Wydział Matematyki, Informatyki i Mechaniki UW

Algebraiczna Teoria Języków

skrypt z wykładu i ćwiczeń

semestr zimowy 2010/2011

Przedmiot prowadzili	Mikołaj Bojańczyk Tomasz Idziaszek Paweł Parys
Teksty spisali	Paweł Pasteczka Krzysztof Gogolewski Marcin Kotowski Michał Kotowski Michał Bendowski Katarzyna Krasnowska Michał Żak Dariusz Leniowski Adam Witkowski Michal Jatrzebski Bartosz Lewinski
Rozdziały zaakceptowane	1, 2, 3

Spis treści

Rozdział 1

Co to jest monoid

Spisali: Krzysztof Gogolewski i Paweł Pasteczka

Definicja 1. Monoid *to zbiór M wraz z określonym działaniem $\cdot$ takim, że:*

- *działanie $\cdot$ jest łączne: zachodzi $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,*
- *istnieje element neutralny 1 taki, że $1 \cdot a = a \cdot 1 = a$.*

Element neutralny może być tylko jeden. Istotnie, gdybyśmy mieli dwa, 1 oraz $1'$, to ich iloczyn spełniałby

$$1 = 1 \cdot 1' = 1'.$$

Łączność oznacza, że w dowolnie długim wyrażeniu postaci $a_1 a_2 \dots a_n$ nawiasowanie nie ma znaczenia.
Przykład.

1. Dla dowolnego zbioru A zbiór wszystkich słów A^* z konkatenacją i słowem pustym jest monoidem.
2. Na $M = \{0,1\}$ określamy działania:
   - Alternatywa: Widać, że w napisie $a_1 \vee a_2 \vee \dots \vee a_n$ nie ma znaczenia jak umieścimy nawiasy.
   - Koniunkcja (tj. mnożenie): Wiemy, że $a_1 \wedge a_2 \wedge \dots \wedge a_n$ jest łączne. Jest to monoid izomorficzny z alternatywą (za pomocą negacji tzn. $a_1 \wedge a_2 \wedge \ldots \wedge a_n = \neg(\neg a_1 \vee \neg a_2 \vee \ldots \vee \neg a_n\ )$
   - XOR (tj. dodawanie modulo 2): Podobnie jak wyżej jest w $a_1 \oplus a_2 \oplus \dots \oplus a_n$. Jest to grupa oznaczana przez $\mathbb{Z}_2$.
   - Implikacja **nie** jest monoidem, gdyż na ogół $a \Rightarrow (b \Rightarrow c)$ nie jest tym samym, co $(a \Rightarrow b) \Rightarrow c$ (na przykład dla $a = b = c = 0$).
   - Równoważność. Zauważmy, że $a \Leftrightarrow b = a \oplus b \oplus 1$. Stąd, $a \Leftrightarrow b \Leftrightarrow c = a \oplus b \oplus c$ niezależnie od nawiasowania. Jest to monoid izomorficzny z XOR (też za pomocą negacji).

□

1.1 Rozpoznawanie

Definicja 2. *Język $L \subseteq A^*$* **jest rozpoznawalny przez homomorfizm** *$\alpha\colon A^* \underset{\text{na}}{\longrightarrow} M$, jeśli jest spełniony jeden z równoważnych warunków:*

- *należenie $w \in L$ zależy tylko od wartości $\alpha(w)$,*
- *istnieje podzbiór $F \subseteq M$ taki, że $L = \alpha^{-1}(F)$.*

Poniżej będziemy zakładać, że M jest monoidem skończonym.

Twierdzenie 1. *Dla dowolnego języka $L \subseteq A^*$ następujące warunki są równoważne:*

1. *L jest regularny,*
2. *L jest rozpoznawalny przez homomorfizm w skończony monoid.*

Dowód
($2 \Rightarrow 1$) Jeżeli L jest rozpoznawalny przez homomorifzm w skończony monoid, to tworzymy automat o stanach $Q = M$ i funkcji przejścia $\delta(q,a) = q \cdot f(a)$.

($1 \Rightarrow 2$) Jeżeli L jest regularny, to jest rozpoznawalny przez deterministyczny automat skończony o stanach Q. Rozpatrzmy zbiór wszystkich funkcji Q^Q wraz ze składaniem. Określamy homomorfizm $f : A^* \to M$ na literach wzorem $f(a) = g$ gdzie $g(q) = \delta^*(q,a)$. (Ta konstrukcja działa dla automatu niedeterministycznego, jeżeli rozpatrzy się monoid relacji $\mathbb{P}(Q \times Q)$ ze składaniem relacji.) $\square$

1.2 Motywacja do algebraicznego podejścia

Automat pamięta tylko informacje o prefiksach słowa. Natomiast monoid musi pamiętać informacje o infiksach. Monoid przez to ma na ogół więcej elementów niż automat. Dobrze to widać na języku $L = A^9aA^*$ słów, których dziesiąta litera to a. Można go rozpoznać za pomocą automatu mającego ok. 10 stanów, natomiast monoid musi mieć ok. 2^{10} stanów. Niekiedy ta dodatkowa struktura ułatwia dowody indukcyjne. Dla słów nieskończonych teoria algebraiczna daje alternatywny sposób determinizacji automatów Büchiego (inny niż drzewa Safry).

1.2.1 Podobieństwo z teorią grup

Ponieważ grupy są monