi \circ \psi = id_N$. Odwzorowanie ψ nazywamy morfizmem odwrotnym do φ. Jeśli z monoidu M do N istnieje izomorfizm, to mówimy, że M i N są **izomorficzne**.

Przykład 2.9. Niech X będzie ustalonym zbiorem. Wówczas z monoidu $(2^X, \cup)$ do monoidu $(2^X, \cap)$ istnieje morfizm $\varphi : 2^X \to 2^X$ określony jako $\varphi(Y) = X \setminus Y$ dla $Y \subseteq X$. Odwzorowanie φ zachowuje element neutralny $\varphi(\emptyset) = X$ oraz działanie $\varphi(Y \cup Z) = X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z) = \varphi(Y) \cap \varphi(Z)$, gdzie $Y, Z \subseteq X$, jest więc morfizmem, a nawet izomorfizmem.

2.4 Monoidy wolne

Szczególną rolę odgrywa klasa monoidów wolnych. Niech A będzie **alfabetem**. Elementy alfabetu nazywamy **literami**. Skończone ciągi liter nazywamy **słowami**. Ciąg długości 0 nazywamy **słowem pustym** i oznaczmy przez ε. Zbiór wszystkich słów nad alfabetem A oznaczymy przez A^*. Podzbiory A^* będziemy nazywać **językami słów**. Zbiór słów niepustych, czyli język $A^* \setminus \{\varepsilon\}$, oznaczać będziemy przez A^+.

Określmy na zbiorze A^* operację złożenia $\cdot\colon A^* \times A^* \to A^*$ w następujący sposób. Niech $u = (a_1, \ldots, a_n) \in A^*$ i $v = (b_1, \ldots, b_m) \in A^*$, gdzie $a_i, b_j \in A$, $n, m \geq 0$. Wówczas $u \cdot v = (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$. Złożenie $\cdot$ jest łączne i słowo puste ε jest jego elementem neutralnym, czyli $(A^*, \cdot)$ jest monoidem, zwanym **monoidem wolnym** nad alfabetem A.

Ogólniej, monoid M jest wolny wtedy i tylko wtedy, gdy istnieje alfabet A taki, że M jest izomorficzny z A^*. Oznacza to tyle, że w monoidzie M istnieje zbiór generatorów G taki, że dowolny element różny od jedynki ma dokładnie jeden rozkład na elementy ze zbioru G, tzn. istnieje zbiór generatorów G będący kodem.

Kategoryjna definicja monoidu wolnego jest następująca. Monoid $(M, \cdot)$ jest monoidem wolnym wtedy i tylko wtedy, gdy istnieje podzbiór G i funkcja $\mu : G \to M$ takie, że dla dowolnego monoidu N i funkcji $\lambda : G \to N$ istnieje dokładnie jeden morfizm $\overline{\lambda} : M \to N$ taki, że $\lambda = \overline{\lambda}\mu$, czyli poniższy diagram jest przemienny.

$$\begin{tikzcd} G \arrow[r, "\mu"] \arrow[dr, "\lambda"'] & M \arrow[d, "\overline{\lambda}"] \\ & N \end{tikzcd}$$

W zapisie słów będziemy pomijać nawiasy i przecinki. Zamiast zapisu $(a_1, a_2, \ldots, a_n)$, gdzie $a_i \in A$, $n \geq 1$, będzie stosowany zapis $a_1 a_2 \ldots a_n$. Symbol operacji $\cdot$ również będzie pomijany, czyli zamiast $u \cdot v$, gdzie $u, v \in A^*$, będzie pisane uv. **Długość słowa** $u \in A^*$, czyli długość ciągu, będziemy oznaczać przez $|u|$, przez $|u|_a$, gdzie $a \in A$, oznaczać liczbę wystąpień litery a w słowie u, a przez $Alph(u)$ zbiór liter występujących w słowie u.

W dalszej części ograniczymy się do monoidów wolnych nad skończonymi alfabetami. Będziemy używać następującej terminologii. Niech A będzie alfabetem. Słowo $x \in A^*$ jest **podsłowem** słowa $w \in A^*$, jeśli jest jego podciągiem, **segmentem**, jeśli istnieją słowa $u, v \in A^*$ takie, że $w = uxv$, **prefiksem**, jeśli x jest segmentem w oraz $u = \varepsilon$, **sufiksem**, gdy x będzie segmentem w oraz $v = \varepsilon$.

Przykład 2.10. Niech $A = \{a\}$ będzie alfabetem jednoliterowym i $A^* = \{a^n \mid n \in \mathbb{N}\}$, przyjmujemy, że $a^0 = \varepsilon$. Wówczas A^* z działaniem składnia jest izomorficzny z monoidem $(\mathbb{N}, +)$. Funkcja długości słowa $\varphi(a^n) = n$ jest izomorfizmem tych monoidów.

2.5 Kongruencje i monoidy ilorazowe

Niech $(M, \cdot)$ będzie monoidem. Relacja równoważności $\approx \subseteq M \times M$ jest **kongruencją** o ile jest zgodna z działaniem monoidowym

$$(\forall x, y, u, v \in M) \quad x \approx u \wedge y \approx v \Rightarrow x \cdot y \approx u \cdot v.$$

Jeśli relacja $\approx$ jest kongruencją, to na zbiorze ilorazowym $M/_\approx$ działanie $\cdot \colon M/_\approx \times M/_\approx \to M/_\approx$, gdzie $[x]_\approx \cdot [y]_\approx = [x \cdot y]_\approx$, jest poprawnie określone. Indeks $\approx$ będzie przeważnie pomijany, gdy kongruencja $\approx$ będzie ustalona. Zbiór ilorazowy z tak określonym złożeniem oraz jedynką $[1_M]_\approx$ tworzy monoid, który nazywamy **monoidem ilorazowym** M przez kongruencję $\approx$.

Niech M będzie monoidem, a $M/_\approx$ monoidem ilorazowym. **Morfizmem kanonicznym** nazywamy morfizm $[\;] \colon M \to M/_\approx$, który każdemu elementowi $m \in M$ przyporządkowuje jego klasę abstrakcji $[m] \in M/_\approx$. Odwrotnie, każdy morfizm $\varphi \colon M \to N$ z monoidu M do monoidu N wyznacza kongruencję $\approx \subseteq M \times M$:

$$x \approx y \iff \varphi(x) = \varphi(y).$$

Niech $\sim \subseteq M \times M$ będzie relacją binarną na monoidzie M. **Kongruencją generowaną** przez $\sim$ nazywamy najmniejszą kongruencję zawierającą $\sim$. Konstrukcja kongruencji jest następująca. Najpierw określamy relację $\approx \subseteq M \times M$:

$$x \approx y \iff (\exists u, v, p, q \in M)\ x = upv \wedge y = uqv \wedge (p \sim q \vee q \sim p).$$

Zwrotne i przechodnie domknięcie $\approx^*$ relacji $\approx$ jest szukaną kongruencją. Przez $M/_\sim$, gdzie $\sim$ jest relacją binarną na monoidzie M, będziemy rozumieli monoid ilorazowy M przez kongruencję generowaną przez $\sim$.

2.5.1 Działania na podzbiorach monoidu

Niech $\approx \subseteq M \times M$ będzie kongruencją w monoidzie M. Rozszerzmy morfizm kanoniczny $[\,]: M \to M/_\approx$ na zbiór potęgowy 2^M. Morfizm $[\,]: 2^M \to 2^{M/\approx}$ przyporządkowuje podzbiorowi $X \subseteq M$ podzbiór

$$[X] = \{[m] \mid m \in X\} \subseteq M/_\approx.$$

Wówczas mówimy, że podzbiór $X \subseteq M$ **indukuje** zbiór $[X] \subseteq M/_\approx$.

Spłaszczeniem nazywamy odwzorowanie $\bigcup : 2^{M/\approx} \to 2^M$ określone dla $Y \subseteq M/_\approx$ następująco

$$\bigcup Y = \{m \in M \mid [m] \in Y\}.$$

Kolejną istotną operacją jest **domknięcie** $Cl : 2^M \to 2^M$. Zamiast pisać $Cl(X)$, będziemy używać tradycyjnego zapisu $\overline{X}$,

$$\overline{X} = \{m \in M \mid [m] \in [X]\} = \bigcup [X].$$

Mówimy, że zbiór X jest domknięty, jeśli jest równy swojemu domknięciu, $X = \overline{X}$.

2.5.2 Przedstawienia równaniowe

Niech A będzie alfabetem i niech $E = \{u_1 \sim v_1, \ldots, u_n \sim v_n\}$ będzie skończoną relacją w A^*. **Przedstawieniem równaniowym** monoidu ilorazowego $A^*/_\sim$ nazywamy parę $\langle A; E\rangle$. Przy opisywaniu relacji E, zamiast symbolu $\sim$, będziemy używać symbolu równości $=$.

Przykład 2.11. Niech $M = \langle a, b; ab = ba = \varepsilon\rangle$. Monoid M jest izomorficzny z monoidem $(\mathbb{Z}, +)$ liczb całkowitych z dodawaniem. Dwa elementy monoidu wolnego są równoważne wtedy i tylko wtedy, gdy różnice liczby wystąpień liter a i b są równe.

Przykład 2.12 (Pierwszy raz o monoidach śladów). Monoidy śladów można zadać przedstawieniem równaniowym. Wówczas zbiór E, to równania postaci $ab = ba$, gdzie $a, b \in A$. Najprostszy monoid śladów, to $\langle a, b; ab = ba\rangle$. Wówczas dla dowolnego słowa $w \in A^*$, jego klasa abstrakcji wygląda następująco

$$[w] = \{v \in A^* \mid |v|_a = |w|_a \wedge |v|_b = |w|_b\}.$$

2.6 Podzbiory racjonalne

Wyrażenia regularne i języki przez nie definiowane to pojęcia doskonale znane z klasycznej teorii języków formalnych. Uogólnienia tych pojęć dla dowolnych monoidów nazywamy wyrażeniami i zbiorami racjonalnymi.

Definicja 2.13. Niech $(M, \cdot)$ będzie monoidem. Klasa **zbiorów racjonalnych** $Rat(M)$ to najmniejsza rodzina podzbiorów monoidu M spełniająca następujące warunki

- zbiór pusty $\emptyset \in Rat(M)$ i dla każdego $m \in M$, singleton $\{m\} \in Rat(M)$,
- jeśli $X, Y \subseteq M$ są racjonalne, to ich suma $X \cup Y \in Rat(M)$, złożenie $X \cdot Y \in Rat(M)$ oraz gwiazdka $X^* \in Rat(M)$ są zbiorami racjonalnymi.

Definicja 2.14. Zbiorem **wyrażeń racjonalnych** $REX(M)$ nad monoidem M nazywamy najmniejszy zbiór słów nad alfabetem $M \cup \{\cup, \cdot, (,), ^*, \emptyset\}$ taki, że:

- $\emptyset \in REX(M)$ – symbol zbioru pustego jest wyrażeniem racjonalnym,
- dla każdego elementu $m \in M$, słowo $(m) \in REX(M)$,
- jeśli słowa $R, S \in REX(M)$ są wyrażeniami racjonalnymi, to słowa $(R \cup S)$, $(R \cdot S)$ oraz $(R)^*$ są wyrażeniami racjonalnymi.

Każde wyrażenie racjonalne jednoznacznie wyznacza zbiór racjonalny. Jeśli $R \in REX(M)$ jest wyrażeniem racjonalnym, to przez $L(R)$ oznaczamy zbiór wyznaczony przez wyrażenie R. Jeśli $R = \emptyset$, to $L(\emptyset) = \emptyset$, jeśli $R = m$, gdzie $m \in M$, to $L(m) = \{m\}$. Jeśli $R = (R_1 \cup R_2)$, to $L(R_1 \cup R_2) = L(R_1) \cup L(R_2)$, gdy $R = (R_1 \cdot R_2)$, to $L(R_1 \cdot R_2) = L(R_1) \cdot L(R_2)$, a gdy $R = (R_1^*)$, to $L(R_1^*) = (L(R_1))^*$. Dla przejrzystości zapisu wrażeń racjonalnych, będziemy pomijać zbędne nawiasy przyjmując jednocześnie, że gwiazdka ma najwyższy priorytet, a składanie wyższy od sumy. Często będziemy opuszczać symbol składania.

Przykład 2.15. Niech $A = \{a, b\}$ będzie alfabetem i A^* monoidem wolnym. Weźmy język $L \subseteq A^*$ wszystkich słów parzystej długości nad alfabetem A. Język L jest racjonalny, a wyrażenie go wyznaczające jest postaci $(aa \cup ab \cup ba \cup bb)^*$.

Dla dowolnego zbioru racjonalnego $Z \subseteq M$ istnieje nieskończenie wiele wyrażeń racjonalnych $R \in REX(M)$ takich, że $L(R) = Z$.

Przykład 2.16. Niech $A = \{a, b\}$ będzie alfabetem. Wyrażenie racjonalne $(a \cup b)^*$ wyznacza cały monoid A^*, podobnie wyrażenie $(a^* b^*)^*$.

Niech A będzie skończonym alfabetem. Tradycyjnie dla monoidów wolnych A^* przyjmuje się w bazie definicji, że singletony liter (a nie wszystkich słów) są zbiorami racjonalnymi. Oczywiście jest to równoważna definicja, gdyż A^* jest generowany przez alfabet A. Wyrażenia racjonalne nad monoidem wolnym A^* nazywać będziemy **wyrażeniami regularnymi**.

2.6.1 Własności zbiorów racjonalnych

Dla dowolnego monoidu M, wprost z definicji klasy zbiorów racjonalnych $Rat(M)$ wynika, że singletony i zbiór pusty są zbiorami racjonalnymi oraz klasa ta jest zamknięta na złożenie, sumę oraz operację gwiazdki. Ponadto dla dowolnych dwóch monoidów M i N oraz dowolnego morfizmu monoidów $\varphi : M \to N$, jeśli zbiór $X \in Rat(M)$ jest racjonalny w monoidzie M, to jego obraz morficzny $\varphi(X) \subseteq N$ jest racjonalny w monoidzie N.

Stwierdzenie 2.17. *Monoid M jest zbiorem racjonalnym wtedy i tylko wtedy, gdy jest skończenie generowany.*

Dowód. Jeśli monoid jest skończenie generowany i zbiór $G = \{m_1, \ldots, m_n\}$ jest zbiorem generatorów, to $M = (m_1 \cup \ldots \cup m_n)^*$, więc jest racjonalny.

Teraz pokażemy, że jeśli istnieje wyrażenie racjonalne definiujące monoid M, to jest on skończenie generowany. Niech $R \in REX(M)$ będzie wyrażeniem racjonalnym. Niech $X \subseteq M$ będzie zbiorem elementów z M występujących w wyrażeniu R.

Najpierw pokażemy, że zbiór $L(R) \subseteq X^*$. Przeprowadźmy indukcję strukturalną. Dla wyrażeń prostych $\emptyset$, m, gdzie $m \in M$, zawieranie jest oczywiste. Przypuśćmy, że dla wyrażeń R_1 i R_2 zachodzą implikacje $L(R_1) \subseteq X_1^*$, $L(R_2) \subseteq X_2^*$, gdzie X_1, X_2 są zbiorami elementów z M występujących w wyrażeniach R_1 i R_2 odpowiednio. Jeśli $R = R_1 \cup R_2$, to $X = X_1 \cup X_2$ oraz $L(R) = L(R_1) \cup L(R_2) \subseteq X_1^* \cup X_2^* \subseteq X^*$. Jeśli $R = R_1R_2$, to $X = X_1 \cup X_2$ oraz $L(R) = L(R_1)L(R_2) \subseteq X_1^*X_2^* \subseteq X^*$. Jeśli $R = R_1^*$, to $X = X_1$ i stąd $L(R) = L(R_1)^* \subseteq (X^*)^* = X^*$. Ponadto z indukcji wynika, że zbiór X jest zbiorem skończonym.

Jeśli istnieje wyrażenie racjonalne $R \in REX(M)$ definiujące M, to monoid $M = L(R)$ zawarty jest w zbiorze X^*, gdzie $X \subseteq M$ to zbiór elementów z M występujących w wyrażeniu R. Ponieważ $X^* \subseteq M$ i X jest skończony, to $M = X^*$, a więc M jest skończenie generowany. $\square$

Istnieją monoidy, w których klasa zbiorów racjonalnych nie jest zamknięta względem różnicy, części wspólnej, dopełnienia oraz przeciwobrazu morficznego. Pokazują to poniższe przykłady.

Przykład 2.18 (Część wspólna i różnica wyprowadzają poza *Rat*). Niech $M = \langle a, b, c; ab = ba, bc = cb \rangle$. Zbiory $X = [a]^*[bc]^*$, $Y = [ab]^*[c]^* \in Rat(M)$ są racjonalne, ale ich część wspólna $X \cap Y = \{[a^n b^n c^n] | n \geq 0\}$ nie jest zbiorem racjonalnym, co zostanie pokazane w podrozdziale 2.7.3.

Stosując prawa de Morgana $X \cap Y = (X' \cup Y')'$ otrzymujemy, że co najmniej jedno z dopełnień wyprowadza poza klasę zbiorów racjonalnych. Zbiory $X' = [a]^*[bc]^*([b][b]^* \cup [c][c]^*) \cup ([a] \cup [b] \cup [c])^*[ca]([a] \cup [c])^*$ i $Y' = ([b][b]^* \cup [a][a]^*)[ab]^*[c]^* \cup ([a] \cup [b] \cup [c])^*[ca]([a] \cup [c])^*$ są racjonalne, więc $X' \cup Y' \in Rat(M)$, stąd $(X' \cup Y')' \notin Rat(M)$. Zatem dopełnienie i różnica, wyprowadzają z $Rat(M)$ (bo $(X' \cup Y')' = M \setminus (X' \cup Y')$).

Przykład 2.19 (Nieracjonalny przeciwobraz morficzny). Niech $A = \{a, b\}$ i $M = \langle a, b; ab = ba \rangle$. Niech $\varphi : A^* \to M$ będzie morfizmem monoidów takim, że $\varphi(a) = [a]$ i $\varphi(b) = [b]$. Wówczas przeciwobraz racjonalnego zbioru $(ab)^*$ jest równy $\varphi^{-1}((ab)^*) = \{w \in A^* \mid |w|_a = |w|_b\}$ i nie jest to zbiór racjonalny, co zostanie pokazane w podrozdziale 2.7.3.

2.7 Podzbiory rozpoznawalne

Zbiory rozpoznawalne można definiować na kilka równoważnych sposobów. Pierwotna definicja, od której pochodzi nazwa tych podzbiorów, wykorzystuje pojęcie automatu, inne wykorzystują pojęcia ilorazu lewostronnego bądź monoidu syntaktycznego.

Definicja 2.20. Automatem monoidowym nazywamy piątkę

$$\mathcal{A} = \langle M, Q, \delta, q_0, F \rangle,$$

gdzie M jest monoidem, Q jest skończonym zbiorem stanów, $\delta \subseteq Q \times M \times Q$ jest relacją przejścia taką, że dla dowolnych $q, p, r \in Q$ oraz $m, n \in M$, zachodzi $(q, 1_M, p) \in \delta$ wtedy i tylko wtedy, gdy $p = q$ oraz jeśli $(q, m, p) \in \delta$ i $(p, n, r) \in \delta$, to $(q, mn, r) \in \delta$, stan $q_0 \in Q$ jest wyróżnionym stanem początkowym, a $F \subseteq Q$ jest podzbiorem stanów końcowych.

Automat nazywamy **deterministycznym**, jeśli $\{((q, m), p) | (q, m, p) \in \delta\}$ jest funkcją (częściową), czyli jeśli $(q, m, p) \in \delta$ i $(q, m, p') \in \delta$, to $p = p'$. Rozważając automaty deterministyczne będziemy pisać $\delta(q, m) = p$ zamiast $(q, m, p) \in \delta$. Automat nazywamy **skończonym** o ile ma skończony zbiór stanów.

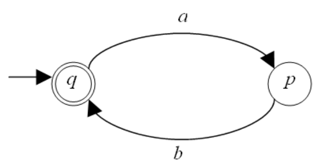
Mówimy, że automat $\mathcal{A}$ rozpoznaje (akceptuje) zbiór $L(\mathcal{A}) = \{m \in M \mid (\exists q \in F)\ (q_0, m, q) \in \delta\}$. Minimalnym automatem deterministycznym, w skrócie m.d.a., nazywamy automat deterministyczny $\mathcal{A}$, którego moc zbioru stanów jest najmniejsza spośród wszystkich deterministycznych automatów rozpoznających język $L(\mathcal{A})$.

W przypadku monoidów wolnych, automaty często będziemy przedstawiać jako etykietowane grafy zorientowane. Niech $\mathcal{A} = \langle A^*, Q, \delta, q_0, F \rangle$ będzie automatem. Zbiór stanów Q odpowiada zbiorowi wierzchołków, krawędź ze stanu $p \in Q$ do stanu $q \in Q$ istnieje wtedy i tylko wtedy, gdy istnieje litera $a \in A$ taka, że $(p, a, q) \in \delta$. Wówczas etykietą krawędzi jest podzbiór liter spełniających powyższy warunek. Stan początkowy oznaczamy zewnętrzną strzałką do niego prowadzącą, stany końcowe wyrózniamy podwójnym kółkiem. Słowo jest akceptowane przez automat $\mathcal{A}$, jeśli istnieje ścieżka od stanu początkowego do stanu końcowego taka, że kolejne litery słowa należą do zbioru etykiet kolejnych krawędzi.

Definicja 2.21 (Zbiór rozpoznawalny). Podzbiór $X \subseteq M$ monoidu M jest **rozpoznawalny** wtedy i tylko wtedy, gdy istnieje skończony deterministyczny automat monoidowy akceptujący X. Klasę zbiorów rozpoznawalnych monoidu M oznaczamy przez $Rec(M)$.

Można pokazać, że jeśli zbiór X jest akceptowany przez niedeterministyczny skończony automat, to istnieje skończony deterministyczny automat rozpoznający X.

Przykład 2.22. Niech $A = \{a, b\}$ będzie dwuliterowym alfabetem. Język $L = (ab)^* \subseteq A^*$ jest zbiorem rozpoznawalnym i deterministyczny automat $\mathcal{A} = \langle A^*, \{q, p\}, \delta, q, \{q\} \rangle$, gdzie $\delta(q, a) = p$ i $\delta(p, b) = q$, akceptuje L. Rysunek 2.3 przedstawia automat jako graf.



Rysunek 2.3: Skończony automat rozpoznający język $(ab)^*$

2.7.1 Ilorazy lewostronne

Definicja 2.23. Niech M będzie monoidem, $X \subseteq M$ podzbiorem oraz $m \in M$ elementem monoidu. **Ilorazem lewostronnym** X przez m nazywamy zbiór

$$m^{-1}X = \{n \in M \mid mn \in X\}.$$

Zbiór wszystkich ilorazów lewostronnych zbioru $X \subseteq M$ oznaczamy przez $LQ(X) = \{m^{-1}X \mid m \in M\}$. **Lewostronną relacją syntaktyczną** wyznaczoną przez zbiór $X \subseteq M$ nazywamy relację $LS_X \subseteq M \times M$:

$$LS_X = \{(m,n) \in M \times M \mid m^{-1}X = n^{-1}X\}.$$

Zauważmy, że indeks LS_X jest dokładnie równy mocy $LQ(X)$. Łatwo sprawdzić, że lewostronna relacja syntaktyczna jest relacją równoważności, ale nie jest kongruencją.

Przykład 2.24. Niech $A = \{a, b\}$. Weźmy język $L = \{aa, ba\} \subseteq A^*$. Ilorazy lewostronne $a^{-1}L$ i $b^{-1}L$ są sobie równe i składają się z jednego elementu a, stąd $(a, b) \in LS_L$. Oczywiście $(a, a) \in LS_L$, ale już $(aa, ab) \notin LS_L$, bo $(aa)^{-1}L = \{\varepsilon\}$, a $(ab)^{-1}L = \emptyset$. Stąd LS_L nie jest kongruencją.

Relacja LS_X jest prawą kongruencją, to znaczy, że dla dowolnych elementów $m, n \in M$ jeśli $(m, n) \in LS_X$, to dla każdego $v \in M$ zachodzi $(mv, nv) \in LS_X$.

Stwierdzenie 2.25. *Zbiór jest rozpoznawalny wtedy i tylko wtedy, gdy ma skończoną liczbę ilorazów lewostronnych.*

Dowód. Niech M będzie monoidem, $X \subseteq M$ jego rozpoznawalnym podzbiorem oraz $\mathcal{A}$ skończonym deterministycznym automatem akceptującym X. Zauważmy, że jeśli $\mathcal{A} = \langle M, Q, \delta, q_0, F\rangle$ jest automatem, to dla $m \in M$, $m^{-1}L(\mathcal{A}) = L(\mathcal{A}')$, gdzie $\mathcal{A}' = \langle Q, M, \delta, \delta(q_0, m), F\rangle$. Zatem jeśli $\delta(q_0, m) = \delta(q_0, n)$, to $m^{-1}L(\mathcal{A}) = n^{-1}L(\mathcal{A})$. Stąd liczba ilorazów lewostronnych jest nie większa niż ilość stanów w automacie $\mathcal{A}$, a więc skończona.

Przypuśćmy, że zbiór X ma skończoną liczbę ilorazów lewostronnych. Wówczas istnieje skończony automat $\mathcal{A} = \langle M, Q, \delta, q_0, F\rangle$, gdzie $Q = \{m^{-1}X \mid m \in M\}$, $q_0 = 1_M{}^{-1}X = X$, $F = \{m^{-1}X \mid m \in X\}$ oraz $\delta(m^{-1}X, n) = \delta(X, mn) = (mn)^{-1}X$. $\square$

Przykład 2.26. Niech $A = \{a, b\}$ oraz $L = \{a^n b^n \mid n \geq 0\} \subseteq A^*$ będzie językiem słów. Język L nie jest rozpoznawalny, ponieważ dla dowolnego $n \in \mathbb{N}$, słowo $b^m \in (a^n)^{-1}L$ wtedy i tylko wtedy, gdy $m = n$. Stąd dla $m \neq n$ mamy $(a^m)^{-1}L \neq (a^n)^{-1}L$, a więc język L ma nieskończenie wiele ilorazów lewostronnych. Ze stwierdzenia 2.25 wynika, że L nie jest rozpoznawalny.

2.7.2 Ilorazy wewnętrzne

Definicja 2.27. Niech M będzie monoidem i $X \subseteq M$ jego podzbiorem. **Ilorazem syntaktycznym** (lub **wewnętrznym**) zbioru X przez element $m \in M$ nazywamy zbiór

$$X//m = \{(x, y) \in M \times M \mid xmy \in X\}.$$

Relacją syntaktyczną wyznaczoną przez podzbiór X nazywamy relację $SY_X \subseteq M \times M$:

$$SY_X = \{(m, n) \in M \times M \mid X//m = X//n\},$$

równoważnie

$$SY_X = \{(m, n) \in M \times M \mid (\forall x, y \in M)\ xmy \in X \Leftrightarrow xny \in X\}.$$

Stwierdzenie 2.28. *Niech M będzie monoidem i $X \subseteq M$ jego podzbiorem. Wówczas relacja syntaktyczna SY_X wyznaczona przez podzbiór $X \subseteq M$ jest kongruencją.*

Dowód. Symetryczność, zwrotność i przechodniość wynikają wprost z definicji. Pokażemy, że jeśli $(m, n), (m', n') \in SY_X$, to $(mm', nn') \in SY_X$. Dla dowolnych $x, y \in X$ zachodzi $xmy \in X \Leftrightarrow xny \in X$. W szczególności $xm(m'y) \in X \Leftrightarrow xn(m'y) \in X$. Ponieważ $(m', n') \in SY_X$, to $(xn)m'y \in X \Leftrightarrow (xn)n'y \in X$. Otrzymaliśmy, że dla dowolnych $x, y \in M$ zachodzi równoważność $xmm'y \in X \Leftrightarrow xnn'y \in X$, czyli $(mm', nn') \in SY_X$. □

Monoidem syntaktycznym wyznaczonym przez podzbiór $X \subseteq M$ nazywamy monoid ilorazowy $M/_{SY_X}$.

Stwierdzenie 2.29. *Niech M będzie monoidem oraz $X \subseteq M$ podzbiorem. Monoid syntaktyczny zbioru X jest skończony wtedy i tylko wtedy, gdy X ma skończoną liczbę ilorazów lewostronnych.*

Dowód. Niech X ma skończoną liczbę ilorazów wewnętrznych. Zauważmy, że $\{1\} \times m^{-1}X = X//m \cap \{1\} \times M$. Stąd, jeśli $X//m = X//m'$, to $m^{-1}X = m'^{-1}X$. Zatem liczba różnych ilorazów lewostronnych jest nie większa niż liczba różnych ilorazów wewnętrznych.

Niech $X \subseteq M$ ma skończoną liczbę k ilorazów lewostronnych. Pokażemy, że liczba ilorazów wewnętrznych jest również skończona. Zauważmy, że

$$X//m = \bigcup_{x \in M} \{x\} \times (xm)^{-1}X$$

oraz jeśli $x^{-1}X = x'^{-1}X$, to $(xm)^{-1}X = (x'm)^{-1}X$. Stąd $X//m = \{[x] \times (xm)^{-1}X \mid x \in M\}$, gdzie $[x] = \{x' \in M \mid x^{-1}X = x'^{-1}X\}$. Liczba różnych zbiorów $[x]$ jest równa liczbie ilorazów lewostronnych, czyli równa k. Zatem liczba różnych ilorazów wewnętrznych nie jest większa od liczby wszystkich funkcji z k-elementowego zbioru wszystkich klas $\{[x] \mid x \in M\}$ do k-elementowego zbioru ilorazów lewostronnych $\{m^{-1}X \mid m \in M\}$, ponieważ każdy element $m \in M$ wyznacza jedną funkcję $[x] \to (xm)^{-1}X$. Stąd różnych ilorazów wewnętrznych jest nie więcej niż k^k. □

Wniosek 2.30. *Zbiór jest rozpoznawalny wtedy i tylko wtedy, gdy jego monoid syntaktyczny jest skończony.*

2.7.3 Własności zbiorów rozpoznawalnych

Stwierdzenie 2.31. *Niech M będzie dowolnym monoidem. Wówczas zbiór M i zbiór pusty $\emptyset$ są rozpoznawalne.*

Dowód. Zauważmy, że dla dowolnego $m \in M$ mamy $m^{-1}M = M$ oraz $m^{-1}\emptyset = \emptyset$, więc zbiory M i $\emptyset$ mają po jednym ilorazie lewostronnym, stąd są rozpoznawalne. □

Stwierdzenie 2.32. *W dowolnym monoidzie M klasa zbiorów rozpoznawalnych $Rec(M)$ zamknięta jest na działanie sumy, różnicy, dopełnienia i części wspólnej.*

Dowód. Niech $X, Y \in Rec(M)$ i niech $k = |\{x^{-1}X \mid x \in M\}|$ oraz $l = |\{y^{-1}Y \mid y \in M\}|$. Zauważmy, że dla dowolnego $x \in M$ zachodzi $x^{-1}(X \cup Y) = (x^{-1}X) \cup (x^{-1}Y)$, $x^{-1}(X \cap Y) = (x^{-1}X) \cap (x^{-1}Y)$ oraz $x^{-1}(X \setminus Y) = (x^{-1}X) \setminus (x^{-1}Y)$. Stąd liczba ilorazów lewostronnych zbiorów $X \cup Y$, $X \cap Y$ i $X \setminus Y$ jest skończona i jest nie większa niż kl. Stąd i ze stwierdzenia 2.31 wynika, że dopełnienie $X' = M \setminus X$ jest rozpoznawalne. □

Twierdzenie 2.33 (Twierdzenie o spłaszczeniu). *Niech M będzie monoidem, $\approx \subseteq M \times M$ kongruencją na M oraz $M/_\approx$ monoidem ilorazowym wyznaczonym przez $\approx$. Niech $X \subseteq M/_\approx$ będzie podzbiorem monoidu ilorazowego. Wówczas*

$$X \in Rec(M/_\approx) \iff \bigcup X \in Rec(M).$$

Dowód. Korzystając ze stwierdzenia 2.25 wystarczy pokazać, że liczba ilorazów lewostronnych zbiorów X i $\bigcup X$ jest jednakowa.

Niech $\alpha = [m]$ i $\beta = [n]$ dla $\alpha, \beta \in M/_\approx$ i $m, n \in M$. Zauważmy, że zachodzą równości $\alpha^{-1}X = [m^{-1}(\bigcup X)]$, $\beta^{-1}X = [n^{-1}(\bigcup X)]$ oraz równoważność

$$[m^{-1}(\bigcup X)] = [n^{-1}(\bigcup X)] \iff m^{-1}(\bigcup X) = n^{-1}(\bigcup X).$$

Stąd

$$\alpha^{-1}X = \beta^{-1}X \iff m^{-1}(\bigcup X) = n^{-1}(\bigcup X),$$

więc X i $\bigcup X$ mają tę samą liczbę ilorazów lewostronnych. □

Ponieważ każdy morfizm monoidów wyznacza kongruencję, otrzymujemy wniosek:

Wniosek 2.34. *Niech M i N będą monoidami, a $\varphi\colon M \to N$ morfizmem monoidów. Jeśli $Y \in Rec(N)$, to $\varphi^{-1}(Y) \in Rec(M)$.*

Klasa zbiorów rozpoznawalnych w dowolnym monoidzie nie jest zamknięta na złożenie i operację gwiazdki. Dla dowolnego monoidu nie każdy singleton jest zbiorem rozpoznawalnym i klasa ta nie zawsze jest zamknięta na morficzne obrazy.

Przykład 2.35 (Nierozpoznawalny singleton). Niech $M = \langle a, b; ab = \varepsilon \rangle$. Zbiory $[a] \subseteq Rec(M)$ i $[b] \subseteq Rec(M)$ są zbiorami rozpoznawalnymi, natomiast ich złożenie, które jest singletonem, $[a][b] = [ab] = \{a^n b^n \mid n \geq 0\}$ nie jest rozpoznawalne, na mocy z przykładu 2.26 i twierdzenia 2.33.

Przykład 2.36 (Gwiazdka wyprowadza poza Rec). Niech $M = \langle a, b; ab = ba \rangle$. Nietrudno sprawdzić, że język $[ab] \subseteq M$ jest rozpoznawalny. Natomiast język $T = [ab]^*$ wobec twierdzenia 2.33 i przykładu 2.26 nie jest rozpoznawalny.

Zauważmy, że języki w przykładach 2.35 i 2.36 są racjonalne. Przykłady te pokazują, że istnieją języki racjonalne, które nie są rozpoznawalne.

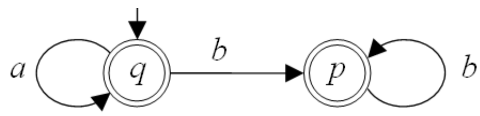
Szczególnymi monoidami są monoidy wolne skończenie generowane. Dla nich zachodzi twierdzenie Kleene'go ([17]).

Twierdzenie 2.37 (Twierdzenie Kleene'go). *Niech A będzie skończonym alfabetem oraz $L \subseteq A^*$ językiem słów nad A. Wówczas*

$$L \in Rat(A^*) \Longleftrightarrow L \in Rec(A^*).$$

Ponieważ w skończenie generowanych monoidach wolnych klasy języków racjonalnych i języków rozpoznawalnych są równe, to w tych monoidach używamy dla nich wspólnej nazwy – klasa **języków regularnych** i oznaczamy przez $Reg(A^*)$, gdzie A jest skończonym alfabetem.

Przykład 2.38. Niech $A = \{a, b\}$ i $L = a^*b^*$. Język L jest racjonalny, bo jest zdefiniowany przez wyrażenie racjonalne i jest rozpoznawalny (rysunek 2.4).



Rysunek 2.4: Automat rozpoznający język a^*b^*.

Dla dowolnych monoidów zachodzi słabsze twierdzenie.

Twierdzenie 2.39. *Monoid M jest skończenie generowany wtedy i tylko wtedy, gdy $Rec(M) \subseteq Rat(M)$.*

Dowód. ($\Longrightarrow$) Niech $\{m_1, \ldots, m_k\}$ będzie zbiorem generatorów M. Niech $A = \{a_1, \ldots, a_k\}$ i $\varphi\colon A^* \to M$ będzie morfizmem, gdzie $\varphi(a_i) = g_i$ dla $i = 1, \ldots, k$. Niech $Y \in Rec(M)$. Ponieważ przeciwobrazy morficzne nie wyprowadzają poza klasę zbiorów rozpoznawalnych i w A^* zachodzi twierdzenie Kleene'go, to $\varphi^{-1}(Y) \in Rec(A^*) = Rat(A^*)$. Morfizmy nie wyprowadzają z klasy zbiorów racjonalnych, więc $Y = \varphi(\varphi^{-1}(Y)) \in Rat(M)$.

($\Longleftarrow$)Wiemy, że dla dowolnego monoidu $M \in Rec(M)$. Z założenia $M \in Rat(M)$. Korzystając ze stwierdzenia 2.17 otrzymujemy, że M jest skończenie generowany. □

Niech A będzie skończonym alfabetem. Klasa języków regularnych $Reg(A^*)$ ma dobre własności klas języków rozpoznawalnych i racjonalnych – jest zamknięta na operacje teoriomnogościowe sumy, części wspólnej, różnicy i dopełnienia, na operacje algebraiczne złożenia i gwiazdki oraz na morficzne obrazy i przeciwobrazy.

Przykład 2.40 (Przykład 2.18 cd.). Niech $M = \langle a, b, c; ab = ba, ac = ca\rangle$. Korzystając z twierdzenia Kleene'go pokażemy, że zbiór $Z = \{[a^n b^n c^n] | n \geq 0\}$ z przykładu 2.18 nie jest racjonalny. Niech $\varphi : M \to \{a, c\}^*$ będzie morfizmem monoidów takim, że $\varphi([a]) = a$, $\varphi([b]) = \varepsilon$ i $\varphi([c]) = c$. Z przykładu 2.26 wynika, że obraz morficzny $\varphi(Z) \notin Reg$. Ponieważ morfizmy zachowują racjonalność, to $Z \notin Rat(M)$.

Przykład 2.41 (Przykład 2.19 cd.). Niech $A = \{a, b\}$ i $M = \langle a, b; ab = ba\rangle$. Do pokazania, że przeciwobraz morficzny nie zachowuje racjonalności wystarczy pokazać, że język $L = \{w \in A \mid |w|_a = |w|_b\} \notin Reg(A^*)$. Ponieważ $L \cap a^*b^* = \{a^n b^n \mid n \geq 0\} \notin Reg(A^*)$, to również $L \notin Reg(A^*)$.

2.8 Problemy decyzyjne

Problemy decyzyjne mają następującą postać:

Dziedzina: klasa obiektów, które chcemy zbadać,
Pytanie: pytanie o własność obiektu.

Nieformalnie mówimy, że problem decyzyjny jest rozstrzygalny, jeśli istnieje algorytm, który zawsze odpowiada czy obiekt (należący do dziedziny) posiada daną własność, czy nie.

Formalne opisanie kiedy problem decyzyjny jest rozstrzygalny, wymaga sprecyzowania pojęcia „algorytm", jak również sprecyzowania, w jaki sposób mają być opisane obiekty, które chcemy badać. W tym podrozdziale przedstawiona zostanie jedynie ogólna idea wykorzystująca pojęcie maszyny Turinga, pominięte zostaną techniczne szczegóły.

2.8.1 Maszyna Turinga i problem stopu

W literaturze można znaleźć wiele równoważnych definicji maszyny Turinga, poniższa z przykładami pochodzi z [33].

Definicja 2.42. Maszyną Turinga nazywamy trójkę (S, A_T, F), gdzie:

1. Zbiory S i A_T są rozłączne, zbiór S jest zbiorem stanów, A_T alfabetem.

2. Element $s_0 \in S$ jest stanem początkowym, $\# \in A_T$ znacznikiem ograniczenia, a podzbiór $S_1 \subseteq S$ zbiorem stanów końcowych. Zbiór $A = A_T \setminus \{\#\}$ jest niepusty, a element $o \in A$ jest wyróżniony.

3. Zbiór F jest zbiorem produkcji następującej postaci:

(i) $s_i a \to s_j b$ (nadpisanie),

(ii) $s_i ac \to as_j c$ (przesunięcie w prawo),

(iii) $s_i a\# \to as_j o\#$ (przesunięcie w prawo i rozszerzenie),

(iv) $cs_i a \to s_j ca$ (przesunięcie w lewo),

(v) $\#s_i a \to \#s_j oa$ (przesunięcie w lewo i rozszerzenie),

gdzie $s_i, s_j \in S$ oraz $a, b, c \in A$, przy czym dla każdych $s_i, s_j \in S$ i $a \in A$, zbiór F zawiera oba typy produkcji (iii) i (ii) dla dowolnego c (odpowiednio (v) i (iv) dla dowolnego c) lub nie zawiera żadnej produkcji (iii) i (ii) (odpowiednio (v) i (iv)). Ponadto dla ustalonych $s_i \in S$ i $a \in A$, słowo $s_i a$ nie jest jednocześnie podsłowem lewych stron dwóch produkcji z typów (i), (iii) i (v).

Mówimy, że słowo sw, gdzie $s \in S$ i $w \in A^*$, jest martwe wtedy i tylko wtedy, gdy w nie zaczyna się na literę $a \in A$ taką, że sa jest podsłowem lewej strony produkcji z F. Nieformalnie, zbiór F wyznacza relację przejścia $\Rightarrow \subseteq \#A^*SA^*\# \times \#A^*SA^*\#$, gdzie $\#ws_1v\# \Rightarrow \#w's_2v'\#$, gdy w' powstaje z w i v' powstaje z v, po zastosowaniu jednej z produkcji do podsłów w i v w stanie s_1 do s_2. Zwrotne i przechodnie domknięcie relacji $\Rightarrow$ oznaczamy przez $\Rightarrow^*$. Język akceptowany przez maszynę Turinga TM definiowany jest następująco:

$$\begin{aligned} L(\mathrm{TM}) \;=\; & \{w \in A^* | \#s_0w\# \Rightarrow^* \#w_1s_1w_2\#, \text{ gdzie } s_1 \in S_1, w_1, w_2 \in A^* \\ & \text{oraz } s_1w_2\# \text{ jest martwe}\}. \end{aligned}$$

Problem decyzyjny jest rozstrzygalny, jeśli istnieje maszyna Turinga taka, że mając dany obiekt opisany skończonym słowem, zawsze zatrzyma się w stanie akceptującym s^+, gdy dany obiekt posiada badaną własność oraz zawsze zatrzyma się w stanie s^-, gdy obiekt tej własności nie posiada.

Opisując poprawny algorytm pokazujemy, że problem decyzyjny jest rozstrzygalny. Aby udowodnić, że dany problem jest nierozstrzygalny, trzeba pokazać, że nie istnieje maszyna Turinga rozstrzygająca dany problem. Najczęściej pokazuje się to pośrednio, sprowadzając jakiś problem, o którym już wiadomo, że jest nierozstrzygalny, do problemu aktualnie badanego.

Przykład 2.43. Jednym z najbardziej znanych i wykorzystywanych problemów nierozstrzygalnych jest problem stopu dla maszyny Turinga

„Czy dana maszyna Turinga mająca na wejściu dane słowo, zatrzyma się?"

Niech TM będzie maszyną Turinga. W alfabecie maszyny zakodujmy jej alfabet bez symbolu #, zbiór stanów, symbol $\to$ i dodatkowy symbol separujący. Przez słowo w_{TM} będziemy oznaczać słowo powstałe z zapisania kolejno zakodowanych produkcji, oddzielonych zakodowanym symbolem separującym. Będziemy mówić, że maszyna Turinga jest samotestująca, jeśli mając na wejściu słowo w_{TM}, zatrzyma się.

Przypuśćmy, że istnieje maszyna Turinga TM_0, która mając na wejściu słowo w_{TM} zatrzymuje się w stanie s^+, gdy maszyna TM jest samotestująca, oraz w stanie s^-, gdy TM nie jest samotestująca. Nietrudno przerobić maszynę TM_0 na maszynę TM_1, która nie zatrzymuje się na słowie w_{TM}, jeśli TM jest samotestująca i zatrzymuje się w stanie s^-, gdy TM nie jest samotestująca. Zauważmy, że TM_1 zatrzymuje się na w_{TM_1} wtedy i tylko wtedy, gdy TM_1 nie zatrzymuje się na w_{TM_1}. Sprzeczność. Stąd problem samotestowania jest nierozstrzygalny.

Problem stopu za dane bierze dowolną maszynę Turinga i dowolne słowo. Problem samotestowania jest więc szczególnym przypadkiem problemu stopu. Ponieważ problem samotestowania jest nierozstrzygalny, więc problem stopu jest również nierozstrzygalny.

Dla danej maszyny TM można skonstruować maszynę TM_1, która akceptuje dokładnie te słowa, na których maszyna TM zatrzymuje się. Dla takiej maszyny Turinga TM_1 można skonstruować gramatykę kontekstową G generującą język $L(\mathrm{TM}_1)$. Wówczas słowo $w \in L(\mathrm{TM}_1)$ wtedy i tylko wtedy, gdy TM_1 zatrzymuje się, gdy na wejściu ma słowo w. Problem należenia słowa do języka generowanego przez daną gramatykę kontekstową jest więc nierozstrzygalny.

Brakujące konstrukcje i szczegóły techniczne można znaleźć między innymi w [33] i [16].

2.8.2 Problem odpowiedniości Posta

Definicja 2.44. Problemem odpowiedniości Posta nazywamy czwórkę

$$\mathrm{PCP} = (A, n, X, Y),$$

gdzie A jest alfabetem, $n \geq 1$ oraz

$$X = (x_1, x_2, \ldots, x_n), \qquad Y = (y_1, y_2, \ldots, y_n)$$

są n-kami niepustych słów nad alfabetem A. **Rozwiązaniem** problemu odpowiedniości Posta nazywamy niepusty skończony ciąg indeksów $(i_1, \ldots, i_k)$ taki, że

$$x_{i_1} \ldots x_{i_k} = y_{i_1} \ldots y_{i_k}.$$

Przykład 2.45. Rozwiązaniem problemu odpowiedniości Posta

$$(\{a, b\}, 3, (a^2, b^2, ab^2), (a^2b, ba, b))$$

jest ciąg $(1, 2, 1, 3)$

$$a^2b^2a^2ab^2 = a^2bbaa^2bb.$$

Twierdzenie 2.46. *Problem „Czy dany problem odpowiedniości Posta posiada rozwiązanie?” jest nierozstrzygalny.*

Dowód wykorzystuje nierozstrzygalność problemu należenia do języka generowanego przez kontekstową gramatykę. Dla ustalonej gramatyki kontekstowej G i danego słowa konstruuje się problem odpowiedniości Posta, który posiada rozwiązanie wtedy i tylko wtedy, gdy słowo należy do języka $L(G)$.

Rozdział 3

Monoidy śladów

Pierwszy raz częściowo przemienne monoidy wolne wprowadzili Cartier i Foata w [2] w 1969 roku. Jednak ślady jako modele opisujące zachowania systemów współbieżnych, zostały wprowadzone przez Mazurkiewicza w [20] w roku 1977.

Alfabetem współbieżnym nazywamy parę (A, I), gdzie A jest skończonym alfabetem oraz $I \subseteq A \times A$ antyzwrotną i symetryczną relacją na alfabecie A, zwaną **relacją niezależności** lub **niezależnością**. Jeśli przyjmiemy, że litery reprezentują akcje systemu współbieżnego, to niezależność opisuje, które z akcji mogą być wykonywane współbieżnie. Dopełnienie relacji niezależności $D = A \times A \setminus I$ nazywamy **relacją zależności** lub **zależnością**.

Niech (A, I) będzie alfabetem współbieżnym. **Monoidem śladów** nazywamy monoid ilorazowy monoidu wolnego A^* przez kongruencję generowaną przez relację niezależności $I \subseteq A \times A$ i oznaczamy przez A^*/I. Jeśli $E = \{ab = ba \mid aIb\}$, to para $\langle A; E \rangle$ jest przedstawieniem równaniowym monoidu śladów A^*/I. Elementy monoidu śladów, czyli klasy abstrakcji kongruencji generowanej przez niezależność, nazywamy **śladami**, a podzbiory monoidu śladów nazywamy **językami śladów**. Ślad słowa $w \in A^*$ (ślad indukowany przez słowo w) będziemy oznaczać przez $[w]_I$ lub $[w]$, gdy relacja niezależności będzie ustalona.

W dowolnym monoidzie śladów A^*/I każdy ślad zawiera skończoną liczbę słów równej długości. **Długością śladu** $\alpha \in A^*/I$ nazywamy wspólną długość jego elementów tzn. jeśli $\alpha = [w]$, to długość śladu $|\alpha| = |w|$. Przez $Alph(\alpha)$ oznaczamy podzbiór $Alph(w) \subseteq A^*$, gdzie $w \in A^*$ i $\alpha = [w]$.

Przykład 3.1. Niech A^*/I będzie monoidem śladów, gdzie $A = \{a, b\}$ oraz aIb. Wówczas dla dowolnego $w \in A^*$, $[w] = \{v \in A^* \mid |w|_a = |v|_a \wedge |w|_b = |v|_b\}$.

Alfabet współbieżny (A, I) można opisać grafem nazywanym **grafem zależności**. Graf zależności jest grafem nieskierowanym, zbiorem jego wierzchołków jest alfabet A, a dwie litery $a, b \in A$ tworzą krawędź wtedy i tylko wtedy, gdy aDb, gdzie $D = A \times A \setminus I$ jest relacją zależności. Graf zależności zwyczajowo będziemy oznaczać parą (A, D). Dla przejrzystości, w grafie nie zaznaczamy zależności elementów samych z sobą.

Przykład 3.2. Niech (A, I) będzie alfabetem współbieżnym, gdzie $A = \{a, b, c\}$ oraz aIc, czyli aDb oraz bDc. Graf zależności dla (A, I) to:

$$(A, D)\colon a - b - c.$$

Mówimy, że podalfabety $B, C \subseteq A$ są niezależne i oznaczmy, BIC, gdy dla każdego $b \in B$ oraz $c \in C$ zachodzi bIc.

Poniższy lemat opisuje istotną własność śladów. Jego dowód można znaleźć między innymi w [6].

Lemat 3.3 (Levi). *Niech $\alpha, \beta, \gamma, \delta \in A^*/I$ będą śladami. Wówczas poniższe zdania są równoważne*

1. $\alpha\beta = \gamma\delta$
2. *Istnieją ślady $\alpha_1, \alpha_2, \beta_1, \beta_2 \in A^*/I$ takie, że $\alpha = \alpha_1\alpha_2$, $\beta = \beta_1\beta_2$, $\gamma = \alpha_1\beta_1$, $\delta = \alpha_2\beta_2$ oraz $Alph(\alpha_1)IAlph(\beta_2)$.*

3.1 Grafy śladów

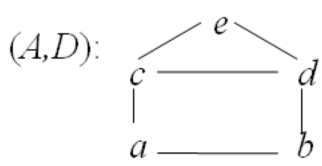
Niech (A, I) będzie alfabetem współbieżnym, $D = A \times A \setminus I$ relacją zależności i $w = a_1 \dots a_n \in A^*$ słowem. **Grafem śladu** słowa w nazywamy trójkę (V, E, λ), gdzie

- $V = \{x_1, \dots, x_n\}$ jest skończonym zbiorem pozycji w słowie w – zbiorem wierzchołków w grafie,
- $\lambda\colon V \to A$ funkcją etykietującą, gdzie $(\forall i)\ \lambda(x_i) = a_i$,
- $E \subseteq V \times V$ zbiorem krawędzi, gdzie $(x_i, x_j) \in E$ wtedy i tylko wtedy, gdy $i < j$ oraz $(\lambda(x_i), \lambda(x_j)) \in D$.

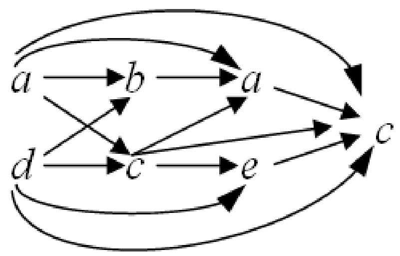
Słowa $w, v \in A^*$ są równoważne wtedy i tylko wtedy, gdy ich grafy śladów są izomorficzne. **Graf śladu** $\alpha \in A^*/I$, nazywamy graf izomorficzny z grafem pewnego słowa $w \in A^*$ indukującego ślad α.

Z definicji wynika, że graf śladu jest acykliczny, a zwrotne i przechodnie domknięcie relacji E jest częściowym porządkiem na zbiorze V.

Przykład 3.4. Niech $A = \{a, b, c, d, e\}$ będzie alfabetem z grafem zależności



Graf śladu $[dabcaec]$ przedstawia rysunek 3.1.



Rysunek 3.1: Graf śladu $[dabcaec]$

3.2 Rozpoznawalne języki śladów

Niech (A, I) będzie alfabetem współbieżnym oraz A^*/I monoidem śladów. Rozpoznawalne i racjonalne klasy języków śladów będziemy oznaczać $Rec(A^*/I)$ i $Rat(A^*/I)$ odpowiednio.

Poniższe twierdzenie jest szczególnym przypadkiem twierdzenia 2.33:

Twierdzenie 3.5 (Twierdzenie o spłaszczeniu dla śladów). *Niech (A, I) będzie alfabetem współbieżnym, oraz $T \subseteq A^*/I$ językiem śladów. Wówczas*

$$T \in Rec(A^*/I) \Longleftrightarrow \bigcup T \in Reg(A^*).$$

Niech $[\ ]\colon A^* \to A^*/I$ będzie morfizmem kanonicznym. Niech $L \subseteq A^*$ będzie językiem słów i $[L] = \{[w] \mid w \in L\} \subseteq A^*/I$ indukowanym językiem śladów przez L. Jeśli L jest językiem regularnym, to $[L]$ jest racjonalnym językiem śladów. Język śladów $T \subseteq A^*/I$ jest racjonalny wtedy i tylko wtedy, gdy istnieje indukujący go regularny język słów, tzn. taki $L \subseteq A^*$, że $[L] = T$. Przykład 2.36 pokazuje, że racjonalny język śladów nie musi być rozpoznawalny. Dla regularnego języka słów $(ab)^*$ indukowany język śladów $[ab]^*$ oczywiście jest racjonalny, ale nie jest rozpoznawalny.

Język słów $\overline{L} = \bigcup[L] = \{w \in A^* \mid (\exists v \in L)[v] = [w]\}$ nazywamy domknięciem języka L (względem I). Twierdzenie 3.5 można sformułować z punktu widzenia języków słów:

Twierdzenie 3.6. *Niech (A, I) będzie alfabetem współbieżnym oraz $L \subseteq A^*$ językiem słów. Wówczas*

$$[L] \in Rec(A^*/I) \Longleftrightarrow \overline{L} \in Reg(A^*).$$

Rozpoznawalne języki śladów są indukowane przez domknięte języki regularne, przy czym dokładnie jednemu rozpoznawalnemu językowi śladów, odpowiada jeden domknięty regularny język słów.

Klasa języków rozpoznawalnych w dowolnym monoidzie jest zamknięta na sumę zbiorów, część wspólną, różnicę oraz na przeciwobrazy morficzne. Ponieważ każdy ślad zawiera skończoną liczbę elementów, to z twierdzenia o spłaszczeniu wynika, że w monoidach śladów każdy singleton jest rozpoznawalny. Przykład 2.36 pokazuje, że już w najprostszym nietrywialnym monoidzie śladów, operacja gwiazdki nie zachowuje rozpoznawalności. Zauważmy, że w przykładzie 2.35 monoid M nie jest monoidem śladów.

Twierdzenie 3.7. *Niech (A, I) będzie alfabetem współbieżnym. Niech $T, S \in Rec(A^*/I)$ będą rozpoznawalnymi językami śladów. Wówczas złożenie $TS \in Rec(A^*/I)$ jest językiem rozpoznawalnym.*

Dowód, wykorzystujący lemat 4.10, będzie podany w rozdziale 4.

3.3 Problemy decyzyjne w monoidach śladów

Rozważane problemy decyzyjne w monoidach śladów będą następującej postaci:

Dane: alfabet współbieżny (A, I), wyrażenie racjonalne $R \in REX(A^*/I)$

Pytanie: pytanie o własność języka śladów definiowanego przez wyrażenie racjonalne

Stosując indukcję strukturalną łatwo pokazać, że następujące problemy są rozstrzygalne:

1. Czy dany ślad $m \in M$ należy do języka śladów $L(R)$?
2. Czy $L(R) = \emptyset$?
3. Czy $L(R) = \varepsilon$?
4. Czy $L(R)$ jest skończony?

W pracy [1] Berstel udowodnił następujące fakty:

Twierdzenie 3.8 (Berstel). *Niech (A, I) będzie alfabetem współbieżnym i $M = A^*/I$ monoidem śladów. Dla danych wyrażeń racjonalnych $R, S \in REX(A^*/I)$, następujące problemy są nierozstrzygalne:*

1. *Czy $L(R) \cap L(S) = \emptyset$?*
2. *Czy $L(R) = M$?*
3. *Czy $L(R) = L(S)$?*
4. *Czy $L(R) \in Rec(A^*/I)$?*

Dowód 1 łatwo wynika z nierozstrzygalności problemu odpowiedniości Posta PCP. Pozostałe dowody są bardziej skomplikowane, ale również wykorzystują nierozstrzygalność problemu odpowiedniości Posta.

W [32] Sakarovitch rozważył, kiedy problem 4 jest rozstrzygalny i uzyskał twierdzenie

Twierdzenie 3.9 (Sakarovitch). *Problem „Czy dany racjonalny język śladów T jest rozpoznawalny w monoidzie śladów A^*/I ?” jest rozstrzygalny wtedy i tylko wtedy, gdy relacja niezależności I jest przechodnia.*

Rozważane są również problemy, w których danymi są zbiory rozpoznawalne. Zbiór rozpoznawalny może być podany na kilka sposobów — automatem monoidowym, domkniętym językiem regularnym lub specjalnym wyrażeniem racjonalnym, o którym będzie mowa w następnym rozdziale.

Wśród otwartych problemów dla monoidów śladów dotyczących rozstrzygalności, **problemem gwiazdki** jest jednym z najciekawszych i najtrudniejszych. Problem ten postawili Clerbout i Latteux w [3, 4] w roku 1985.

Problem gwiazdki: Czy dla danego monoidu śladów M i języka rozpoznawalnego $T \subseteq M$, język T^* jest rozpoznawany?

Dziwność problemu gwiazdki pokazuje przykład monoidu śladów, w którym jest on rozstrzygalny (Gastin, Ochmański, Petit, Rozoy [11]) podczas gdy problem rozpoznawalności jest w nim nierozstrzygalny (Gibons, Rytter [12]). Jest to monoid:

$$(A,D): \quad \begin{array}{ccc} a & \text{———} & c \\ & b & \end{array}$$

Rozdział 4

Iteracyjnie spójne języki słów

Iteracyjnie spójne języki śladów, zdefiniowane i badane w [24], odgrywają dużą rolę w teorii rozpoznawalnych języków śladów. Pojęcie to, w zupełnie naturalny sposób, przenosi się na języki słów. Dobre zbadanie tej klasy języków słów wydaje się ważne, gdyż są to języki indukujące rozpoznawalne języki śladów, co oznacza, że ich współbieżna implementacja może być realizowana przez systemy o skończonej liczbie stanów.

Niech (A, I) będzie ustalonym alfabetem współbieżnym i A^*/I monoidem śladów. Wówczas morfizm kanoniczny $[\,]\colon A^* \to A^*/I$ dowolnemu słowu $w \in A^*$ przyporządkowuje jego ślad $[w]$. Określmy odwzorowanie $[\,]\colon 2^{A^*} \to 2^{A^*/I}$ przyporządkowujące językom słów $L \subseteq A^*$ języki śladów $[L] \subseteq A^*/I$. Obraz $[\,]\colon 2^{A^*} \to 2^{A^*/I}$, czyli odwzorowanie $[\,]\colon 2^{2^{A^*}} \to 2^{2^{A^*/I}}$, przyporządkowuje klasom języków słów odpowiednie klasy języków śladów. Dla dowolnego $L \in Reg(A^*)$, język śladów $[L] \in Rat(A^*/I)$. Z przykładu 2.36 wiadomo, że jeśli $I \neq \emptyset$, to istnieją języki regularne $L \subseteq A^*$ takie, że indukowane języki śladów $[L] \notin Rec(A^*/I)$. Stąd zawieranie $Rec(A^*/I) \subset [Reg(A^*)]$ jest właściwe. Klasę języków regularnych indukujących rozpoznawalne języki śladów oznaczmy przez $InvRec(A^*/I)$ lub przez $InvRec$, gdy alfabet współbieżny będzie ustalony .

Definicja 4.1. Niech (A, I) będzie alfabetem współbieżnym oraz $D = A \times A \setminus I$ relacją zależności.

- Słowo $w \in A^*$ jest **spójne** wtedy i tylko wtedy, gdy graf zależności obcięty do $Alph(w)$ jest spójny.
- Język słów $L \subseteq A^*$ jest **spójny** wtedy i tylko wtedy, gdy wszystkie jego słowa są spójne.
- Ślad $[w] \in A^*/I$ jest **spójny** wtedy i tylko wtedy, gdy słowo w jest spójne.
- Język śladów $T \subseteq A^*/I$ jest **spójny** wtedy i tyko wtedy, gdy wszystkie jego ślady są spójne.

Poniższe stwierdzenie zostało udowodnione przez Ochmańskiego w [24] oraz, w ogólniejszym przypadki tzw. półprzemienności, przez Clerbout i Latteuxa w [4].

Stwierdzenie 4.2. *Niech (A, I) będzie alfabetem współbieżnym i $M = A^*/I$ monoidem śladów. Jeśli język śladów $T \subseteq M$ jest rozpoznawalny i spójny, to język śladów T^* jest rozpoznawalny.*

Definicja 4.3. Niech (A, I) będzie alfabetem współbieżnym. Wyrażenie racjonalne $R \in REX(A^*/I)$ nad alfabetem A jest **spójne** wtedy i tylko wtedy, gdy język $L(R)$ jest spójny.

Stwierdzenie 4.4. *Problem „Czy język $L(R)$ definiowany przez dane wyrażenie racjonalne $R \in REX(A^*)$, przy danym alfabecie współbieżnym (A, I), jest językiem spójnym?" jest rozstrzygalny.*

Dowód. Niech $ALPH(R) = \{Alph(w) \mid [w] \in L(R)\}$ będzie zbiorem wszystkich podzbiorów alfabetu będących alfabetami elementów z języka $L(R)$. Ponieważ alfabet A z założenia jest skończony, to $ALPH(R)$ jest skończony dla dowolnego $R \in REX(A^*)$. Język $L(R)$ jest spójny wtedy tylko i wtedy, gdy każdy element zbioru $ALPH(R)$ jest alfabetem spójnym.

Testowanie czy podalfabet $A_1 \subseteq A$ jest spójny sprowadza się do testowania, czy graf zależności $(A_1, D \cap A_1 \times A_1)$ jest grafem spójnym. Stąd problem, czy przy ustalonym alfabecie współbieżnym dany podzbiór alfabetu jest spójny, jest rozstrzygalny.

Ponieważ zbiór $ALPH(R)$ jest skończony, to wystarczy pokazać, jak skonstruować $ALPH(R)$.

Niech $R \in REX(A)$.
Baza. Jeśli $R = \emptyset$ to $ALPH(R) = \emptyset$ i $L(R)$ jest spójny. Jeśli $R = m$ dla $m \in M$, to $ALPH(R) = \{Alph(w)\}$, gdzie $[w] = m$. W szczególnym przypadku, gdy $R = [\varepsilon]$, to $ALPH(R) = \{\emptyset\}$.
Rekurencja. Mamy do rozważenia 3 przypadki:

- Niech $R = R_1 \cup R_2$. Wówczas $ALPH(R) = ALPH(R_1) \cup ALPH(R_2)$.
- Niech $R = R_1 R_2$. Wówczas $ALPH(R) = \{A_1 \cup A_2 | A_1 \in ALPH(R_1), A_2 \in ALPH(R_2)\}$ (jeśli co najmniej jeden z $ALPH(R_1)$ i $ALPH(R_2)$ jest pusty, to $ALPH(R) = \emptyset$).
- Jeśli $R = (R_1)^*$, to $ALPH(R) = ALPH(R_1^{|ALPH(R_1)|}) \cup \{\emptyset\}$.

□

Przejdźmy do wyrażeń i języków iteracyjnie spójnych i ich własności.

Definicja 4.5. Niech (A, I) będzie alfabetem współbieżnym.

- Wyrażenie racjonalne (nad A) jest **iteracyjnie spójne** (względem I) wtedy i tylko wtedy, gdy wyrażenia pod każdą gwiazdką są spójne. Formalnie – każde wyrażenie atomowe ($\emptyset$, ε, $a \in A$) jest iteracyjnie spójne. Jeśli wyrażenia R i S są iteracyjnie spójne, to $(R \cup S)$, (RS) są iteracyjnie spójne. Jeśli ponadto R jest spójne, to R^* jest iteracyjnie spójne. Klasa iteracyjnie spójnych wyrażeń racjonalnych jest najmniejszą klasą spełniającą te warunki.

- Język słów $L \subseteq A^*$ jest **iteracyjnie spójny** (względem I) wtedy i tylko wtedy, gdy istnieje iteracyjnie spójne wyrażenie R takie, że $L = L(R)$. Klasę iteracyjnie spójnych języków słów (nad A względem I) będziemy oznaczać przez $StarCon_I(A)$.

- Język śladów $T \subseteq A^*/I$ jest **iteracyjnie spójny** wtedy i tylko wtedy, gdy istnieje iteracyjnie spójne wyrażenie R takie, że $T = [L(R)]$. Równoważnie, istnieje iteracyjnie spójny język słów $L \subseteq A^*$ indukujący język T; $T = [L]$.

Stwierdzenie 4.6. *Niech alfabet współbieżny (A, I) i wyrażenie racjonalne R nad A będą danymi. Wówczas problem „Czy wyrażenie R jest iteracyjnie spójne?” jest problemem rozstrzygalnym.*

Dowód. Indukcja strukturalna, z wykorzystaniem stwierdzenia 4.4

□

Iteracyjnie spójne języki słów indukują całą klasę $Rec(A^*/I)$ rozpoznawalnych języków śladów. Dowód poniższego twierdzenia znajduje się w [24] i [25].

Twierdzenie 4.7. *Niech (A, I) będzie alfabetem współbieżnym. Wówczas zachodzi równość $Rec(A^*/I) = [StarCon_I(A)]$. Równoważnie, język śladów $T \subseteq A^*/I$ jest rozpoznawalny wtedy i tylko wtedy, gdy istnieje iteracyjnie spójny język słów $L \subseteq A^*$ indukujący T ($T = [L]$).*

Przykład 4.8. Dowolny język regularny jest definiowany przez nieskończenie wiele wyrażeń regularnych. W szczególności, nie wszystkie wyrażenia definiujące iteracyjnie spójne języki są iteracyjnie spójne. Na przykład:

$$\begin{aligned} (a \cup b)^* &= (a^* b^*)^* \\ (a \cup b)^* b &= (a^* \cup bb^* a)^* bb^*. \end{aligned}$$

Wyrażenia po lewej stronie są iteracyjnie spójne, a po prawej nie są, jeśli aIb.

4.1 Relacje między klasami $StarCon$ i $InvRec$.

Hashiguchi w [15] wprowadził pojęcie stopnia rozproszenia języka słów względem relacji niezależności oraz udowodnił, że każdy język regularny o skończonym stopniu indukuje rozpoznawalny język śladów.

Definicja 4.9 (Stopień rozproszenia). Niech (A, I) będzie alfabetem współbieżnym. Niech $L \subseteq A^*$ będzie językiem słów oraz $u, v \in A^*$ takimi słowami, że $[uv] \in [L]$. Mówimy, że $rank_{L,I}(u, v) \leq n$ (dla $n \in \mathbb{N}$) gdy istnieje takie słowo $w \in L$, że

$$\begin{aligned} w = v_0 u_1 v_1 \dots u_n v_n, \quad & u_1 \dots u_n \in [u], \; v_0 v_1 \dots v_n \in [v] \\ \text{oraz} \quad & (v_i, u_j) \in I \text{ dla } i < j. \end{aligned}$$

Określmy częściową funkcję $rank_{L,I}\colon A^* \times A^* \dashrightarrow \mathbb{N}$ w następujący sposób:

$$rank_{L,I}(u,v) = \begin{cases} \min\{n \in \mathbb{N} \mid rank_{L,I}(u,v) \leq n\} & \text{gdy } [uv] \in [L] \\ \text{nieokreślone} & \text{w przeciwnym wypadku} \end{cases}$$

Stopniem rozproszenia języka $L \subseteq A^*$ (względem I) nazywamy liczbę (o ile istnieje) lub nieskończoność:

$$Rank_I(L) = \begin{cases} \max\{rank_{L,I}(u,v) \mid [uv] \in [L]\} & \text{gdy zbiór jest ograniczony} \\ \infty & \text{w przeciwnym wypadku} \end{cases}$$

W pierwszym przypadku mówimy, że $Rank_I(L)$ jest skończony i będziemy pisać $Rank_I(L) < \infty$, w drugim, że $Rank_I(L)$ jest nieskończony. Indeksy L oraz I zazwyczaj będą pomijane, gdy nie będzie to prowadzić do nieporozumień.

Klasę języków regularnych nad alfabetem A o skończonym rzędzie względem I będziemy oznaczać przez $FinRank_I(A)$,

$$FinRank_I(A) = \{L \in Reg(A^*) \mid Rank_I(L) < \infty\}.$$

Poniższy lemat jest znany jest jako lemat Hashiguchiego. Jego dowód można znaleźć w [15] (oryginał) i [25] (prostszy).

Lemat 4.10 (Hashiguchi). *Niech (A, I) będzie alfabetem współbieżnym oraz $L \subseteq A^*$ językiem słów. Jeśli stopień $Rank_I(L)$ jest skończony, to język L indukuje rozpoznawalny język śladów ($[L] \in Rec(A^*/I)$).*

Teraz możemy podać dowód twierdzenia 3.7 o złożeniu rozpoznawalnych języków śladów.

Dowód twierdzenia 3.7. Niech $K = \bigcup T$ i $L = \bigcup S$. Pokażemy, że język słów KL ma skończony stopień rozproszenia, a więc z lematu 4.10, indukowany język śladów $[KL] = TS$ jest rozpoznawalny.

Nich $uv \in \overline{KL}$, gdzie $u, v \in A^*$. Z definicji zbiorów K i L, istnieją słowa $x, y \in A^*$ takie, że $x \in K$, $y \in L$ oraz $[uv] = [xy]$. Z lematu Levi'ego 3.3 istnieją słowa $u', v', u'', v'' \in A^*$ takie, że

$$[u] = [u'u''], \quad [v] = [v'v''], \quad [x] = [u'v'], \quad [y] = [u''v''],$$

oraz $u''Iv'$. Ponieważ K i L są domknięte, to $u'u'' \in K$ i $v'v'' \in L$. Stąd $u'v'u''v'' \in KL$ oraz stopień rozproszenia KL jest co najwyżej 2.

□

Z lematu Hashiguchi'ego otrzymujemy następujący wniosek.

Wniosek 4.11. *Klasa rozpoznawalnych języków śladów Rec jest równa klasie indukowanej przez klasę języków o skończonym stopniu rozproszenia,*

$$Rec = [FinRank].$$

Dowód. Zawieranie z prawa na lewo $\supseteq$ wynika wprost z lematu Hashiguchiego.

Pokażemy zawieranie w drugą stronę. Niech język śladów $T \subseteq A^*/I$ będzie rozpoznawalny. Stąd jego spłaszczenie $\bigcup T \subseteq A^*$ jest regularne. Ponieważ stopień rozproszenia domkniętego języka jest zawsze równy 1, więc $\bigcup T \in FinRank$. W szczególności T jest indukowane przez swoje spłaszczenie, więc $T \in [FinRank]$. □

Odwrócenie lematu Hashiguchi'ego nie jest prawdziwe, co obrazuje poniższy przykład.

Przykład 4.12. Niech $A = \{a, b\}$ oraz aIb. Język słów $L = (ab)^*(a^* \cup b^*)$ indukuje rozpoznawalny język śladów $[L] = A^*/I$, ale stopień rozproszenia $Rank_I(L) = \infty$, bo $rank(a^n, b^n) = n$ dla dowolnego $n \in \mathbb{N}$.

Stwierdzenie 4.13. *Klasa języków słów FinRank jest właściwą podklasą klasy InvRec.*

$$FinRank \subset InvRec$$

Dowód. Zawieranie wynika z lematu Hashiguchi'ego, a przykład 4.12 pokazuje, że zawieranie jest właściwe. □

Teraz przypatrzmy się umiejscowieniu klasy języków śladów $StarCon$ względem klasy $FinRank$. Prostym wnioskiem z definicji jest fakt, że złożenie i suma języków o skończonym stopniu rozproszenia $Rank$ dają nam znów języki o skończonym $Rank$. Natomiast operacja gwiazdki zachowuje się różnie na różnych językach, np. dla aIb, jeśli $L = ab$, to $Rank(L) = 1$, ale już $Rank(L^*) = \infty$. Jeśli weźmiemy język z przykładu 4.12, $L = (ab)^*(a^* \cup b^*)$, to $Rank(L) = \infty$, ale $Rank(L^*) = 1$. Zauważmy jednak, że w obu przykładach wystąpiły języki niespójne. Pokażemy, że dla języków spójnych gwiazdka zachowuje skończony stopień rozproszenia $Rank$.

Lemat 4.14. *Niech $L, K \subseteq A^*$ będą językami słów o skończonym stopniu rozproszenia i niech $Rank(L) = n$ oraz $Rank(K) = m$. Wówczas*

1. $Rank(L \cup K) \leq \max(n, m)$,
2. $Rank(LK) \leq n + m$,
3. *Jeśli L jest językiem spójnym, to* $Rank(L^*) \leq (n + 1)|A| + 1$.

Dowód. Punkty 1 i 2 wynikają z definicji stopnia rozproszenia. Trudniejszy do udowodnienia jest punkt 3.

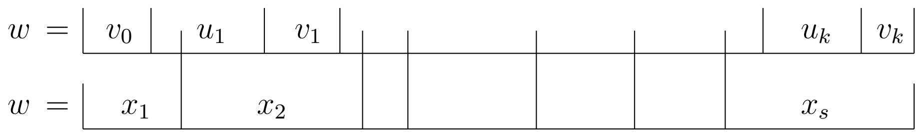
Niech L będzie językiem spójnym oraz $[uv] \in [L^*]$. Wówczas istnieje słowo $w \in L^*$ takie, że $[w] = [uv]$ oraz

(a) $w = v_0u_1v_1 \dots u_kv_k$

(b) $[u_1 \dots u_k] = [u]$

(c) v_iIu_j dla $i < j$.

(d) Niech $w = x_1 \dots x_s$, dla pewnych $x_1, \dots, x_s \in L$.



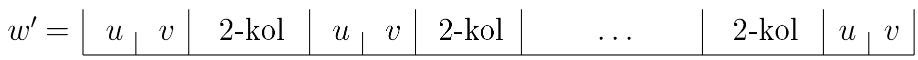
Segmenty u_i, v_i, x_i będziemy nazywać u-segmentami, v-segmentami i L-segmentami odpowiednio. Ponieważ $Rank(L) = n$, to możemy założyć, że liczba u-segmentów w każdym x_i nie przekracza n.

Pokażemy, że liczba L-segmentów, zawierających obydwa rodzaje segmentów, u-segmentów i v-segmentów, (takie segmenty będziemy nazywać 2-kolorowymi) nie jest większa od $|A|$, mocy alfabetu A.

Oznaczmy przez $u(x_i)$ oraz $v(x_i)$ podsłowa x_i składające się z u- i v-segmentów odpowiednio. Niech $x_i \in L$ będzie 2-kolorowym L-segmentem. Ponieważ L jest z założenia językiem spójnym, to x_i jest słowem spójnym, więc istnieją litery a_i w $u(x_i)$ oraz b_i w $v(x_i)$, które są zależne, czyli $a_i D b_i$. Niech x_i, x_j będą 2-kolorowymi i różnymi segmentami, przypuśćmy, że $i < j$. Wówczas na mocy punktu (c) istnieją litery a_i, b_i w x_i oraz a_j, b_j w x_j takie, że $a_i D b_i$, $a_j D b_j$ oraz $b_i I a_j$. Stąd litery a_i, a_j są różne, $a_i \neq a_j$. Ponieważ A zawiera $|A|$ różnych liter, to liczba 2-kolorowych segmentów w słowie w nie przekracza $|A|$.

Niech x_i i x_j będą dwoma kolejnymi 2-kolorowymi segmentami w słowie w. Stąd wszystkie pośrednie segmenty $x_{i+1}, \dots, x_{j-1}$ są 1-kolorowe. Rozważmy złożenie $z_1 z_2 z_3 z_4$, gdzie $z_1 = x_1 \dots x_i$, z_2 jest złożeniem wszystkich u-segmentów występujących w $x_{i+1}, \dots, x_{j-1}$ zachowującym kolejność, z_3 jest zdefiniowane jak z_2, ale dla v-segmentów oraz $z_4 = x_j \dots x_s$. Słowo $z_1 z_2 z_3 z_4$ znów należy do języka L^* i jest równoważne w. W ten sposób dostaliśmy co najwyżej jeden u-segment między x_i a x_j.

Zróbmy powyższe przestawienie między każdymi dwoma 2- kolorowymi segmentami w słowie w oraz przed pierwszym i po ostatnim. Skonstruowaliśmy w ten sposób słowo $w' \in L^*$ takie, że $[w] = [w'] = [uv]$ z co najwyżej $|A|$ oddzielnymi 2-kolorowymi segmentami, co najwyżej jednym u-segmentem między każdą kolejną parą 2-kolorowych segmentów oraz z co najwyżej jednym u-segmentem przed pierwszym i po ostatnim 2-kolorowym.



Teraz wystarczy zauważyć, że liczba u-segmentów w dowolnym 2-kolorowym segmencie jest ograniczona przez $Rank(L) = n$. Stąd całkowita liczba oddzielnych u-segmentów w w' nie przekracza $n|A| + |A| + 1 = (n+1)|A| + 1$.

W ten sposób udowodniliśmy, że jeśli $[uv] \in [L^*]$, to istnieje $w' \in L^*$ takie, że $uv \in [w']$ oraz liczba u-segmentów w słowie w' nie przekracza $(n+1)|A|+1$. Stąd $Rank(L^*) \leq (n+1)|A| + 1$. □

Jako wniosek z powyższego lematu otrzymujemy zawieranie klas

Twierdzenie 4.15. *Każdy język iteracyjnie spójny ma skończony stopień rozproszenia, czyli* $StarCon \subseteq FinRank$.

Dowód. Indukcja strukturalna ze względu na racjonalne wyrażenie iteracyjnie spójne. Dla języków atomowych stwierdzenie jest prawdziwe, bo stopień rozproszenia skończonego języka jest skończony. W kroku indukcyjnym wykorzystuje się punkty 1, 2 i 3 z lematu 4.14. □

Następujący przykład pokazuje, że inkluzja z powyższego twierdzenia jest właściwa.

Przykład 4.16. Niech $L = (ab \cup ba \cup aa \cup bb)^*$ z aIb. Stopień rozproszenia $Rank(L) = 1 < \infty$, ponieważ $L = \bigcup[L]$ jest domknięty, ale L nie jest iteracyjnie spójny, co pokazała Klunder w [18].

Podsumujmy uzyskane wyniki.

Twierdzenie 4.17. *Klasa* $StarCon$ *jest właściwą podklasą klasy* $FinRank$, $StarCon \subset FinRank$.

Dowód. Twierdzenie wynika wprost z twierdzenia 4.15 i przykładu 4.16. □

Twierdzenie 4.18. *Klasa języków regularnych* Reg *z jej podklasami* $InvRec$, $FinRank$ *i* $StarCon$ *tworzy ściśle malejącą hierarchię*

$$Reg \supset InvRec \supset FinRank \supset StarCon.$$

4.2 Własności boolowskie klasy $StarCon$

Mówimy, że rodzina zbiorów jest algebrą Boole'a o ile jest zamknięta na teoriomnogościowe działania sumy, iloczynu oraz różnicy. Klasa Reg języków regularnych tworzy algebrę Boole'a. W monoidach śladów inne własności mają klasy języków racjonalnych i rozpoznawalnych. Klasa racjonalnych języków śladów Rat, indukowana przez klasę Reg, nie jest algebrą Boole'a, natomiast klasa rozpoznawalnych języków śladów Rec jest.

Powstaje pytanie, czy któraś z klas $InvRec$, $FinRank$, $StarCon$ tworzy algebrę Boole'a?

Każda z klas języków słów $InvRec$, $FinRank$, $StarCon$ indukuje klasę rozpoznawalnych języków śladów Rec, $Rec = [InvRec] = [FinRank] = [StarCon]$. Ponieważ każda z tych klas zawiera cały monoid wolny A^* oraz jest zamknięta na sumę, wystarczy sprawdzić, czy są zamknięte na dopełnienie.

Poniższy przykład pokazuje, że żadna z klas $InvRec$, $FinRank$, $StarCon$ nie jest algebrą Boole'a.

Przykład 4.19. Niech $A = \{a, b\}$ oraz aIb. Oczywiście język $L = (ab)^*$ jest spoza klasy $InvRec$, gdyż $\bigcup[L] \cap a^*b^* = \{a^n b^n \mid n \in \mathbb{N}\} \notin Reg$. Jednakże dopełnienie L

$$A^* \setminus L = b(a \cup b)^* \cup (a \cup b)^* a \cup (a \cup b)^* aa(a \cup b)^* \cup (a \cup b)^* bb(a \cup b)^*$$

jest językiem iteracyjnie spójnym. Korzystając z twierdzenia 4.18, otrzymujemy, że żadna z klas *InvRec*, *FinRank*, *StarCon* nie jest zamknięta na dopełnienie.

Rozważmy kolejne pytanie, czy któraś z klas *InvRec*, *FinRank*, *StarCon* jest zamknięta na iloczyn zbiorów?

Poniższy przykład pokazuje, że klasa *InvRec* nie jest zamknięta na iloczyn.

Przykład 4.20. Niech $A = \{a, b\}$ oraz aIb. Niech $L = (ab)^*(a^* \cup b^*)$ oraz $K = (a^* \cup b^*)(ab)^*$. Ponieważ $[L] = [K] = A^*/I \in Rec$, oba języki są w klasie *InvRec*. Jednak część wspólna $L \cap K = (ab)^* \cup a^* \cup b^*$ jest poza klasą *InvRec*, bo $[L \cap K] \notin Rec$.

Języki L i K z powyższego przykładu nie mają skończonego stopnia rozproszenia. Następny przykład jest ogólniejszy. Pokazuje, że przecięcie języków z klasy *FinRank* nie tylko może wyprowadzić poza klasę *FinRank*, ale nawet z klasy *InvRec*.

Przykład 4.21. Niech $A = \{a, b\}$ oraz aIb. Weźmy języki $L = a^*(ab)^*b^*$ oraz $K = b^*(ab)^*a^*$. Można pokazać, że $Rank(L) = Rank(K) = 2$. Część wspólna $L \cap K = (ab)^* \cup a^* \cup b^*$ jest poza klasą *InvRec*, więc również poza klasą *FinRank*.

Klunder pokazała w [18], że języki L i K z powyższego przykładu nie są iteracyjnie spójne. W związku z tym, problem przecięcia dla języków iteracyjnie spójnych pozostaje otwarty.

4.3 Problemy decyzyjne

Przypomnijmy ścisłą hierarchię podklas klasy języków regularnych *Reg*:

$$Reg \supset InvRec \supset FinRank \supset StarCon.$$

Rozważmy następujące problemy decyzyjne:

Problem 1. Czy $L \in Reg$ należy do *InvRec*?
Problem 2. Czy $L \in Reg$ należy do *FinRank*?
Problem 3. Czy $L \in Reg$ należy do *StarCon*?

Problem 1 jest równoważny klasycznemu problemowi decyzyjnemu

Czy $T \in Rat$ jest rozpoznawalny?

Berstel w [1] pokazał, że problem ten jest nierozstrzygalny. Problem 2 jest otwartym problemem postawionym w pracy [29].

Trzeci problem jest po raz pierwszy postawiony w pracy [19]. W wersji dla języków śladów „Czy $T \in Rat$ należy do $[StarCon]$?” jest nierozstrzygalny, bo $[StarCon] = Rec$, a Problem 1 jest nierozstrzygalny. Problem 3 można sformułować następująco

„Czy dla danego języka regularnego i relacji niezależności istnieje iteracyjnie spójne wyrażenie racjonalne definiujące dany język?”

Rozstrzygalność dla wyrażeń racjonalnych, (czy dane wyrażenie jest iteracyjnie spójne) nie jest rozwiązaniem problemu dla języków słów. Podobnie, w [18] Klunder opisała automatową charakteryzację iteracyjnie spójnych języków słów. Jednak przedstawiona konstrukcja automatu oparta jest na istnieniu iteracyjnie spójnego wyrażenia racjonalnego. Wobec tego, Problem 3 pozostaje nadal otwarty.

Rozdział 5

Bezgwiazdkowe języki słów

Kolejną interesującą klasą podzbiorów monoidów jest klasa podzbiorów bezgwiazdkowych. W monoidach wolnych klasa ta ma szczególne własności, opisane twierdzeniami Schützenbergera i McNaughtona, Paperta. W monoidach śladów zachodzą analogiczne twierdzenia, które zostaną podane w następnym rozdziale wraz z nowymi dowodami. W tym rozdziale zostanie zdefiniowana nowa operacja – bezgwiazdkowa gwiazdka – i przy jej użyciu przedstawiona zostanie nowa charakteryzacja bezgwiazdkowych języków słów.

Definicja 5.1. Niech M będzie monoidem. Klasą $SF(M)$ **bezgwiazdkowych podzbiorów** M nazywamy najmniejszą klasę podzbiorów M spełniającą warunki:

- $\emptyset \in SF(M)$, $\{m\} \in SF(M)$ dla $m \in M$,
- Jeśli $X, Y \in SF(M)$, to $X \cup Y, XY, X' \in SF(M)$.

Podobnie jak wyrażenia racjonalne, definiujemy wyrażenia bezgwiazdkowe.

Definicja 5.2. Zbiorem **wyrażeń bezgwiazdkowych** $SFEX(M)$ nad monoidem M nazywamy najmniejszy zbiór słów nad alfabetem $M \cup \{\cup, \cdot, (,), ', \emptyset\}$ taki, że

- $\emptyset \in SFEX(M)$ – symbol zbioru pustego jest wyrażeniem bezgwiazdkowym,
- dla każdego elementu $m \in M$, słowo $(m) \in SFEX(M)$,
- jeśli słowa $X, Y \in SFEX(M)$ są wyrażeniami bezgwiazdkowymi, to $(X \cup Y)$, $(X \cdot Y)$ oraz $(X)'$ są wyrażeniami bezgwiazdkowymi.

Przykład 5.3. Każdy monoid M jest zbiorem bezgwiazdkowym, ponieważ $M = \emptyset'$.

Ponieważ klasa $SF(M)$ jest zamknięta na sumę zbiorów i dopełnienie, to jest również zamknięta na operacje iloczynu i różnicy zbiorów.

Przykład 5.4. Niech A będzie skończonym alfabetem i $B \subseteq A$ podalfabetem A. Wówczas zbiór $B^* \in SF(A^*)$ jest bezgwiazdkowy:

$$B^* = (\emptyset'(A \setminus B)\emptyset')'.$$

Przykład 5.5. Niech $A = \{a, b\}$ będzie alfabetem. Wówczas język $L = (ab)^*$ jest bezgwiazdkowy, bo $L = (b\emptyset' \cup \emptyset' a \cup \emptyset' aa\emptyset' \cup \emptyset' bb\emptyset')'$.

W monoidach, w których złożenie zachowuje rozpoznawalność, np. monoidach wolnych i monoidach śladów, języki bezgwiazdkowe są rozpoznawalne.

5.1 Twierdzenie Schützenbergera

Z twierdzenia Kleene'go wynika, że w monoidzie wolnym każdy język bezgwiazdkowy jest regularny. Klasa języków bezgwiazdkowych w monoidzie wolnym ma szczególne własności, o czym mówi twierdzenie Schützenbergera. Do przedstawienia tego twierdzenia potrzebne nam będą pojęcie monoidu i podzbioru aperiodycznego.

Definicja 5.6. Monoid M nazywamy **monoidem aperiodycznym**, jeśli jest skończony oraz istnieje liczba naturalna $n \in \mathbb{N}$ taka, że dla dowolnego elementu $m \in M$, zachodzi $m^n = m^{n+1}$. Najmniejsze takie n będziemy nazywać **indeksem monoidu** M i oznaczać przez $i(M)$.

Definicja 5.7. Niech M będzie monoidem, $X \subseteq M$ jego podzbiorem i M_X monoidem syntaktycznym zbioru X. Mówimy, że zbiór X jest **aperiodyczny**, jeśli monoid syntaktyczny M_X jest aperiodyczny.
Równoważnie: Zbiór X jest aperiodyczny jeśli X jest rozpoznawalny oraz

$$(\exists n \in \mathbb{N})(\forall x, y, z \in M)\ xy^n z \in X \iff xy^{n+1}z \in X$$

Klasę aperiodycznych podzbiorów monoidu M będziemy oznaczać przez $AP(M)$.

Przykład 5.8. Niech $M = a^*$ będzie monoidem wolnym nad alfabetem jednoliterowym. Wówczas język $L = (aa)^*$ nie jest aperiodyczny, ponieważ dla dowolnej liczby naturalnej $n \in \mathbb{N}$, słowo $a^n \in (aa)^*$ wtedy i tylko wtedy, gdy $a^{n+1} \notin (aa)^*$. Monoid syntaktyczny M_L języka L ma dwa elementy – $[\varepsilon]$, $[a]$ i działanie określone jest następująco

$\cdot$	ε	a
ε	ε	a
a	a	ε

Zauważmy, że monoid M_L w powyższym przykładzie jest izomorficzny z grupą $\mathbb{Z}_2$. Łatwo pokazać, że nie jest to możliwe w monoidzie aperiodycznym, mianowicie monoidy aperiodyczne nie zawierają podgrup nietrywialnych.

Stwierdzenie 5.9. *Niech M będzie monoidem aperiodycznym o indeksie $i(M) = n$. Jedynym podmonoidem monoidu M będącym grupą jest podmonoid trywialny $\{1_M\}$.*

Dowód. Przypuśćmy, że m^{-1} jest odwrotnością elementu $m \in M$, więc $(m^{-1})^n$ jest odwrotnością elementy m^n. Ale wtedy $m = (m^{-1})^n \cdot m^n \cdot m = (m^{-1})^n \cdot m^n = 1_M$. □

Przykład 5.10. Weźmy język $L = (ab)^*$ z przykładu 5.5. Monoid syntaktyczny opisuje poniższa tabela

$\cdot$	ε	a	b	ab	ba	0
ε	ε	a	b	ab	ba	0
a	a	0	ab	0	a	0
b	b	ba	0	b	0	0
ab	ab	a	0	ab	0	0
ba	ba	0	b	0	ba	0
0	0	0	0	0	0	0

Stąd $a^2 = a^3 = 0$, $b^2 = b^3 = 0$, $(ab)^2 = (ab)^3 = ab$, $(ba)^2 = (ba)^3 = ba$, $\varepsilon^2 = \varepsilon^3 = \varepsilon$, $0^2 = 0^3 = 0$. Ponieważ dla każdego elementu z monoidu, jego kwadrat jest równy sześcianowi, to zbiór L jest aperiodyczny i indeks $i(M_L) = 2$.

Stwierdzenie 5.11. *Niech M będzie dowolnym monoidem. Zbiór rozpoznawalny $X \in Rec(M)$ jest aperiodyczny wtedy i tylko wtedy, gdy*

$$(\exists n)(\forall x \in M_X)(\forall m \geq n)\ x^m = x^n.$$

Dowód. $\Rightarrow$: Z założenia dla dowolnego $x \in M_X$, $x^n = x^{n+1} = xx^{n+1} = \ldots = x^m$, gdzie $m \geq n$.

$\Leftarrow$: Oczywiste. □

Teraz możemy sformułować twierdzenie Schützenberger z [34].

Twierdzenie 5.12 (Schützenberger). *Niech A będzie skończonym alfabetem. Język $L \subseteq A^*$ jest bezgwiazdkowy wtedy i tylko wtedy, gdy jest aperiodyczny.*

Pełny dowód twierdzenia zostanie podany w następnym rozdziale. Tutaj pokażemy, że każdy język bezgwiazdkowy jest aperiodyczny. Dowód pochodzi z pracy [30].

Stwierdzenie 5.13. *Niech A będzie skończonym alfabetem. Jeśli język $L \subseteq A^*$ jest bezgwiazdkowy, to jest aperiodyczny.*

Dowód. Indukcja strukturalna na wyrażeniach bezgwiazdkowych. Dla $L = \emptyset$ i $L = \varepsilon$, indeks $i(M_L) = 0$, dla liter z alfabetu $a \in A$, indeks $i(a) = 2$. Przypuśćmy, że monoidy ilorazowe zbiorów $L, K \subseteq A^*$ mają skończone indeksy. Oczywiście $i(M_L \cup M_K) \leq \max(i(M_L), i(M_K))$ oraz $i(M_{L'}) = i(M_L)$. Pozostaje pokazać, że $i(M_{LK}) \leq i(M_L) + i(M_K)$. Przypuśćmy, że $uv^n w \in LK$ i $n = i(M_L) + i(M_K)$. Ponadto możemy założyć, że $n > 0$, ponieważ w przypadku $n = 0$, zbiór $LK = \emptyset$ lub $LK = \varepsilon$, czyli jest aperiodyczny. Jeśli $n > 0$, to istnieje rozkład $v = rs$ oraz $n = h + k + 1$ takie, że $uv^h r \in L$ oraz $sv^k w \in K$. Wówczas $h \geq i(M_L)$ lub $k \geq i(M_K)$, czyli $uv^{h+1} r \in L$ lub $sv^{k+1} w \in K$, stąd $uv^{n+1} w \in LK$. Dowód, że jeśli $uv^{n+1} w \in LK$, to $uv^n w \in LK$ przebiega podobnie, więc $i(M_{KL}) = n$. □

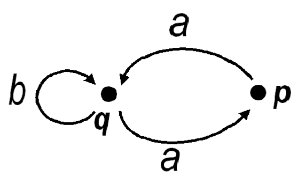
Prostym wnioskiem z twierdzenia Schützenbergera jest fakt, że język $(aa)^*$ z przykładu 5.8 nie jest bezgwiazdkowy.

5.2 Języki bezgwiazdkowe a automaty

W monoidach wolnych istnieje charakteryzacja języków bezgwiazdkowych za pomocą automatów. Charakteryzacja wynika z twierdzenie Schützenbergera i omówiona zastanie w tym podrozdziale.

Niech A będzie skończonym alfabetem i $\mathcal{A} = \langle A, Q, \delta, q_0, F\rangle$ skończonym automatem. Ciąg $q_1a_1q_2\dots q_{n-1}a_{n-1}q_n$ nazywamy ścieżką w automacie $\mathcal{A}$, jeśli $(q_i, a_i, q_{i+1}) \in \delta$, dla $i = 1, \dots, n-1$. Pętlą nazywamy ścieżkę $q_1a_1\dots a_{n-1}q_n$, gdzie $q_1 = q_n$. Pętlę nazywamy **nietrywialną**, jeśli $q_1a_1\dots a_{n-1}q_n = q_1uq_iu^kq_1$, gdzie $q_1 \neq q_i$, a **prostą** w przeciwnym wypadku. Mówimy, że automat jest **aperiodyczny**, jeśli wszystkie jego pętle są proste.

Przykłady automatu z pętlami prostą i nietrywialną przedstawia rysunek 5.1



Rysunek 5.1: Pętla qbq jest prosta, $qapaq$ jest nietrywialna

Niech $L \subseteq A^*$ będzie językiem słów i $\approx \subseteq A^* \times A^*$ relacją syntaktyczną języka L.

Lemat 5.14. *Jeśli $L \subseteq A^*$ jest regularnym i nieaperiodycznym językiem słów, to istnieje słowo $w \in A^*$ takie, że dla każdego $n \geq 0$ zachodzi $w^n \not\approx w^{n+1}$.*

Dowód. Przypuśćmy, że dla każdego $w \in A^*$

$$(\exists n)\ w^n \approx w^{n+1}. \tag{5.1}$$

Z każdej klasy abstrakcji kongruencji syntaktycznej wybierzmy po jednym reprezentancie. Ponieważ język L jest regularny, to ich liczba jest skończona. Niech $w_1, \dots, w_k$ będą ich reprezentantami oraz $n_1, \dots, n_k$ liczbami spełniającymi warunek (5.1) dla $w_1, \dots, w_k$ odpowiednio. Wówczas dla dowolnego $i = 1, \dots, k$ i $u_i \approx w_i$ zachodzi $u_i^{n_i} \approx u_i^{n_i+1}$. Wówczas ze stwierdzenia 5.11 dla $n = \max\{n_1, \dots, n_k\}$ i dowolnego $w \in A^*$, mamy $w^n \approx w^{n+1}$. Stąd język L jest aperiodyczny. Sprzeczność. $\square$

Poniższe twierdzenie daje charakteryzację automatów akceptujących języki bezgwiazdkowe.

Twierdzenie 5.15. *Niech A będzie skończonym alfabetem i $L \subseteq A^*$ regularnym językiem słów. Wówczas następujące zdania są równoważne:*

1. *Język L jest bezgwiazdkowy.*

2. *Język L jest aperiodyczny.*

3. *Minimalny deterministyczny automat akceptujący L jest aperiodyczny.*

4. *Istnieje aperiodyczny automat akceptujący L.*

Dowód. Równoważność $1 \Leftrightarrow 2$ jest dokładnie twierdzeniem Schützenbergera 5.12.

$2 \Rightarrow 3$: Niech $\mathcal{A} = \langle A, Q, \delta, q_0, F \rangle$ będzie m.d.a. akceptujący język L. Przypuśćmy, że $\mathcal{A}$ nie jest aperiodyczny. Niech $qwpw^{k-1}q$ będzie nietrywialną pętlą w $\mathcal{A}$. Niech $\mathcal{A}_{q0/q} = \langle A, Q, \delta, q_0, q \rangle$. Ponieważ $\mathcal{A}$ jest minimalny, to język $L(\mathcal{A}_{q0/q})$ jest niepusty. Niech $\mathcal{A}_q = \langle A, Q, \delta, q, F \rangle$ i $\mathcal{A}_p = \langle A, Q, \delta, p, F \rangle$. Ponieważ automat $\mathcal{A}$ jest minimalny i $p \neq q$, to $L(\mathcal{A}_q) \neq L(\mathcal{A}_p)$. Stąd zachodzi co najmniej jeden z przypadków:

(a) istnieje $z \in L(\mathcal{A}_q)$ takie, że $z \notin L(\mathcal{A}_p)$,

(b) istnieje $z \in L(\mathcal{A}_p)$ takie, że $z \notin L(\mathcal{A}_q)$.

Weźmy słowo $x \in L(\mathcal{A}_{q0/q})$. Ponieważ automat $\mathcal{A}$ jest deterministyczny, to dla dowolnej liczby naturalnej i zachodzi jeden z przypadków:

(a) $xw^{ik}z \in L$ i $xw^{ik+1}z \notin L$, stąd $w^{ik} \not\approx w^{ik+1}$;

(b) $xw^{ik}z \notin L$ i $xw^{ik+1}z \in L$, stąd $w^{ik} \not\approx w^{ik+1}$;

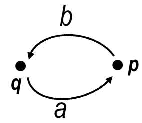
Ze stwierdzenia 5.11 wynika, że język L nie jest aperiodyczny.

$3 \Rightarrow 4$: Oczywiste.

$4 \Rightarrow 2$: Przypuśćmy, że automat $\mathcal{A}$ jest aperiodycznym i język $L = L(\mathcal{A}) \subseteq A^*$ nie jest aperiodyczny. Wówczas, z lematu 5.14, istnieje słowo $w \in A^*$ takie, że dla każdego $n \in \mathbb{N}$ zachodzi $w^n \not\approx w^{n+1}$. Stąd dla dowolnego n, słowo w^n jest segmentem pewnego słowa z L, tzn. $(\forall n)(\exists x, z \in A^*)\ xw^nz \in L$ (bo w przeciwnym wypadku $w^n \approx w^{n+1}$). Stąd w automacie $\mathcal{A} = \langle A, Q, \delta, q_0, F \rangle$ akceptującym L istnieje pętla postaci qw^iq, ponieważ każde słowo z L zawierające segment w^n dla $n \geq |Q|$ musi przejść przez taką pętlę. Z założenia w automacie $\mathcal{A}$ występują tylko pętle proste. Niech $n \geq |Q|$ i niech $xw^nz \in L$. Wówczas obliczenie xw^nz musi przejść przez pętlę qwq, więc pełne obliczenie jest postaci $q_0xq_iw^i\mathbf{qwq}w^jq_jzq_f$. Stąd również słowo $xw^{n+1}z \in L$ (o jedno przejście qwq więcej). Podobnie, jeśli $xw^{n+1}z \in L$, to $xw^nz \in L$ (o jedno przejście qwq mniej). Stąd $w^n \approx w^{n+1}$. Sprzeczność. □

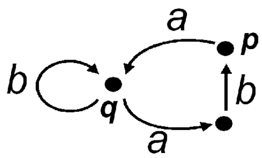
Powyższe twierdzenie, ale bez zdania 4, zostało udowodnione w [22]. Z wykorzystaniem lematu 5.14 dostajemy dowód implikacji $4 \Rightarrow 2$. W punkcie 4 nie ma ograniczeń na automat – może być niedeterministyczny.

Przykład 5.16. Na rysunku 5.2 przedstawiony jest minimalnym deterministycznym automat akceptujący język $L = (ab)^*$. Automat ma tylko jedną pętlę $qapbq$ i jest to pętla prosta. W kolejny sposób pokazaliśmy, że język $(ab)^*$ jest bezgwiazdkowy.



Rysunek 5.2: M.d.a. dla języka $(ab)^*$

Przykład 5.17. Niech $A = \{a, b\}$. M.d.a dla języka $L = (aba \cup b)^*$ przedstawia rysunek 5.3. Stan q jest stanem początkowym i jedynym końcowym. Ponieważ pętla $qabpabq$ jest nietrywialna, język L nie jest aperiodyczny, więc nie jest bezgwiazdkowy.



Rysunek 5.3: M.d.a. dla $(aba \cup b)^*$

5.3 Bezgwiazdkowa gwiazdka

Wiemy, że klasyczne wyrażenia regularne wyprowadzają poza klasę języków bezgwiazdkowych (twierdzenie 5.12 i przykład 5.8). Operacją wyprowadzającą jest gwiazdka Kleene'go. Zastępując klasyczną gwiazdkę pewnym jej ograniczeniem, nazwanym gwiazdką bezgwiazdkową, możemy opisywać języki bezgwiazdkowe przy pomocy klasycznych wyrażeń regularnych (choć nie wszystkich). Uzyskujemy w ten sposób nową charakteryzację bezgwiazdkowych języków słów i śladów, co będzie tematem pozostałej części rozprawy.

Definicja 5.18. Niech M będzie monoidem i $X \subseteq M$ podzbiorem.

- Operację $^\times$ **bezgwiazdkowej gwiazdki** definiujemy w następujący sposób:
$$X^\times = \begin{cases} X^*, & \text{gdy } X^* \text{ jest bezgwiazdkowy,} \\ \text{nieokreślone} & \text{w przeciwnym przypadku} \end{cases}.$$
- Wyrażenie racjonalne zbudowane z użyciem operacji sumy, złożenia i bezgwiazdkowej gwiazdki nazywać będziemy SFS-**wyrażeniami**.

Klasa $SFS(M)$ jest najmniejszą klasą podzbiorów monoidu M zbudowaną z atomów za pomocą operacji sumy, złożenia i bezgwiazdkowej gwiazdki; elementy klasy $SFS(M)$ nazywamy SFS-językami.

Zauważmy, że zgodnie z definicją, SFS-wyrażenia są klasycznymi wyrażeniami racjonalnymi, w których gwiazdki są zwykłymi gwiazdkami Kleene'go, tyle że dającymi w wyniku języki bezgwiazdkowe. W związku z tym w dalszej części rozprawy bezgwiazdkowa gwiazdka będzie oznaczana zwykłym symbolem $*$.

Pokażemy, że bezgwiazdkowa gwiazdka potrafi w pełni zastąpić operację dopełnienia w opisie języków bezgwiazdkowych. Tym samym, uzyskamy nową charakteryzację języków bezgwiazdkowych, bardzo pomocną w dalszych rozważaniach.

Twierdzenie 5.19. *W monoidach wolnych skończenie generowanych zachodzi równość klas $SF = SFS$.*

Dowód. Zawieranie $SF \supseteq SFS$ wynika wprost z definicji.

Pokażemy zawieranie $SF \subseteq SFS$. Niech A będzie skończonym alfabetem. Weźmy minimalny deterministyczny automat $\mathcal{A} = \langle A, Q, \delta, q_1, F \rangle$ akceptujący bezgwiazdkowy język $L \subseteq A^*$. Z twierdzenia 5.15 wynika, że w automacie $\mathcal{A}$ nie ma cykli nietrywialnych. Ponumerujmy stany automatu kolejnymi liczbami naturalnymi od 1 do n, gdzie n jest liczbą stanów automatu $\mathcal{A}$. Niech 1 będzie numerem stanu początkowego.

Pokażemy, że wyrażenie regularne konstruowane dla automatu $\mathcal{A}$ przy pomocy konstrukcji McNaughtona i Yamady z [21] i opisanej w [16], jest SFS-wyrażeniem. Przypomnijmy tę konstrukcję.

Przez $R_{ij}^{(k)}$ oznaczmy wyrażenie regularne definiujące język słów w, które są etykietami takich ścieżek w automacie $\mathcal{A}$ ze stanu i do stanu j, że wszystkie pośrednie stany w ścieżkach mają numery nie większe niż k. Konstrukcja wyrażeń $R_{ij}^{(k)}$ jest indukcyjna, zaczynamy od $k = 0$. W tym przypadku rozważane ścieżki nie przechodzą przez żaden pośredni stan, tzn. są długości 0 lub 1. W zależności od i oraz j otrzymujemy dwa przypadki:

1. Jeśli $i \neq j$, to
$$R_{ij}^{(0)} = a_1 + \ldots + a_l,$$
gdzie $a_1, \ldots, a_l \in A$ są etykietami łuków w automacie $\mathcal{A}$ ze stanu i do stanu j. W szczególności, gdy takie łuki nie istnieją,
$$R_{ij}^{(0)} = \emptyset.$$

2. Jeśli $i = j$, to
$$R_{ii}^{(0)} = a_1 + \ldots + a_l + \varepsilon,$$
gdzie $a_1, \ldots, a_l \in A$ są etykietami pętelek w automacie ze stanu i do i. W szczególności, gdy nie ma takich pętelek, to
$$R_{ii}^{(0)} = \varepsilon.$$

Przypuśćmy, że dla ustalonego k mamy skonstruowane wszystkie wyrażenia $R_{ij}^{(k-1)}$. Wówczas dla dowolnych $i, j \in \{1, \ldots, n\}$ zachodzi następujący wzór

$$R_{ij}^{(k)} = R_{ij}^{(k-1)} + R_{ik}^{(k-1)} \cdot (R_{kk}^{(k-1)})^* \cdot R_{kj}^{(k-1)}. \tag{5.2}$$

Wyrażenie regularne wyznaczające język L uzyskane z tej konstrukcji jest postaci

$$R = \bigcup_{j \in F} R_{1j}^{(n)}. \tag{5.3}$$

Zauważmy, że jeśli wyrażenia $R_{1j}^{(n)}$ są SFS-wyrażeniami, to również wyrażenie R jest SFS. Pokażemy indukcyjnie, że każde wyrażenie $R_{ij}^{(k)}$, dla dowolnego i, j oraz k są SFS.

W przypadku dla $k = 0$ konstruowane wyrażenia oczywiście są SFS, bo nie występuje w nich żadna gwiazdka.

Załóżmy, że wyrażenia $R_{ij}^{(k-1)}$, dla dowolnych i oraz j, są SFS. Pokażemy, że dla dowolnych i oraz j wyrażenia $R_{ij}^{(k)}$ są SFS. Zauważmy, że we wzorze na wyrażenie $R_{ij}^{(k)}$, gdy $k > 0$, gwiazdki występują jedynie nad wyrażeniami $R_{kk}^{(k-1)}$. Aby udowodnić, że dowolne wyrażenie $R_{ij}^{(k)}$ jest SFS, wystarczy pokazać, że język $L(R_{kk}^{(k-1)})^*$ jest bezgwiazdkowy.

Do dowodu faktu, że język $L(R_{kk}^{(k-1)})^*$ jest bezgwiazdkowy wykorzystamy automat $\mathcal{A}$. Skonstruujemy automat akceptujący język $L((R_{kk}^{(k-1)})^*)$, który nie posiada nietrywialnych cykli. Z twierdzenia 5.15, istnienie takiego automatu dowodzi bezgwiazdkowości akceptowanego języka. Skonstruowany w ten sposób automat nie musi być jednak minimalny.

Dla dowolnego $0 < k \leq n$ zdefiniujmy następujący automat

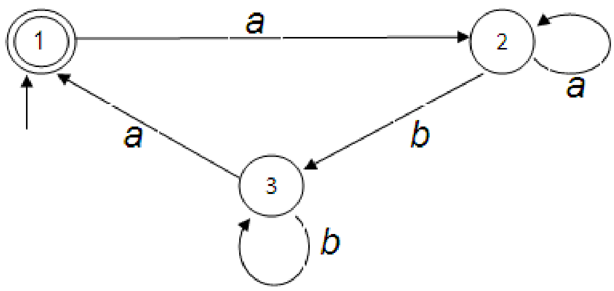
$$\mathcal{A}_k = \langle A, \{1, \ldots, k\}, \delta_k, k, \{k\} \rangle,$$

gdzie funkcja przejścia δ_k jest obcięciem funkcji δ automatu $\mathcal{A}$ do zbioru $1, \ldots, k$. Innymi słowy, automat $\mathcal{A}_k$ powstaje z automatu $\mathcal{A}$ przez usunięcie stanów o numerze większym od k oraz przez usunięcie wszystkich łuków do nich prowadzących. Zauważmy, że taki automat akceptuje język, który jest zbiorem słów w będących etykietami ścieżek ze stanu k do k przechodzących przez stany o numerze nie większym od k. Stan k może powtarzać się dowolnie wiele razy, więc akceptowany język jest dokładnie językiem definiowany przez wyrażenie $(R_{kk}^{(k-1)})^*$. Ponadto automat $\mathcal{A}_k$ nie ma nietrywialnych cykli, bo jest fragmentem automatu $\mathcal{A}$, a ten nie ma cykli nietrywialnych.

Zatem ze wzoru (5.2) wyrażenie $R_{ij}^{(k)}$ jest SFS, co kończy dowód indukcyjny.

Wobec powyższego i ze wzoru (5.3), R jest SFS-wyrażeniami. □

Przykład 5.20. Niech $A = \{a, b\}$ i $L \subseteq A^*$ będzie językiem akceptowanym przez automat z rysunku 5.4.



Rysunek 5.4: Automat akceptujący L

Kolejne tabelki przedstawiają uzyskane podczas konstrukcji języki $L(R_{ij}^k)$ z automatu (k w lewym górnym rogu, i numer wiersza, j numer kolumny).

0	1	2	3
1	ε	a	$\emptyset$
2	$\emptyset$	$a \cup \varepsilon$	b
3	a	$\emptyset$	$b \cup \varepsilon$

1	1	2	3
1	ε	a	$\emptyset$
2	$\emptyset$	$a \cup \varepsilon$	b
3	a	aa	$b \cup \varepsilon$

2	1	2	3
1	ε	aa^*	aa^*b
2	$\emptyset$	a^*	a^*b
3	a	aaa^*	$\varepsilon \cup b \cup aaa^*b$

Uzyskane w tej konstrukcji wyrażenie SFS dla języka $L = L(R)$ jest postaci $R = R_{11}^{(3)} = \varepsilon \cup aa^*b(b \cup aaa^*b)^*a$. Zauważmy, że $L = (aa^*bb^*a)^*$; wyrażenie otrzymane jako wynik algorytmu McNaughtona i Yamady nie jest na ogół najprostszym SFS-wyrażeniem dla danego języka.

5.4 Logika pierwszego rzędu w monoidach wolnych

Niech A^* będzie monoidem wolnym i $w = a_1 \dots a_n$ słowem długości n. Modelem słowa w nazywamy trójkę $\underline{w} = (V, \prec, \lambda)$, gdzie $V = \{1, \dots, n\}$ jest zbiorem pozycji w słowie w, $\prec \subseteq V \times V$ jest naturalnym liniowym porządkiem na V oraz $\lambda\colon V \to A$ jest funkcją etykietującą $\lambda(i) = a_i$.

W formułach pierwszego rzędu używamy zmiennych $x, y, \dots$ odpowiadających pozycjom w słowie. Formuły budowane są z formuł atomowych

$$x = y,\ x \prec y,\ \lambda(x) = a \text{ dla } a \in A$$

przy użyciu alternatywy $\vee$, koniunkcji $\wedge$, negacji $\neg$, implikacji $\to$ i równoważności $\leftrightarrow$ oraz kwantyfikatorów egzystencjalnego $\exists$ i ogólnego $\forall$.

Zapis $\varphi(x_1, \dots, x_n)$ oznacza, że w formule φ występuje n zmiennych wolnych (niezwiązanych z kwantyfikatorami) $x_1, \dots, x_n$. Formułę nazywamy zdaniem, gdy nie występują w niej zmienne wolne. Jeśli zdanie ψ jest spełnione w modelu $\underline{w}$ słowa w, to piszemy $\underline{w} \models \psi$. Językiem definiowanym przez zdanie ψ nazywamy język $L(\psi) = \{w \in A^* \mid \underline{w} \models \psi\}$. Klasę języków definiowalnych w logice pierwszego rzędu w monoidzie A^* oznaczamy przez $FO(A^*)$.

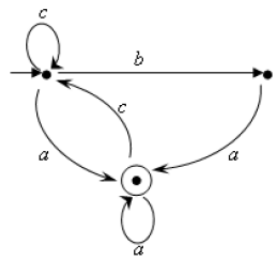
Przykład 5.21. Formuła pierwszego rzędu

$$S(x, y) = x \prec y \wedge \neg\exists z(x \prec z \wedge z \prec y)$$

opisuje relację bezpośredniego następnika pozycji w słowie.

Przykład 5.22. Niech $A = \{a, b, c\}$ i L językiem akceptowanym przez automat $\mathcal{A}$ z rysunku 5.5.
Język L można opisać za pomocą formuły pierwszego rzędu

$$\begin{aligned}\varphi_1 \quad : \quad & \neg\exists x\exists y(S(x, y) \wedge \lambda(x) = a \wedge \lambda(y) = b) \wedge \\ & \forall x(\lambda(x) = b \to \exists y(S(x, y) \wedge \lambda(y) = a)) \\ & \wedge\exists x(\neg\exists y S(x, y) \wedge \lambda(x) = a).\end{aligned}$$



Rysunek 5.5: Skończony automat $\mathcal{A}$

Język L jest bezgwiazdkowy, wyrażenie bezgwiazdkowe jest

$$L = (\emptyset' ab \emptyset' \cup \emptyset' bb \emptyset' \cup \emptyset' bc \emptyset' \cup \emptyset' b \cup \emptyset' c)'.$$

W książce [22] podane zostało następujące powiązanie między bezgwiazdkowymi językami słów a językami słów definiowalnymi w logice pierwszego rzędu.

Twierdzenie 5.23 (McNaughton, Papert 1971). *Niech A będzie skończonym alfabetem. Język słów $L \subseteq A^*$ jest bezgwiazdkowy wtedy i tylko wtedy, gdy jest definiowalny w logice pierwszego rzędu.*

$$SF(A^*) = FO(A^*).$$

Rozdział 6

Bezgwiazdkowe języki śladów

W tym rozdziale zostaną przedstawione znane wyniki dotyczące bezgwiazdkowych języków śladów wraz z nowymi dowodami. Ponadto zostaną opisane nowe charakteryzacje – leksykograficzna oraz wykorzystująca pojęcie bezgwiazdkowej gwiazdki.

Przypomnijmy, że dla ustalonego monoidu M, klasa zbiorów bezgwiazdkowych $SF(M)$ jest najmniejszą rodziną zbiorów, do której należą singletony i zbiór pusty, zamknięta na operacje sumy, złożenia i dopełnienia.

6.1 Aperiodyczne języki śladów

Schützenberger [34] udowodnił równość klas języków aperiodycznych i języków bezgwiazdkowych w monoidach wolnych. W pracy [14] Guaiana, Restivo i Salemi pokazali, że również w monoidach śladów te klasy są sobie równe. Poniższe twierdzenie wraz dowodem zostało przedstawione w pracach [14] oraz [13].

Twierdzenie 6.1 (Guaiana, Restivo, Salemi). *Niech A^*/I będzie monoidem śladów. Język śladów $T \subseteq A^*/I$ jest bezgwiazdkowy wtedy i tylko wtedy, gdy T jest aperiodyczny.*

Dowód twierdzenia Schützenbergera, że każdy aperiodyczny język słów jest bezgwiazdkowy jest skomplikowany, ale bez trudu można go uogólnić dla języków śladów, co zauważyli autorzy artykułu [14]. Dowód będzie przedstawiony w dalszej części rozprawy. Guaiana, Restivo i Salemi dowodzą wersję śladową stwierdzenia 5.13 pokazując, że indeks monoidu bezgwiazdkowego języka śladów jest zawsze skończony. Dowód przeprowadzony tą metodą jest długi i kombinatorycznie skomplikowany. Dowód przedstawiony w tym rozdziale, wykorzystujący pojęcie bezgwiazdkowej gwiazdki, jest znacznie prostszy.

6.1.1 Aperiodyczny $\Longrightarrow$ bezgwiazdkowy

Poniższy dowód stwierdzenia 6.2 pochodzi z pracy [30], gdzie był przedstawiony dla języków słów. Niewielka modyfikacja, wprowadzona również w [13], pozwoliła uogólnić go dla języków śladów.

Stwierdzenie 6.2. *Niech A^*/I będzie monoidem śladów. Jeśli język śladów $T \subseteq A^*/I$ jest aperiodyczny, to T jest bezgwiazdkowy.*

Do udowodnienia powyższego stwierdzenia potrzebne są następujące pomocnicze lematy.

Lemat 6.3. *Niech M będzie monoidem aperiodycznym. Wówczas dla dowolnego $q \in M$, jeśli $q = pqr$, gdzie $p, r \in M$, to $q = pq = qr$. Własność tę nazwijmy „prawem częściowego skracania”.*

Dowód. Niech $n = i(M)$. Ponieważ $q = pqr$, to zachodzi ciąg równości $q = p(pqr)r = \ldots = p^n qr^n$. Ponadto z aperiodyczności M, mamy $p^n = p^{n+1}$ oraz $r^n = r^{n+1}$. Stąd otrzymujemy $q = p^{n+1}qr^n = pq$ oraz $q = p^n qr^{n+1} = qr$. □

Lemat 6.4. *Niech M będzie monoidem aperiodycznym, $m \in M$ dowolnym ustalonym elementem monoidu oraz $J = \{r \in M \mid m \notin MrM\}$. Wówczas*

$$m = mM \cap Mm \setminus J.$$

Dowód. Niech $K = mM \cap Mm \setminus J$. Oczywiście $m \in K$, bo $m \cdot 1_M = m = 1_M \cdot m$, czyli $m \in mM \cap Mm$ oraz $m = 1_M \cdot m \cdot 1_M \in MmM$, stąd $m \notin J$.

Niech $n \in K$. Wówczas istnieją $p, q \in M$ takie, że $n = mp = qm$ oraz $u, v \in M$ takie, że $m = unv$. Stąd $m = uqmv$ i korzystając z prawa częściowego skracania otrzymujemy ciąg równości $m = uqm = un = ump = mp = n$. □

Lemat 6.5. *Niech $N = A^*/I$ będzie monoidem śladów, M monoidem aperiodycznym, a $\varphi : A^*/I \to M$ morfizmem monoidów. Wówczas dla dowolnego $m \in M \setminus \{1_M\}$ przeciwobraz elementu m*

$$\varphi^{-1}(m) = U \cdot N \cap N \cdot V \setminus N \cdot W \cdot N, \tag{6.1}$$

gdzie

$$U = \bigcup_{a \in A} \bigcup_{\substack{n \in M \setminus mM \\ n\varphi([a]) \in mM}} \varphi^{-1}(n) \cdot [a],$$

$$V = \bigcup_{a \in A} \bigcup_{\substack{n \in M \setminus Mm \\ \varphi([a])n \in Mm}} [a] \cdot \varphi^{-1}(n),$$

$$\begin{aligned} W \;=\; & \{[a] \mid a \in A \wedge m \notin M\varphi([a])M\} \cup \bigcup_{a,b \in A} \{[a]\varphi^{-1}(n)[b] \mid n \in M \wedge \\ & \wedge m \in M\varphi([a])nM \cap Mn\varphi([b])M \setminus M\varphi([a])n\varphi([b])M\}. \end{aligned}$$

Dowód. $(\subseteq)$: Niech $\alpha \in \varphi^{-1}(m)$ oraz $\beta \in A^*/I$ będzie śladem najkrótszej długości takim, że $\alpha = \beta\gamma$ dla pewnego $\gamma \in A^*/I$ oraz $mM = \varphi(\beta)M$. Gdyby $\beta = [\varepsilon]$, to z faktu, że $mM = M$, wynikałoby istnienie elementu $p \in M$ spełniającego równość $mp = 1$. Korzystając z prawa częściowego skracania $m1_Mp = m1_M$ otrzymujemy, że $m = 1_M$, co jest sprzeczne z założeniem. Stąd $|\beta| \geq 1$.

Niech $\beta = \delta \cdot [a]$, gdzie $\delta \in A^*/I$ oraz $a \in A$ (rozkład nie jest jednoznaczny). Niech $n = \varphi(\delta)$. Wówczas $n\varphi([a])M = mM$ oraz $n \notin mM$, z wyboru β. Stąd $\alpha \in U \cdot N$. Analogicznie, $\alpha \in N \cdot V$ – wybieramy sufiks najkrótszej długości spełniający analogiczne warunki.

Ponadto $\alpha \notin N \cdot W \cdot N$ z definicji zbioru W. Stąd zachodzi zawieranie $\subseteq$ w (6.1).

($\supseteq$) : Przypuśćmy, że α należy do prawej strony równania (6.1) i niech $n = \varphi(\alpha)$. Ponieważ $\alpha \in UN$ i $\alpha \in NV$, to $n \in mM$ i $n \in Mm$. Aby udowodnić, że $m = n$, to z lematu 6.4 wystarczy pokazać, że $m \in MnM$.

Przeprowadźmy dowód przez sprzeczność. Przypuśćmy, że istnieje $m \in MmM$. Wówczas $\alpha = \beta\gamma\delta$ gdzie γ jest śladem najkrótszej długości takim, że $m \notin M\varphi(\gamma)M$. Oczywiście $\gamma \neq [\varepsilon]$. Jeśli $\gamma = [a]$ dla $a \in A$, to $\gamma \in W$ – sprzeczność z założeniem $\alpha \notin NWN$.

Przypuśćmy teraz, że istnieje rozkład śladu $\gamma = [a]\gamma_1[b]$, gdzie $a, b \in A$. Wówczas $m \in M\varphi([a])\varphi(\gamma_1)M$ oraz $m \in M\varphi(\gamma_1)\varphi([b])M$, bo γ miało być najkrótszej długości. Stąd $\gamma \in W$ – sprzeczność i koniec dowodu drugiej inkluzji. □

Dowód stwierdzenia 6.2. Niech $N = A^*/I$. Niech M będzie monoidem aperiodycznym oraz odwzorowanie $\varphi\colon A^*/I \to M$ będzie morfizmem monoidów. Pokażemy indukcyjnie, że przeciwobraz morficzny $\varphi^{-1}(m)$ dla dowolnego elementu $m \in M$ jest bezgwiazdkowy. W szczególności, przeciwobraz morfizmu kanonicznego z monoidu śladów do monoidu syntaktycznego języka T, który z założenia jest aperiodyczny, będzie miał tę własność. Ponieważ z założenia monoid syntaktyczny jest skończony (bo T rozpoznawalny), to również zbiór $\{\varphi(\alpha) \mid \alpha \in T\}$ jest skończony, więc T będzie można przedstawić jako skończoną sumę bezgwiazdkowych przeciwobrazów.

Do udowodnienia, że przeciwobraz każdego elementu z M jest bezgwiazdkowy przeprowadzimy indukcję malejącą ze względu na moc $r(m)$ zbioru MmM, gdzie $m \in M$.

Zauważmy, że $r(m)$ ma maksymalną wartość, gdy $m = 1_M$, jest to dokładnie moc monoidu M. Co więcej, z prawa częściowego skracania otrzymujemy, że jeśli $mn = m1_Mn = 1_M$, to $m = n = 1_M$, więc r osiąga maksymalną wartość jedynie w 1_M.

Rozważmy przypadek, gdy $m = 1_M$. Wówczas

$$\varphi^{-1}(1_M) = N \setminus N \cdot W \cdot N,$$

gdzie W jest zbiorem śladów liter $a \in A$ takich, że $\varphi([a]) \neq 1_M$. Wystarczy sprawdzić tylko litery, bo z prawa częściowego skracania dla $\varphi(\alpha\beta) = 1$ mamy $\varphi(\alpha) = \varphi(\beta) = 1_M$. Tak więc dla przeciwobrazu 1_M znaleźliśmy wyrażenie bezgwiazdkowe.

Niech $m \in M \setminus \{1_M\}$. Załóżmy, że dla elementów $n \in M$, dla których $r(n) > r(m)$ przeciwobrazy $\varphi^{-1}(n)$ są bezgwiazdkowe. Z równości (6.1) otrzymujemy

$$\varphi^{-1}(m) = U \cdot N \cap N \cdot V \setminus N \cdot W \cdot N,$$

gdzie U, V i W jak w lemacie 6.5. Pokażemy, że zbiory te są bezgwiazdkowe, wykorzystując założenie indukcyjne.

Niech $n \in M$ oraz $a \in A$ będą takie, że $n\varphi([a])M = mM$ oraz $n \notin mM$. Wówczas $MnM \supseteq MmM$, więc $r(n) \geq r(m)$. Przypuśćmy, że $r(n) = r(m)$. Wówczas $n \in MmM$, bo M jest skończony. Stąd $n = umv$ dla $u, v \in M$. Ponieważ $m \in n\varphi([a])M$, otrzymujemy, że $m = np$ dla pewnego $p \in M$. Stąd $n = unpv$ i korzystając z prawa częściowego skracania dostajemy $n = npv = mv$, co przeczy założeniu, że $n \notin mM$. Stąd $r(n) > r(m)$ i korzystając z założenia indukcyjnego otrzymujemy, że $\varphi^{-1}(n)$ jest bezgwiazdkowy, a więc również U jest bezgwiazdkowy jako skończona suma zbiorów postaci $\varphi^{-1}(n)[a]$.

Analogicznie dowodzimy, że V jest bezgwiazdkowy.

Do zakończenia dowodu pozostało pokazać, że W jest bezgwiazdkowy. Rozważmy $n \in M$ oraz $a, b \in A$ takie, że $m \in M\varphi([a])nM \cap Mn\varphi([b])M$ oraz $m \notin M\varphi([a])n\varphi([b])M$. Znów $r(n) \geq r(m)$. Przypuśćmy, że $r(n) = r(m)$. Wówczas $n = umv$ oraz $m = r\varphi([a])ns = pn\varphi([b])t$ dla $p, r, u, v, s, t \in M$. Dalej, $n = ur\varphi([a])nsv$ daje $n = ur\varphi([a])n$ i $m = pur\varphi([a])n\varphi([b])t$, co przeczy założeniu. Stąd $r(n) > r(m)$ i wykorzystując założenie indukcyjne otrzymujemy, że W jest bezgwiazdkowy jako skończona suma zbiorów bezgwiazdkowych, co kończy dowód stwierdzenia 6.2. □

6.1.2 Lemat o domknięciu złożenia

Lemat przedstawiony w tym podrozdziale, będzie często wykorzystywany w dalszej części rozprawy. Jego dowód w istotny sposób wykorzystuje charakteryzację języków bezgwiazdkowych za pomocą bezgwiazdkowej gwiazdki (twierdzenie 5.19).

Poniższy przykład pokazuje, że dla języków bezgwiazdkowych lemat Hashiguchi'ego o stopniach rozproszenia nie zachodzi.

Przykład 6.6. Niech $A = \{a, b, c\}$ i relacja zależności określona następująco:

$$(A, D) : \ a — c — b.$$

Weźmy język bezgwiazdkowy $L = (abcbac)^*$. Ponieważ L jest opisany wyrażeniem iteracyjnie spójnym, to ze stwierdzenia 4.15 wynika, że L ma skończony stopień rozproszenia. Jednak domknięcie $\overline{L} = ((ab \cup ba)c(ab \cup ba)c)^*$ nie jest językiem bezgwiazdkowym.

Ponieważ w dla bezgwiazdkowych języków słów nie ma odpowiednika lematu Hashiguchi'ego, poniższy lemat dowodzimy w sposób bardziej złożony niż dla języków rozpoznawalnych.

Lemat 6.7. *Jeśli $K, L \subseteq A^*$ są domkniętymi językami bezgwiazdkowymi, to $\overline{KL}$ jest językiem bezgwiazdkowym.*

Dowód. Niech $A' = \{a' \mid a \in A\}$ i $A'' = \{a'' \mid a \in A\}$ będą różnie pokolorowanymi (więc rozłącznymi) kopiami alfabetu A, oznaczmy $C = A' + A''$.

Określmy relację niezależności $I_C \subseteq C \times C$ jako najmniejszą relację niezależności w C taką, że jeśli aIb, to $a'I_Cb''$. Z domkniętości języków K i L wynika, że

$$\overline{KL} = h(\overline{K'L''}),$$

gdzie K' i L'' są różnie pokolorowanymi kopiami języków K i L, morfizm $h : C \to A$ jest morfizmem zmywającym kolory, tzn. $h(a') = h(a'') = a$, lewe domknięcie jest względem I, a prawe względem I_C.

Zdefiniujmy podstawienia $f', f'' : A \to 2^{C^*}$, $f'(a) = A''^* a' A''^*$ i $f''(a) = A'^* a'' A'^*$ kolorujące litery alfabetu A i otaczające je słowami przeciwnego koloru.

Do dokończenia dowodu musimy udowodnić dwa postulaty.

Postulat 6.8. *Jeśli $X \subseteq A^*$ jest bezgwiazdkowy, to $f'(X), f''(X) \subseteq C^*$ są językami bezgwiazdkowymi.*

Dowód. Zbudujemy automat dla $f'(X)$, przerabiając minimalny, deterministyczny automat dla X, który nie ma pętli nietrywialnych (bo X jest SF). Kolorując etykiety łuków ($\xrightarrow{a}$ na $\xrightarrow{a'}$) dostajemy automat dla X' (nadal bez pętli nietrywialnych). Dołączając do każdego stanu pętelki etykietowane wszystkimi literami a'' dla $a \in A$, otrzymujemy automat dla $f'(X)$. Nie ma on pętli nietrywialnych (bo nie miał ich automat dla X'), więc $f'(X)$ jest bezgwiazdkowy. Analogicznie (zamieniając primowanie z bisowaniem) pokazujemy, że $f''(X)$ jest bezgwiazdkowy. *Koniec dowodu postulatu 6.8* □

Teraz zauważmy, że zawsze $a'D_Cb''$, gdy aDb, więc

$$\overline{K'L''} = f'(K) \cap f''(L) \setminus \bigcup_{aDb} C^*b''C^*a'C^*.$$

Wobec postulatu 6.8 język $\overline{K'L''}$ jest SF, bo klasa SF jest zamknięta względem operacji boolowskich.

Pokazaliśmy, że $\overline{K'L''}$ jest bezgwiazdkowy. Teraz pokażemy, że po zmyciu kolorów pozostanie bezgwiazdkowy.

Postulat 6.9. *Jeśli $X \subseteq C^* \setminus \bigcup_{aDb} C^*b''C^*a'C^*$ jest bezgwiazdkowy, to $h(X)$ też jest bezgwiazdkowy.*

Dowód. Indukcja strukturalna na SFS-wyrażeniach.

Dla atomów stwierdzenie jet oczywiste.

Założenie indukcyjne: Jeśli $Y, Z \subseteq C^* \setminus \bigcup_{aDb} C^*b''C^*a'C^*$ są bezgwiazdkowe i $h(Y), h(Z)$ są bezgwiazdkowe.

Krok indukcyjny:

Jeśli $X = Y \cup Z$, to z założenia indukcyjnego $Y, Z \subseteq C^* \setminus \bigcup_{aDb} C^*b''C^*a'C^*$ oraz bezgwiazdkowe, więc $h(X) = h(Y) \cup h(Z)$ jest bezgwiazdkowy.

Jeśli $X = YZ$, to z założenia indukcyjnego $Y, Z \subseteq C^* \setminus \bigcup_{aDb} C^*b''C^*a'C^*$ oraz bezgwiazdkowe, więc $h(X) = h(Y)h(Z)$ jest bezgwiazdkowy.

Aby pokazać, że $h(Y^*)$ jest bezgwiazdkowy zauważmy, że co najwyżej jedna litera z liter a', a'' może wystąpić w $Alph(Y)$, bo aDa, więc a'' nie może wystąpić przed a' w Y^*. Zatem $h(Y^*)$ jest izomorficzną kopią Y^*, więc jest bezgwiazdkowy. *Koniec dowodu postulatu 6.9* □

Teraz zauważając, że język $\overline{K'L''}$ spełnia założenia postulatu 6.9, wnioskujemy, że $h(\overline{K'L''})$ jest bezgwiazdkowy. Co, wobec równości $\overline{KL} = h(\overline{K'L''})$, kończy dowód lematu 6.7. □

6.1.3 Bezgwiazdkowy $\Longleftrightarrow$ aperiodyczny

Twierdzenie 6.10. *Niech A^*/I będzie monoidem śladów i niech $T \subseteq A^*/I$ językiem śladów. Następujące zdanie są równoważne:*

1. *T jest bezgwiazdkowy w A^*/I.*
2. *$\bigcup T$ jest bezgwiazdkowy w A^*.*
3. *$\bigcup T$ jest aperiodyczny w A^*.*
4. *T jest aperiodyczny w A^*/I.*

Dowód. Implikację $1 \Rightarrow 2$ dowodzimy indukcją strukturalną na SF-wyrażeniach. Dla języków atomowych implikacja jest oczywista. Przypuśćmy, że dla bezgwiazdkowych języków śladów X i Y, języki słów $\bigcup X$ i $\bigcup Y$ są bezgwiazdkowe. Rozważmy trzy przypadki

a) Jeśli $T = X \cup Y$, to $\bigcup T = \bigcup(X \cup Y) = \bigcup X \cup \bigcup Y$ jest bezgwiazdkowy.

b) Jeśli $T = XY$, to $\bigcup T = \bigcup(XY) = \overline{\bigcup X \bigcup Y}$ jest bezgwiazdkowy z lematu 6.7

c) Jeśli $T = X'$, to $\bigcup T = \bigcup X' = (\bigcup X)'$.

Implikacja $2 \Rightarrow 3$ wynika wprost z twierdzenia Schützenbergera.

Implikacja $3 \Rightarrow 4$ wynika z definicji spłaszczenia i monoidu syntaktycznego. Monoidy syntaktyczne języka śladów i jego spłaszczenia są równe.

Implikacja $4 \Rightarrow 1$ to stwierdzenie 6.2. □

Zauważmy, że równoważność $1 \Leftrightarrow 4$ to dokładnie twierdzenie 6.1 Guaiany, Restivo i Salemi. Przypomnijmy, że odpowiednik równoważności $1 \Leftrightarrow 2$ zachodzi dla języków rozpoznawalnych, a jej dowód jest bardzo prosty. Natomiast dowód dla języków bezgwiazdkowych jest złożony i korzysta z kilku nietrywialnych faktów, kolejno twierdzenia 5.19, lematu 6.7 i stwierdzenia 6.2.

Równoważność $1 \Leftrightarrow 2$ w twierdzeniu 6.10 będzie często wykorzystywana w dalszej części rozprawy, dlatego wyróżniamy ją jako oddzielny wniosek.

Wniosek 6.11. *Niech (A, I) będzie alfabetem współbieżnym i T językiem śladów. Wówczas zachodzi równoważność*

$$T \in SF(A^*/I) \Longleftrightarrow \bigcup T \in SF(A^*).$$

Przykład 6.12. Niech $A = \{a, b\}$ oraz aIb. Niech $T \subseteq A^*/I$ będzie językiem śladów definiowanym wyrażeniem bezgwiazdkowym $[ab]\emptyset'$. Wówczas $\bigcup T = \emptyset' ab \emptyset' \cup \emptyset' ba \emptyset' \subseteq A^*$.

Język T jest również definiowany wyrażeniem $(\emptyset'[a]\emptyset' \cup \emptyset'[b]\emptyset')'$ i również jego spłaszczenie $\bigcup T = (\emptyset' a \emptyset' \cup \emptyset' b \emptyset')'$.

6.2 Monoidy śladów z przechodnią orientacją

Niech (A, I) będzie alfabetem współbieżnym i $<$ liniowym porządkiem na alfabecie A. Trójkę $(A, <, I)$ nazywamy **uporządkowanym alfabetem współbieżnym**. W monoidzie wolnym definiujemy porządek leksykograficzny. Słowo puste ε jest mniejsze od każdego niepustego słowa $v \in A^+$ – $\varepsilon < v$. Niepuste słowo $u \in A^+$ jest mniejsze w porządku leksykograficznym od słowa $v \in A^+$, jeśli

$$(\exists a, b \in A)(\exists u_1, v_1 \in A^*)\ u = au_1 \wedge v = bv_1 \wedge (a < b \vee a = b \wedge u_1 < v_1).$$

Niech A^*/I będzie monoidem śladów. **Leksykograficzną reprezentacją śladu** $\alpha \in A^*/I$ nazywamy słowo $Lex(\alpha) = \min_<\{w \mid w \in \alpha\} \in A^*$, najmniejsze słowo w porządku leksykograficznym ze śladu α. **Leksykograficzną reprezentacją języka śladów** $T \subseteq A^*/I$ nazywamy zbiór słów $Lex(T) = \{Lex(\alpha) \mid \alpha \in T\}$, czyli zbiór najmniejszych w porządku leksykograficznym reprezentantów śladów z języka T. Zbiór $Lex(A^*/I)$ będziemy oznaczać przez LEX. Dla wygody, jeśli słowo $w \in LEX$, to będziemy mówić, że w jest leksykograficzne, podobnie, jeśli $L \subseteq LEX$, to będziemy mówić, że L jest językiem leksykograficznym.

Niech $(A, <, I)$ będzie uporządkowanym alfabetem współbieżnym, niech $T \subseteq A^*/I$ będzie językiem śladów i $L \subseteq A^*$ językiem słów. Następujące równości wynikają wprost z powyższych definicji i definicji operacji domknięcia.

$$Lex(T) = \bigcup T \cap LEX \tag{6.2}$$

$$\overline{Lex(T)} = \bigcup T. \tag{6.3}$$

$$\overline{\overline{L} \cap LEX} = \overline{L}. \tag{6.4}$$

Poniższe twierdzenie z [24] pokazuje znaczenie leksykograficznej reprezentacji w badaniu rozpoznawalności języków śladów.

Twierdzenie 6.13 (Ochmański). *Niech $(A, <, I)$ będzie alfabetem współbieżnym i $M = A^*/I$ monoidem śladów. Język śladów $T \subseteq M$ jest rozpoznawalny wtedy i tylko wtedy, gdy jego leksykograficzna reprezentacja $Lex(T) \subseteq A^*$ jest językiem regularnym,*

$$T \in Rec(M) \iff Lex(T) \in Reg(A^*),$$

równoważnie – domknięcie języka słów $\overline{L} \subseteq A^*$ jest językiem regularnym wtedy i tylko wtedy, gdy $\overline{L} \cap LEX$ jest regularny,

$$\overline{L} \in Reg(A^*) \iff \overline{L} \cap LEX \in Reg(A^*).$$

Powstaje pytanie, jakie kryterium ma spełniać język bezgwiazdkowy, żeby indukował bezgwiazdkowy język śladów. Problem, czy język śladów indukowany przez bezgwiazdkowy język słów jest bezgwiazdkowy, zbadali Muscholl i Petersen w [23]. W połączeniu z wnioskiem 6.11 ich wynik można sformułować następująco.

Twierdzenie 6.14 (Muscholl, Petersen). *Niech (A, I) będzie alfabetem współbieżnym z przechodnią relacją zależności $D = A \times A \setminus I$ oraz niech $L \subseteq A^*$ będzie bezgwiazdkowym językiem słów. Wówczas język śladów $[L]$ jest bezgwiazdkowy lub nie jest rozpoznawalny.*

Musholl i Petersen pokazali, że założenie przechodniości jest konieczne.

Przykład 6.15. Niech $A = \{a, b, c\}$ oraz

$$(A, D): \ a — c — b.$$

Jest to najprostszy przykład alfabetu współbieżnego z nieprzechodnią relacją zależności. Weźmy język $L = (abcbac)^*$. Język ten jest bezgwiazdkowy (bo m.d.a. dla L nie ma cykli nietrywialnych), ale jego domknięcie $\overline{L} = ((ab \cup ba)c(ab \cup ba)c)^*$ jest językiem regularnym i nie jest bezgwiazdkowym (przecięcie z bezgwiazdkowym językiem $(abc)^*$ nie daje nam języka bezgwiazdkowego – $\overline{L} \cap (abc)^* = (abcabc)^* \notin SF(A^*)$).

6.2.1 Leksykograficzne języki bezgwiazdkowe

Ustalmy uporządkowany alfabet współbieżny $(A, <, I)$. Najpierw zauważmy, że język LEX słów leksykograficznie pierwszych jest bezgwiazdkowy, ponieważ

$$A^* \setminus LEX = \bigcup_{\substack{aIb \\ a<b}} A^* b I_a^* a A^*, \text{ gdzie } I_a = \{c \in A \mid aIc\}.$$

Przez analogię do twierdzenia 6.13, powstają pytania:

Czy język śladów $T \in A^*$ jest bezgwiazdkowy wtedy i tylko wtedy, gdy leksykograficzna reprezentacja $Lex(T)$ jest bezgwiazdkowa?

$$T \in SF(A^*/I) \Leftarrow ? \Rightarrow Lex(T) \in SF(A^*).$$

Czy domknięcie języka słów $\overline{L}$ jest bezgwiazdkowe wtedy i tylko wtedy, gdy część wspólna jego domknięcia z LEX jest bezgwiazdkowa?

$$\overline{L} \in SF(A^*) \Leftarrow ? \Rightarrow \overline{L} \cap LEX \in SF(A^*).$$

Mając wniosek 6.11 wiemy, że powyższe pytania są równoważne. Ponadto twierdzenie 6.14 z wykorzystaniem twierdzenia 6.13 daje pozytywną odpowiedź w przypadku przechodniej relacji zależności. Jednak przykład 6.15 nie jest kontrprzykładem, gdyż język L z tego przykładu nie jest zawarty w LEX.

Zauważmy dodatkowo, że implikacje $\Longrightarrow$ są prawdziwe dla dowolnego alfabetu współbieżnego. Sformułujmy pytanie o odwrotną implikację w wygodniejszej postaci.

Czy jeśli $L \subseteq A^*$ jest bezgwiazdkowy i zawarty w LEX, to domknięcie $\overline{L}$ jest również językiem bezgwiazdkowym?

$$L \in SF \wedge L \subseteq LEX =? \Rightarrow \overline{L} \in SF$$

W tym podrozdziale odpowiemy na to pytanie przy pewnym dodatkowym założeniu o strukturze porządku na alfabecie współbieżnym.

Definicja 6.16. Zorientowany alfabet współbieżny $(A, <, I)$ jest **przechodnio-zorientowany**, gdy relacja $< \cap I$, czyli mniejszy i niezależny, jest przechodnia.

Od tego momentu zakładamy, że rozważane w tym podrozdziale alfabety współbieżne mają przechodnią orientację.

Stwierdzenie 6.17. *Jeśli zorientowany alfabet współbieżny $(A, <, I)$ jest przechodnio-zorientowany, to*

$$LEX = \{w \in A^* \mid (\forall a, b \in A)(\forall u, v \in A^*)\ w = uabv \Longrightarrow aDb \vee a < b\}.$$

Dowód. Zawieranie $\subseteq$ jest oczywiste.

Pokażemy zawieranie $\supseteq$. Przypuśćmy, że $w \notin LEX$. Wówczas istnieją $a, b \in A$ oraz słowa $u, v, x \in A^*$ takie, że $w = ubxav$, $a < b$ oraz $aIbx$. Niech bx będzie najkrótszym segmentem słowa w dla ustalonego a i u. Jeśli x jest słowem pustym, to w nie należy do prawej strony równości. Załóżmy, że $x \neq \varepsilon$. Przypuśćmy, że $x = cy$, gdzie $c \in A$ i $y \in A^*$. Wówczas cIa, $c < a$ (bo bx jest najkrótsze dla a) oraz aIb, a<b. Z przechodniej orientacji alfabetu wynika, że cIb oraz $c < b$. Stąd w nie należy do prawej strony równości. $\square$

Powyższe stwierdzenie nie jest prawdziwe, gdy alfabet nie ma przechodniej orientacji. Dokładniej, warunek $w = uabv \in LEX \Longrightarrow aDb \vee a < b$ jest konieczny, ale nie wystarczający w ogólnym przypadku.

Przykład 6.18. Niech $A = \{a, b, c\}$, $a < b < c$ oraz

$$(A, D) \colon a \quad b \quad c$$

Ponieważ $\neg aIc$, zorientowany alfabet $(A, <, I)$ nie ma przechodniej orientacji. Rozważmy słowo cab. Zauważmy, że każda sąsiednia para spełnia warunek opisany w stwierdzeniu, ale to słowo nie jest leksykograficznie pierwsze. Leksykograficznie pierwszym słowem równoważnym z cab jest bca.

Wprowadźmy pomocnicze pojęcia leksykograficznego produktu, leksykograficznego dopełnienia i języków LSF. Pojęcia te będą pomocne przy dowodzie, że pytanie, czy domknięcie leksykograficznego bezgwiazdkowego języka słów jest bezgwiazdkowe, ma pozytywną odpowiedź w monoidów śladów z przechodnią relacją niezależności.

Definicja 6.19. Niech $K, L \subseteq LEX$ będą leksykograficznymi językami słów. **Leksykograficznym produktem** nazywamy operację $\circ$ określoną następująco:

$$K \circ L = \begin{cases} KL, & \text{gdy } KL \subseteq LEX \\ \text{nieokreślone}, & \text{w przeciwnym wypadku.} \end{cases}.$$

Dopełnieniem leksykograficznym języka K, oznaczanym K'', nazywamy dopełnienie do podzbioru LEX,

$$K'' = LEX \setminus K.$$

Definicja 6.20. Języki zbudowane ze zbioru pustego, słowa pustego i liter z alfabetu przy użyciu operacji sumy zbiorów $\cup$, produktu leksykograficznego $\circ$ oraz dopełnienia leksykograficznego $''$ nazywamy LSF**-językami**. Klasę LSF-języków oznaczamy przez LSF.

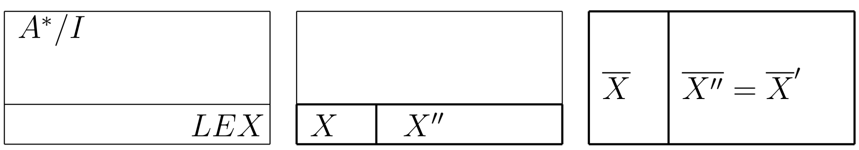
Wyrażenie zbudowane z atomów przy użyciu symboli tych operacji nazywamy LSF**-wyrażeniami**. Oczywiście język słów L jest LSF wtedy i tylko wtedy, gdy istnieje LSF-wyrażenie definiujące L.

Lemat 6.21. *Jeśli język słów $L \subseteq A^*$ jest LSF, to jego domknięcie $\overline{L}$ jest bezgwiazdkowe.*

Dowód. Indukcja strukturalna ze względu na wyrażenia LSF.
Baza indukcji. Dla atomów lemat jest oczywisty.
Założenie indukcyjne. Niech $X, Y \in LSF$ oraz $\overline{X}, \overline{Y}$ są bezgwiazdkowe
Krok indukcyjny. Przypuśćmy, że $L = X \cup Y$. Wówczas $\overline{L} = \overline{X \cup Y} = \overline{X} \cup \overline{Y}$, czyli z założenia indukcyjnego domknięcie $\overline{L}$ jest bezgwiazdkowe.

Przypuśćmy, że $L = X \circ Y$. Wówczas $\overline{L} = \overline{XY} = \overline{\overline{X} \cdot \overline{Y}}$. Z lematu 6.7, domknięcie złożenia domkniętych języków bezgwiazdkowych jest bezgwiazdkowe.

Jeśli $L = X''$, to $\overline{X''} = \overline{X}'$, gdy X jest zawarte w LEX.



□

Wprost z definicji i bezgwiazdkowości LEX wynika, że każdy LSF-język jest bezgwiazdkowy i zawarty w LEX. W następnym podrozdziale pokażemy, że w alfabetach z przechodnią orientacją zachodzi też twierdzenie odwrotne, tzn. każdy język bezgwiazdkowy zawarty w LEX jest LSF-językiem.

6.2.2 Automaty dla LEX-ów

Podstawowym narzędziem w tym podrozdziale będą automaty. Z ich pomocą pokażemy twierdzenie o leksykograficznej charakteryzacji bezgwiazdkowych języków śladów w monoidach nad przechodnio-zorientowanymi alfabetami.

Poniższa własność wynika wprost z definicji słów leksykograficznych.

Własność 6.22. *Niech $(A, <, I)$ będzie dowolnym zorientowanym alfabetem współbieżnym. Wówczas dowolny segment słowa leksykograficznego jest również słowem leksykograficznym.*

$$(\forall w \in LEX)(\forall u, v, z \in A^*)\ w = uvz \Longrightarrow v \in LEX.$$

Własność 6.22 oraz stwierdzenie 6.17 umożliwiają w przypadku przechodnio-zorientowanego alfabetu współbieżnego, następującą konstrukcję minimalnego automatu deterministycznego dla LEX.

Konstrukcja:

Na wejściu mamy dany zorientowany alfabet współbieżny $(a_1 < \ldots < a_m; D)$, $D = A \times A \backslash I$ jest relacją zależności. Konstrukcja jest indukcyjna. Dla ułatwienia zapisu, zbiorem stanów będą kolejne liczby naturalne. W konstruowanych automatach wszystkie stany są stanami końcowymi (nie są to automaty zupełne), w związku z tym w ich opisie będziemy pomijać wyróżnianie stanów końcowych.

Na początku budujemy automat $\mathbf{A}_1$ dla LEX gdzie alfabet składa się z pierwszej litery w uporządkowanym alfabecie:

$$\mathbf{A}_1 = \mathbf{A}_{LEX}(a_1; D) = (\{a_1\}, \{1\}, \delta_1, 1),\ \text{gdzie}\ \delta_1(1, a_1) = 1.$$

Mając skonstruowany automat

$$\mathbf{A}_n = \mathbf{A}_{LEX}(a_1 < \ldots < a_n; D) = (\{a_1, \ldots, a_n\}, Q_n, \delta_n, q_1),$$

dla $n < m$, $|Q_n| = \{1, \ldots, k\}$, w kolejnych krokach zbudujemy automat

$$\mathbf{A}_{n+1} = \mathbf{A}_{LEX}(a_1 < \ldots < a_n < a_{n+1}; D) = (\{a_1, \ldots, a_n, a_{n+1}\}, Q_{n+1}, \delta_{n+1}, 1).$$

1. Niech $i \in \{1, \ldots, k\}$ będzie najmniejszym stanem spełniającym warunek

   $$(\forall x \in \{a_1, \ldots, a_n\})\ (i, x) \in dom(\delta_n) \Longrightarrow xDa_{n+1} \tag{6.5}$$

   czyli wszystkie wychodzące łuki ze stanu i są etykietowane literami zależnymi z a_{n+1}. Jeśli taki stan nie istnieje, to dodajemy nowy stan $i = k+1$, $Q_{n+1} = Q_n \cup \{i\}$.

2. Funkcję przejścia δ_{n+1} jest rozszerzeniem funkcji δ_n, $\delta_n(j, a_{n+1}) = i$ dla każdego $j \in Q_{n+1}$ (Do stanu i z każdego stanu prowadzimy łuk etykietowany literą a_{n+1}.)

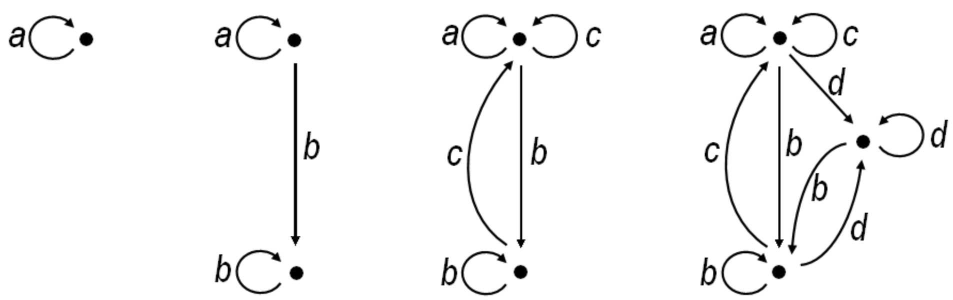
3. Jeśli $i = k+1$, tzn. w punkcie 1 doszedł nowy stan, to dla liter $x \in \{a_1, \dots, a_n\}$ takich, że $x < a_{n+1}$ oraz xDa_{n+1}, określamy funkcję δ_n na parze $(k+1, x)$ w następujący sposób. Znajdujemy najmniejsze j takie, że
$$(\forall y \in \{a_1, \dots, a_n\})\ (j, y) \in dom(\delta_n) \Longrightarrow x < y \vee yDx.$$
Wówczas $\delta_{n+1}(k+1, x) = j$. (Znajdujemy najmniejszy stan j, z którego wszystkie wychodzące łuki są etykietowane literami większymi lub zależnymi z x i dodajemy łuk ze stanu $k+1$ do stanu j etykietowany literą x.)

Poniższy przykład dobrze ilustruje wszystkie kroki konstrukcji.

Przykład 6.23. Dla współbieżnego alfabetu

$$(A, D)\colon a \quad b - c \quad d$$

z porządkiem $a < b < c < d$, w kolejnych krokach otrzymujemy automaty z rysunku 6.1.



Rysunek 6.1: Kolejne kroki konstrukcji automatu dla LEX

Stwierdzenie 6.24. *Niech $(A, <, I)$ będzie przechodnio zorientowanym alfabetem oraz $\mathbf{A}_{LEX} = \langle A, Q, \delta, q_0 \rangle$. Wówczas dla dowolnej litery $a \in A$ istnieje dokładnie jeden stan $q_a \in Q$ taki, że jeśli dla stanu $p \in Q$, $(p, a) \in dom(\delta)$, to $\delta(p, a) = q_a$. (Wszystkie łuki etykietowane literą a, wskazują na dokładnie jeden stan q_a.)*

$$(\forall a \in A)(\exists q_a \in Q)(\forall p \in Q)\ (p, a) \in dom(\delta) \Longrightarrow \delta(p, a) = q_a.$$

Dowód. Bezpośrednio z konstrukcji. □

Niech $\mathbf{A}_{LEX} = \langle A, Q, \delta, q_0 \rangle$ będzie automatem dla LEX i niech, $p, r \in Q$ będą stanami tego automatu (niekoniecznie różnymi). Przez $L(p, r)$ oznaczmy język akceptowany przez automat $\langle A, Q, \delta, p, \{r\} \rangle$, tzn. język ścieżek w automacie $\mathbf{A}_{LEX}$ ze stanu p (stan początkowy) do stanu r (stan końcowy).

Lemat 6.25. *Niech $(A, <, I)$ będzie przechodnio-zorientowanym alfabetem oraz $\mathbf{A}_{LEX} = \langle A, Q, \delta, q_0 \rangle$. Wówczas*

$$(\forall p, r \in Q)\ L(p, r) \in LSF.$$

Dowód. Przez ${}_xLEX$ gdzie $x \in A$ oznaczmy podzbiór słów LEX zaczynających się na literę x, a przez LEX_x podzbiór LEX słów kończących się na x.

Najpierw pokażemy, że dla każdej litery $x \in A$ języki ${}_xLEX$ i LEX_x są LSF językami. Niech $a_1 < \ldots < a_m$ będzie wejściowym porządkiem na alfabecie A. Dowód jest indukcyjny ze względu na pozycje litery w alfabecie.
Baza indukcji. Zauważmy, że ${}_{a_1}LEX = a_1LEX$, podobnie $LEX_{a_m} = LEXa_m$. Oba języki są LSF, gdyż $LEX = \emptyset''$, a te złożenia nie wyprowadzają poza LEX.
Założenie indukcyjne. Przypuśćmy, że dla $n < m$ języki ${}_{a_i}LEX$ i $LEX_{a_{m+1-i}}$ są LSF dla $1 \leq i \leq n$.
Krok indukcyjny. Pokażemy, że ${}_{a_{n+1}}LEX$ i $LEX_{a_{m-n}}$ są LSF. Ze stwierdzenia 6.17 wynika, że dla $x \in A$

$$ {}_xLEX = x(LEX \setminus \bigcup_{\substack{yIx \\ y<x}} {}_yLEX) = x(\bigcup_{\substack{yIx \\ y<x}} {}_yLEX)'' $$

oraz

$$ LEX_x = (LEX \setminus \bigcup_{\substack{zIx \\ z>x}} LEX_z)x = (\bigcup_{\substack{zIx \\ z>x}} LEX_z)''x. $$

Zauważmy, że we wzorze dla ${}_{a_{n+1}}LEX$ i $LEX_{a_{m-n}}$ występują jedynie te zbiory ${}_yLEX$ i LEX_z, które z założenia indukcyjnego są LSF. Stąd również ${}_{a_{n+1}}LEX$ i $LEX_{a_{m-n}}$ są LSF.

Ze stwierdzenia 6.24 wiemy, że istnieje dokładnie jeden stan, na który wskazują krawędzie o tej samej etykiecie. Stąd dla dowolnego stanu $r \in Q$

$$ L(q_0, r) = \bigcup_{\xrightarrow{a} r} LEX_a(\cup\varepsilon, \text{ gdy } r = q_0). $$

Niech $L(r)$ oznacza język akceptowany przez automat $\langle A, Q, \delta, r\rangle$. Zauważmy, że

$$ L(r) = \bigcup_{r \xrightarrow{a}} {}_aLEX(\cup\varepsilon, \text{ gdy } r = q_0), $$

więc dla dowolnego $r \in Q$ język $L(r)$ jest LSF.

Zauważmy teraz, że dla dowolnych $p, r \in Q$ zachodzi

$$ L(p, r) = L(q_0, p) \cap L(r). $$

Operacja iloczynu zbiorów leksykograficznych nie wyprowadza poza klasę LSF, więc $L(p, r) \in LSF$. □

Lemat 6.26. *Niech $(A, <, I)$ będzie zorientowanym alfabetem współbieżnym, $\mathbf{A}_{LEX} = \langle A, Q, \delta, q_0\rangle$ deterministycznym automatem akceptującym LEX takim, że języki $L(p, r)$ są LSF dla dowolnych $p, r \in Q$ oraz Z bezgwiazdkowym językiem słów. Wówczas dla dowolnych $p, r \in Q$, język $Z \cap L(p, r)$ jest LSF.*

Dowód. Indukcja strukturalna.
Baza indukcji. Przypuśćmy, że Z jest językiem atomowym. Wówczas $Z \cap L(p,r) = Z$, gdy $Z \subseteq L(p,r)$ lub $Z \cap L(p,r) = \emptyset$ w przeciwnym wypadku. W obu przypadkach zbiór $Z \cap L(p,r)$ z definicji należy do LSF.
Założenie indukcyjne. Przypuśćmy, że języki X, Y są bezgwiazdkowe i dla dowolnych $p, r \in Q$ języki $(X \cap L(p,r)), (Y \cap L(p,r))$ należą do klasy LSF.
Krok indukcyjny. Niech język Z będzie językiem bezgwiazdkowym zbudowanym z X i Y.

- Jeśli $Z = X \cup Y$, to $Z \cap L(p,r) = (X \cup Y) \cap L(p,r) = (X \cap L(p,r)) \cup (Y \cap L(p,r))$. Z założenia indukcyjnego $Z \in LSF$.
- Jeśli $Z = XY$, to również $X, Y \subseteq LEX$. Wówczas $Z \cap L(p,r) = \bigcup_{q \in Q}(X \cap L(p,q))(Y \cap L(q,r))$. Z założenia indukcyjnego otrzymujemy, że $Z \cap L(p,r) \in LSF$.
- Niech $Z = X'$. Wówczas $X = (X \backslash LEX) \cup (X \cap LEX)$. Stąd $Z \cap L(p,r) = LEX \setminus (X \cap L(p,r))$. Ponieważ z założenia indukcyjnego $(X \cap L(p,r)) \in LSF$, to $Z \cap L(p,r) = (X \cap L(p,r))'' \in LSF$.

□

Lemat 6.27. *Niech $(A, <, I)$ będzie zorientowanym alfabetem współbieżnym oraz $\mathbf{A} = \langle A, Q, \delta, q_0 \rangle$ automatem akceptującym LEX. Jeśli każdy język $L(p,r)$ jest LSF oraz język $Z \subseteq A^*$ jest bezgwiazdkowy i zawarty w LEX, to Z jest LSF-językiem.*

Dowód. Zauważmy, że $LEX = \bigcup_{p,r \in Q} L(p,r)$ oraz $Z = Z \cap LEX = Z \cap \bigcup_{p,r \in Q} L(p,r) = \bigcup_{p,r \in Q} Z \cap L(p,r)$. Z powyższego lematu otrzymujemy, że Z jest LSF. □

Z lematów 6.25 i 6.27 wynika

Wniosek 6.28. *W alfabetach przechodnio-zorientowanych każdy język bezgwiazdkowy i zawarty w LEX jest LSF-językiem.*

Teraz uwzględniając lemat 6.21, uzyskujemy

Twierdzenie 6.29. *Niech $(A, <, I)$ będzie przechodnio-zorientowanym alfabetem współbieżnym. Jeśli język L jest bezgwiazdkowy i $L \subseteq LEX$, to jego domknięcie $\overline{L}$ jest językiem bezgwiazdkowym.*

Twierdzenie 6.29 w połączeniu w wnioskiem 6.11 pozwala stwierdzić, że bezgwiazdkowy odpowiednik twierdzenia 6.13, czyli twierdzenie o leksykograficznej charakteryzacji bezgwiazdkowych języków śladów, zachodzi dla alfabetów przechodnio-zorientowanych. W następnym podrozdziale pokażemy, że implikacja

$$L \in LEX \wedge L \in SF \Longrightarrow \overline{L} \in SF,$$

a zatem twierdzenie o leksykograficznej charakteryzacji, zachodzi dla dowolnego zorientowanego alfabetu współbieżnego $(A, <, I)$. Jednak dowód nie będzie kombinatoryczny i będzie wykorzystywać logiczną charakteryzację języków bezgwiazdkowych w monoidach śladów.

Przykład 6.30. Niech $A = \{a, b, c\}$ będzie alfabetem z zależnością

$$(A, D): \; a \text{ — } b \text{ — } c.$$

Weźmy leksykograficzny język bezgwiazdkowy $L = (cba)^+ \subseteq A^*$. Poniższe wyrażenie bezgwiazdkowe definiuje L

$$c\emptyset' \cap \emptyset' a \setminus \emptyset'(aa \cup bb \cup cc \cup ab \cup ca \cup bc)\emptyset'.$$

Indukowany przez L język śladów $[cba]^+$ jest opisany przez poniższe wyrażenie

$$[c]\emptyset' \cap \emptyset'[a] \setminus ([ca]\emptyset' \cup \emptyset[ac] \cup \emptyset'([aa] \cup [bb] \cup [cc] \cup [ab] \cup [bc])\emptyset').$$

6.3 Logiczna charakteryzacja bezgwiazdkowych języków śladów

W tym rozdziale zostaną pokazane dwie charakteryzacje bezgwiazdkowych języków śladów – logiczna i leksykograficzna. Używane tutaj pojęcie modelu śladu zaproponował Thomas [36], oznaczenia i terminologia pochodzą z [6].

Niech (A, I) będzie alfabetem współbieżnym. Logicznym modelem dla śladu $\alpha \in A^*/I$ jest jego graf śladu $\underline{\alpha} = (V, E, \lambda)$. W tym rozdziale ślady będziemy identyfikować z ich grafami. Formuły w logice pierwszego rzędu dla śladów zbudowane są ze zmiennych $x, y, \ldots$ podstawianych za wierzchołki grafu śladu (elementy zbioru V), formuł atomowych

$$x = y, \;\; (x, y) \in E, \;\; \lambda(x) = a \text{ dla } a \in A$$

przy pomocy $\vee$, $\wedge$, $\neg$, $\rightarrow$ i $\leftrightarrow$ oraz kwantyfikatorów $\exists$ i $\forall$. Jeśli model śladu α graf $\underline{\alpha} = (V, E, \lambda)$ spełnia zdanie ψ, to piszemy $\underline{\alpha} \models \psi$. Językiem śladów definiowanym przez zdanie ψ nazywamy język $L(\psi) = \{\alpha \in A^*/I \mid \underline{\alpha} \models \psi\}$. Klasę języków definiowalnych w logice pierwszego rzędu w monoidzie A^*/I oznaczamy przez $FO(A^*/I)$.

Z definicji grafu śladu, graf jest acykliczny. Zauważmy, że relacja E nie zawsze jest porządkiem. Porządkiem jest przechodnie domknięcie E – relacja E^+. Relację E^+ można wyrazić w logice pierwszego rzędu formułą przy użyciu co najwyżej $|A| - 2$ dodatkowych zmiennych

$$\begin{aligned}(x, y) \in E^+ \quad &\equiv \quad (x, y) \in E \vee \\ \vee \bigvee_{k \leq |A|-2} (\exists z_1 \ldots \exists z_k \quad &(x, z_1) \in E \wedge \bigwedge_{1 < i \leq k} (z_{i-1}, z_i) \in E \wedge (x_k, y) \in E).\end{aligned}$$

W przypadku słów, relacja $E = E^+$ jest liniowym porządkiem na zbiorze V i oznaczamy ją symbolem $\prec$.

Twierdzenie 6.31 (Ebinger, Muscholl 1993). *Niech (A, I) będzie alfabetem współbieżnym i $T \subseteq A^*/I$ językiem śladów. Następujące zdania są równoważne:*

1. $T \in FO(A^*/I)$,

2. $\bigcup T \in FO(A^*)$,

3. $Lex(T) \in FO(A^*)$.

Dowód. Poniższy dowód pochodzi z [9], jest również opisany w [6].

$1 \Rightarrow 2$: Niech $T = L(\psi) \subseteq A^*/I$, gdzie ψ jest zdaniem w logice pierwszego rzędu. Niech $\underline{\alpha} = (V, E, \lambda)$ będzie śladem grafem śladu α i $w \in A^*$ słowem reprezentującym α. Istnieje bijekcja między zbiorem pozycji w słowie w oraz wierzchołkami grafu śladu $\underline{\alpha}$, przy czym w grafie śladu $(x, y) \in E$ wtedy i tylko wtedy, gdy $x \prec y$ oraz $(\lambda(x), \lambda(y)) \in D$ w słowie w. Zamieniając każdą atomową formułę $(x, y) \in E$ koniunkcją pierwszego rzędu

$$x \prec y \wedge (\lambda(x), \lambda(y)) \in D,$$

otrzymujemy zdanie pierwszego rzędu $\widetilde{\psi}$ takie, że $\underline{\alpha} \models \psi$ wtedy i tylko wtedy, gdy $\underline{w} \models \widetilde{\psi}$. Stąd zdanie $\widetilde{\psi}$ definiuje język $\bigcup T$, co dowodzi implikacji $T \in FO(A^*/I) \Longrightarrow \bigcup T \in FO(A^*)$.

$2 \Rightarrow 3$: Ponieważ zbiór LEX jest językiem słów pierwszego rzędu, więc jeśli $\bigcup T \in FO$, to $Lex(T) = \bigcup T \cap LEX$ jest również językiem pierwszego rzędu.

$3 \Rightarrow 1$: Niech $\underline{\alpha} = (V, E, \lambda)$ będzie modelem śladu α oraz $w = x_1 \ldots x_n = Lex(\alpha) \in A^*$ jego leksykograficznym reprezentantem. Każdy wierzchołek $x \in V$ odpowiada pewnemu x_i ze zbioru pozycji słowa w i każda pozycja x_i odpowiada wierzchołkowi x z V. Niech $lex(x, y)$ oznacza, że x_i odpowiadające w w wierzchołkowi x, jest w słowie w przed x_j odpowiadającemu wierzchołkowi y oraz $i < j$. Taka sytuacja zdarza się, gdy $(x, y) \in E^+$, czyli w grafie śladu istnieje ścieżka z wierzchołka x do y lub gdy istnieje minimalny indeks k, taki, że $i < k \leq j$ oraz x_k odpowiada pewnemu wierzchołkowi $z \in V$ takiemu, że $(z, y) \in E^*$, czyli istnieje ścieżka z z do y, przy czym jeśli dodatkowo $(\lambda(x), \lambda(z)) \in I$, to $\lambda(x) < \lambda(z)$. Stąd otrzymujemy następującą formułę na $lex(x, y)$:

$$\begin{aligned} lex(x,y) \quad &\equiv \quad (x,y) \in E^+ \vee \exists z \; (\lambda(x) < \lambda(z) \wedge (\lambda(x), \lambda(z)) \in I \\ &\qquad \wedge \neg lex(z, x) \wedge (z, y) \in E^*). \end{aligned}$$

Ponieważ alfabet jest skończony, wystarczy przeprowadzić rekurencję p razy, gdzie p jest długością najdłuższej ścieżki bez cykli w grafie niezależności (A, I) (w takim, gdzie krawędzie łączą litery niezależne). Powyższa formuła jest więc formułą pierwszego rzędu.

Niech φ będzie zdaniem pierwszego rzędu. W formule φ zastąpmy każdą formułę atomową postaci $x \prec y$ przez powyższą formułę na $lex(x, y)$. Oznaczmy tę nową formułę $\widetilde{\varphi}$, jest ona 1-go rzędu, bo $lex(x, y)$ jest 1-go rzędu. Z konstrukcji tej wynika, że dla $w \in LEX$ zachodzi równoważność:

$$\underline{w} \models \varphi \text{ wtedy i tylko wtedy, gdy } \underline{[w]} \models \widetilde{\varphi},$$

w szczególności dla każdego elementu języka leksykograficznego $L \subseteq LEX$. Stąd, jeśli L jest definiowane zdaniem pierwszego rzędu ψ, to język śladów $[L]$ jest definiowany przez zdanie $\widetilde{\psi}$, więc jest językiem śladów 1-go rzędu.

$\square$

Przykład 6.32. Niech $A = \{a, b\}$ i aIb. Niech $L = a^*b = (\emptyset' b \emptyset')' b$ jest definiowany zdaniem pierwszego rzędu:

$$\psi = \forall x \; \forall y \; (x \prec y \to \lambda(x) = a) \land \exists z \; \lambda(z) = b. \tag{6.6}$$

Zauważmy, że dla grafów śladów z monoidu A^*/I zachodzi $E^+ = E$ i $(x, y) \in E$ *wtw* $\lambda(x) = \lambda(y) \land \neg(y, x) \in E$ oraz

$$lex(x, y) \equiv (\lambda(x) = a \land \lambda(y) = b) \lor (\lambda(x) = \lambda(y) \land (x, y) \in E).$$

Jeśli do zdania (6.6) podstawimy formułę $lex(x, y)$ w miejsce $x \prec y$, to dostaniemy zdanie pierwszego rzędu $\widetilde{\psi}$ definiujące indukowany język śladów $[a^*b]$:

$$\begin{aligned} \widetilde{\psi} \equiv \; & \forall x \; \forall y \; ((\lambda(x) = a \land \lambda(y) = b) \\ & \lor(\lambda(x) = \lambda(y) \land (x, y) \in E) \to \lambda(x) = a) \land \exists z \; \lambda(z) = b. \end{aligned}$$

Przykład 6.33. Niech $A = \{a, b, c\}$ będzie alfabetem z zależnością

$$(A, D): \; a — b — c.$$

Wówczas w grafie śladu $\underline{\alpha} = (V, E, \lambda)$ wierzchołki $x, y \in V$ tworzą krawędź $(x, y) \in E$ wtedy i tylko wtedy, gdy $\lambda(x) D \lambda(y)$, tzn. gdy $\lambda(x) = \lambda(y)$ lub $\lambda(x) = b$ lub $\lambda(y) = b$. Dodatkowo z definicji grafu śladu wynika, że graf $\underline{\alpha}$ jest acykliczny i relacja E^+ jest częściowym porządkiem na V. Wówczas formuła na relację E^+ jest następująca

$$\begin{aligned} (x, y) \in E^+ & \equiv (x, y) \in E \lor \exists z ((x, z) \in E \land (z, y) \in E) \\ & \equiv (x, y) \in E \lor (\lambda(x) = a \land \lambda(y) = c \land \\ & \quad \land \exists z (\lambda(z) = b \land (x, z) \in E \land (z, y) \in E)) \end{aligned}$$

Formuła na relację $lex \subseteq V \times V$ jest następująca

$$lex(x, y) \equiv (x, y) \in E^+ \lor (\lambda(x) = a \land \lambda(y) = c \land \neg(y, x) \in E^+)$$

Weźmy $L = (cba)^+ \subseteq A^*$ z przykładu 6.30. Jest to bezgwiazdkowy i leksykograficzny język słów definiowany poniższym zdaniem φ

$$\begin{aligned} \varphi \equiv \; & \forall x (\neg \exists z \; (z \prec x) \to \lambda(x) = c \land \neg \exists z \; (x \prec z) \to \lambda(x) = a \land \\ & \land \exists y (x \prec y \land \neg \exists z \; (x \prec z \land z \prec y) \to \\ & \to (\neg \lambda(x) = \lambda(y) \land \neg(\lambda(x) = a \land \lambda(y) = b) \land \\ & \land \neg(\lambda(x) = b \land \lambda(y) = c) \land \neg(\lambda(x) = c \land \lambda(y) = a)))) \end{aligned}$$

Zamieniając w formule φ relację $\prec \subseteq V \times V$ na $lex \subseteq V \times V$ otrzymamy zdanie $\widetilde{\varphi}$ definiujące indukowany język śladów $[cba]^*$.

Teraz, łącząc twierdzenie 6.31 z charakteryzacją bezgwiazdkowych języków słów (twierdzenie 5.19) i wcześniej uzyskanymi wynikami (wniosek 6.11), możemy całkiem prosto udowodnić twierdzenie o definiowalności bezgwiazdkowych języków śladów w logice 1-go rzędu.

Twierdzenie 6.34. *Niech (A, I) będzie alfabetem współbieżnym i $T \subseteq A^*/I$ językiem śladów. Wówczas T jest bezgwiazdkowy wtedy i tylko wtedy, gdy jest definiowalny w logice pierwszego rzędu.*

$$SF(A^*/I) = FO(A^*/I).$$

Dowód. Niech $T \subseteq A^*/I$ będzie językiem śladów. Z wniosku 6.11 mamy równoważność

$$T \in SF(A^*/I) \Longleftrightarrow \bigcup T \in SF(A^*).$$

Dalej, z twierdzenia 5.23

$$\bigcup T \in SF(A) \Longleftrightarrow \bigcup T \in FO(A^*).$$

Korzystając z twierdzenia 6.31 dostajemy

$$\bigcup T \in FO(A^*) \Longleftrightarrow T \in FO(A^*/I).$$

□

Powyższe twierdzenie zostało sformułowane w [10], prawie bez dowodu. Obszerny, lecz nadal niepełny szkic dowodu został przedstawiony w [6]. Prostota tutaj zademonstrowanego dowodu uzyskana została dzięki zastosowaniu, wcześniej nieznanej, charakteryzacji bezgwiazdkowych języków śladów za pomocą bezgwiazdkowej gwiazdki (twierdzenie 5.19).

Twierdzenie 6.35. *Niech $(A, I, <)$ będzie uporządkowanym alfabetem współbieżnym i $L \subseteq A^*$ językiem słów. Wówczas zachodzą równoważności:*

$$L \subseteq LEX \wedge L \in SF(A^*) \Longleftrightarrow \overline{L} \in SF(A^*), \tag{6.7}$$

$$L \subseteq LEX \wedge L \in SF(A^*) \Longleftrightarrow [L] \in SF(A^*/I) \tag{6.8}$$

Dowód. Równoważność (6.7) wynika wprost z twierdzenia 6.31 oraz twierdzenia 5.23. Równoważność (6.8) wynika z pierwszej i wniosku 6.11. □

Zauważmy, że w poprzednim podrozdziale powyższe twierdzenie zostało udowodnione dla alfabetów współbieżnych z przechodnią orientacją. Dowód był kombinatoryczny i nie wykorzystywał narzędzi logicznych. Znalezienie podobnego dowodu, bez użycia aparatu logiki, wydaje się interesującym wyzwaniem.

6.4 Bezgwiazdkowa gwiazdka w monoidach śladów

W rozdziale 5 została zdefiniowana operacja bezgwiazdkowej gwiazdki, zbiory SFS oraz zostało pokazane, że w monoidach wolnych klasy języków SF i SFS są sobie równe. W dowolnym monoidzie zachodzi zawieranie $SFS \subseteq SF$, jednak poniższy przykład pokazuje, że nie w każdym monoidzie zachodzi zawieranie w drugą stronę.

Przykład 6.36. Niech $M = (\mathbb{Z}, +)$ będzie monoidem liczb całkowitych z operacją dodawania. Pokażemy, że w tym monoidzie zawieranie $SFS \subseteq SF$ jest właściwe.

Najpierw stosując indukcję strukturalną na wyrażeniach bezgwiazdkowych pokażemy, że zbiór $X \subseteq \mathbb{Z}$ jest bezgwiazdkowy wtedy i tylko wtedy, gdy X lub jego dopełnienie X' jest zbiorem skończonym.
Baza indukcji. Każdy zbiór wyznaczony przez wyrażenie atomowe (zbiór pusty, i singleton liczby) jest skończony.
Założenie indukcyjne. Przypuśćmy, że zbiory U i V są bezgwiazdkowe oraz oba są skończone lub jeden ze zbiorów jest skończony i drugi ma skończone dopełnienie lub obydwa mają skończone dopełnienia.

- Jeśli $X = U \cup V$, to łatwo zauważyć, że jeden ze zbiorów X lub X' jest skończony.
- Jeśli U i V są skończone, to zbiór $X = U+V$ jest również skończony. Jeśli oba zbiory mają skończone dopełnienia, to $X = U+V$ jest równe całemu zbiorowi $\mathbb{Z}$. Jeśli jeden ze zbiorów jest skończony, a moc dopełnienia drugiego jest skończona i wynosi $n \geq 0$, to wynik dodawania zbiorów jest zbiorem pustym lub moc jego dopełnienia jest nie większa niż n.
- Jeśli $X = U'$ równoważność jest oczywista.

Rozważmy teraz wyrażenia SFS. Zauważmy, że zbiór X^*, gdzie X jest skończony, jest zbiorem bezgwiazdkowym wtedy i tylko wtedy, gdy X^* jest zbiorem skończonym i wówczas $X = \emptyset$ lub $X = \{0\}$ lub $X^* = \mathbb{Z}$ (X zawiera zbiór liczb względnie pierwszych, przy czym co najmniej jedna para liczb jest różnych znaków). Stąd klasa zbiorów SFS jest najmniejszą klasą zbiorów zbudowanych z 1, -1, $\emptyset$ oraz $\mathbb{Z}$ przy użyciu operacji $+$ i $\cup$. Stąd w monoidzie liczb całkowitych z dodawaniem zbiory SFS są skończone lub równe $\mathbb{Z}$. Zbiór $\mathbb{Z} \setminus \{0\}$ jest zbiorem bezgwiazdkowym, ale nie należy do klasy SFS.

Jednak monoid liczb całkowitych nie jest monoidem śladów. Nasuwa się pytanie, czy w monoidach śladów zachodzi równość klas SF i SFS?

Niech $(A, I, <)$ będzie uporządkowanym alfabetem współbieżnym. Przypomnijmy, że dla języków słów zachodzi następująca własność

$$L \in SF(A^*) \wedge L \subseteq LEX \Longrightarrow \overline{L} \in SF(A^*). \tag{6.9}$$

oraz równoważność dla języka śladów $T \subseteq A^*/I$

$$T \in SF(A^*/I) \Longleftrightarrow \bigcup T \in SF(A^*). \tag{6.10}$$

Lemat 6.37. *Niech $(A, I, <)$ będzie uporządkowanym alfabetem współbieżnym. Wówczas dla dowolnego języka słów $L \subseteq A^*$ zachodzi implikacja*

$$L \in SFS(A^*) \wedge L \subseteq LEX \Longrightarrow [L] \in SFS(A^*/I).$$

Dowód. Indukcja strukturalna po SFS-wrażeniach.

Dla wyrażeń atomowych – oczywiste.

Założenie indukcyjne. Implikacja zachodzi dla $X, Y \subseteq A^*$

Krok indukcyjny. Niech $L \in SFS(A^*)$ i $L \subseteq LEX$.

1. Niech $L = X \cup Y$. Z założenia indukcyjnego języki śladów $[X], [Y] \in SFS(A^*/I)$. Stąd $[L] = [X] \cup [Y] \in SFS(A^*/I)$.

2. Niech $L = XY$. Z założenia indukcyjnego, $[X], [Y] \in SFS(A^*/I)$. Stąd $[L] = [X][Y] \in SFS(A^*/I)$.

3. Niech $L = X^*$, gdzie $X \in SFS(A^*)$, $X^* \in SF(A) = SFS(A^*)$ i $X^* \subseteq LEX$. Z implikacji (6.9) mamy, że $\overline{X^*} \in SF(A)$, więc $Lex([X]^*) = \overline{X^*} \cap LEX \in SF(A)$. Z równoważności 6.10 mamy $[Z] = [X]^* \in SF(A^*/I)$ oraz z założenia indukcyjnego $[X] \in SFS(A^*/I)$. Stąd $[Z] = [X]^* \in SFS(A^*/I)$.

□

Lemat 6.38. *Niech $(A, I, <)$ będzie uporządkowanym alfabetem współbieżnym. Niech $T \subseteq A^*/I$ będzie językiem śladów. Wówczas zachodzi implikacja*

$$\bigcup T \in SFS(A^*) \Longrightarrow T \in SFS(A^*/I).$$

Dowód. Niech $T \subseteq (A^*/I)$ będzie językiem śladów takim, że $\bigcup T \in SFS(A^*) = SF(A^*)$. Stąd $Lex(T) = \bigcup T \cap LEX \in SF(A^*)$. Z twierdzenia 5.19 mamy $Lex(T) \in SFS(A^*)$. Z lematu 6.37 otrzymujemy, że $T = [Lex(T)] \in SFS(A^*/I)$. □

Twierdzenie 6.39. *Niech $(A, I, <)$ będzie uporządkowanym alfabetem współbieżnym. Wówczas dla dowolnego języka śladów $T \in A^*/I$ zachodzą następujące implikacje*

$$\begin{array}{ccc} T \in SF(A^*/I) & \Longrightarrow & \bigcup T \in SF(A^*) \\ \Uparrow & & \Downarrow \\ T \in SFS(A^*/I) & \Longleftarrow & \bigcup T \in SFS(A^*) \end{array}$$

Zatem powyższe cztery warunki są równoważne.

Dowód. Implikacja $\Longrightarrow$ wynika z równoważności (6.10). Implikacja $\Downarrow$ wynika z twierdzenia 5.19. Implikacja $\Longleftarrow$ wynika z lematu 6.38. Implikacja $\Uparrow$ wynika wprost z definicji języków SFS. □

6.5 Problemy decyzyjne dla języków bezgwiazdkowych

Dla języków bezgwiazdkowych nasuwają się następujące pytania

Pytanie 1. Czy problem bezgwiazdkowości języka racjonalnego jest rozstrzygalny?

W monoidach wolnych odpowiedź na powyższe pytanie jest pozytywna – wystarczy zbadać, czy minimalny deterministyczny automat jest aperiodyczny. W monoidów śladów problem ten jest nierozstrzygalny. W [23] udowodnione zostało następujące twierdzenie

Twierdzenie 6.40. *Niech (A, I) będzie monoidem śladów. Problem „Czy racjonalny język śladów jest bezgwiazdkowy?” jest rozstrzygalny wtedy i tylko wtedy, gdy relacja I jest przechodnia.*

Wiemy, że problem bezgwiazdkowości języka rozpoznawalnego jest, wobec twierdzenia 3.5 i wniosku 6.11, rozstrzygalny.

Kolejne pytanie jest problemem otwartym, podobnym do problemu gwiazdki.

Pytanie 2. Czy w dowolnym monoidzie śladów problem „Czy dla danego bezgwiazdkowego języka śladów T, język T^* jest bezgwiazdkowy” jest rozstrzygalny?

Rozdział 7

Podsumowanie

Podsumowując najważniejsze wyniki pracy, możemy wszechstronnie scharakteryzować klasę podzbiorów bezgwiazdkowych w dowolnych monoidach śladów:

T jest bezgwiazdkowy
wtw
$\bigcup T$ jest bezgwiazdkowy
wtw
$Lex(T)$ jest bezgwiazdkowy
wtw
T jest aperiodyczny
wtw
T jest definiowalny w logice 1-go rzędu
wtw
T można zbudować z atomów za pomocą operacji
sumy, złożenia i bezgwiazdkowej gwiazdki

Dokładniej wyniki rozprawy zostały omówione w rozdziale wstępnym. Tutaj chciałabym zasygnalizować możliwe kierunki badań, zainspirowane uzyskanymi wynikami oraz sformułować kilka problemów z nimi związanych.

Jak wiemy, że różnica języków iteracyjnie spójnych nie zawsze jest iteracyjnie spójna (przykład 4.19).

Problem 1. Czy klasa iteracyjnie spójnych języków słów jest zamknięta względem iloczynu zbiorów?

Ostatnio Klunder [18] pokazała egzystencjalną charakteryzację języków iteracyjnie spójnych za pomocą automatów. Ciągle jednak nie wiemy, jak sprawdzać, czy taki automat istnieje.

Problem 2. Czy iteracyjna spójność języków regularnych jest rozstrzygalna?

Wiemy, że istnieją monoidy, w których bezgwiazdkowa gwiazdka jest słabsza od dopełnienia (przykład 6.36).

Problem 3. Zbadać dokładniej klasę monoidów, w których bezgwiazdkowa gwiazdka (wraz z sumą i złożeniem) potrafi zbudować dowolny podzbiór bezgwiazdkowy.

Przypomnijmy równoważne warunki, charakteryzujące bezgwiazdkowe języki śladów (lewa kolumna) i zauważmy, że analogiczne warunki charakteryzują rozpoznawalne języki śladów (prawa kolumna).

(1bg) T jest bezgwiazdkowy	(1rp) T jest rozpoznawalny
(2bg) $\bigcup T$ jest bezgwiazdkowy	(2rp) $\bigcup T$ jest rozpoznawalny
(3bg) $Lex(T)$ jest bezgwiazdkowy	(3rp) $Lex(T)$ jest rozpoznawalny

Implikacje (1rp)⇒(2rp)⇒(3rp) są prawie oczywiste, a implikacja (3rp)⇒(1rp) jest trudna, ale można ją pokazać kombinatorycznie, bez użycia technik logiki (Ochmański [24, 25]). W przypadku bezgwiazdkowym jedynie implikacja (2bg)⇒(3bg) jest prosta, już (1bg)⇒(2bg) jest trudna kombinatorycznie, natomiast implikacja (3bg)⇒(1bg) wymagała użycia technik logiki 1-go rzędu.

Problem 4. Czy (i jak) można udowodnić implikację (3bg)⇒(1bg) metodami czysto kombinatorycznymi, bez logiki?

Definicja bezgwiazdkowej gwiazdki ma naturę semantyczną (czy gwiazdka jest bezgwiazdkowa czy nie, zależy od wyniku jej działania). Podobną operację „rozpoznawalnej gwiazdki" można opisać syntaktycznie (tzn. zależnie od argumentu pod gwiazdką) jako tzw. „spójną gwiazdkę" (jak w rozdziale 4).

Problem 5. Opisać syntaktycznie operację bezgwiazdkowej gwiazdki.

Wiemy, że w monoidach śladów nierozstrzygalne są problemy rozpoznawalności języka racjonalnego (Berstel [1]) i bezgwiazdkowości języka racjonalnego (Muscholl i Petersen [23]). Chyba najsłynniejszym (i najstarszym, Clerbout/Latteux [4] z 1985) otwartym problemem teorii śladów jest problem rozpoznawalności gwiazdki: Czy rozpoznawalność języka śladów T^* jest rozstrzygalna dla rozpoznawalnych T?

Problem 6 (Problem bezgwiazdkowości gwiazdki). Czy bezgwiazdkowość języka śladów T^* jest rozstrzygalna dla bezgwiazdkowych T?

Bibliografia

[1] J. Berstel: *Transductions and Context Free Languages.* B.G.Teubner, Stuttgart, 1979.

[2] P. Cartier, D. Foata: *Problèmes Combinatores de Commutation et réarrangements*, Lecture Notes in Mathematics, Vol. 85, Springer Berlin, 1969.

[3] M. Clerbout, M. Latteux: *On a generalization of partial commutations.* Proc. Fourth Hung. Computer Science Conf, 1985.

[4] M. Clerbout, M. Latteux: *Semi-commutations.* Information & Computation 73, pp. 59-74, 1987.

[5] V. Diekert: *Combinatorics on Traces*, Springer, 1990.

[6] V. Diekert, Y. Métivier: *Partial Commutation and Traces*, w [31] vol. 3, pp. 457-533, 1997.

[7] V. Diekert, G. Rozenberg (eds.): *The Book of Traces.* World Scientific, 1995.

[8] M. Droste, D. Kuske: *Languages and Logical Definability in Concurrency Monoids*, Proc. of CSL 1995, LNCS 1092, pp. 233-251, Springer, 1996.

[9] W. Ebinger: *Appendix: Logical Definability of Trace Languages*, w [7], pp. 383-390, 1995.

[10] W. Ebinger, A. Muscholl: *Logical definability on infinite traces.* Theoretical Computer Science 154(1), pp. 67-84, 1996.

[11] P. Gastin, E. Ochmański, A. Petit, B. Rozoy: *Decidability of the Star problem in* $A^* \times \{b\}^*$. Information Processing Letters 44, pp. 65-71, 1992.

[12] A. Gibons, W. Rytter: *On the Decidability of Some Problems about Rational Subsets of Free Partially Commutative Monoids.* Theoretical Computer Science 48(3), pp. 329-337, 1986.

[13] G. Guaiana: *Parties Reconnaissables et Morphismes sur les Monoides Trace*, These de Doctorat, Universite Paris VII, LITP TH94.07, 1994

[14] G. Guaiana, A. Restivo, S. Salemi: *Star-free trace languages.* Theoretical Computer Science 97, pp. 301-311, 1992.

[15] K. Hashiguchi: *Recognizable Closures and Submonoids of Free Partially Commutative Monoids.* Theoretical Computer Science 86, pp. 233-241, 1991.

[16] J.E. Hopcroft, R. Motwani, J.D. Ullman: *Introduction to Automata Theory, Languages and Computation.* Addison-Wesley, 2001.

[17] S. C. Kleene: Reprezentation of events in nerve nets and finite automata, Automata Studies. Princton Univ. Press, p. 3–42, 1956.

[18] B. Klunder: *Star-Connected Flat Languages and Automata.* Fundamenta Informaticae 72(1-3), pp. 235-243, 2006.

[19] B. Klunder, E. Ochmański, K. Stawikowska: *On Star-Connected Flat Languages.* Fundamenta Informaticae 67(1-3), pp. 93-105, 2005

[20] A. Mazurkiewicz: *Concurrent program schemes and their interpretations*, DAIM Rep. PB-78, Aarhus Univ., Aarhus, 1977.

[21] R. McNaughton, R. Yamada: *Regular expressions and state graphs for automata.* Trans. of IRE EC-9(1), pp. 11-18, 1960.

[22] R. McNaughton, S. Papert: *Counter-free Automata.* The M.I.T. Press, 1971.

[23] A. Muscholl, H. Petersen: *A Note on the Commutative Closure of Star-Free Languages.* Information Processing Letters 57(2), pp. 71-74, 1996.

[24] E. Ochmański: *Regular Behaviour of Concurrent Systems.* Bulletin of EATCS 27, pp. 56-67, 1985.

[25] E. Ochmański: *Recognizable Trace Languages*, w [7], pp.167-204. World Scientific, 1995.

[26] E. Ochmański, K. Stawikowska: *On closures of lexicoraphic star-free languages*, Proc. of AFL 2005, pp. 227-234, Institute of Informatics, University of Szeged, Węgry, 2005.

[27] E. Ochmański, K. Stawikowska: *Star-free star and trace langueages.* Fundamenta Informaticae 72(1-3), pp. 323-331, 2006.

[28] E. Ochmański, K. Stawikowska: *A Star Operation for Star-Free Trace Languages*, Proc. of DLT 2007, LNCS 4588, pp. 337-345, Springer 2007.

[29] E. Ochmański, P.A. Wacrenier: *On Regular Compatibility of Semi-Commutations.* Proc. of ICALP 1993, LNCS 700, pp. 445-456, Springer, 1993.

[30] D. Perrin: *Finite Automata.* Handbook of Theoretical Computer Science, vol. B, pp. 1-57, Elsevier, 1990.

[31] G. Rozenberg, A. Salomaa (eds.): Handbook ok Formal Languages, vol.1-3, Springer, 1997.

[32] J. Sakarovitch: *The "Last" Decision Problem for Rational Trace Languages.* Proc of LATIN 1992, LNCS 583, pp. 460-473, Springer 1992.

[33] A. Salomaa: Formal Languages. Academic Press, 1973.

[34] M. P. Schützenberger: *On finite monoids having only trivial subgroups*, Information and Control 8, pp. 190-194, 1965.

[35] K. Stawikowska, E. Ochmański: *On Star-Free Trace Languages and their Lexicographic Representations.* Proc. of the LATA2007, pp. 541-552, Universitat Rovira i Virgilli, Hiszpania, 2007.

[36] W. Thomas: *On Logical Definability of Trace Languages*, Proc. of ASMICS workshop, Report TUM-I9002, pp. 172-182, 1990.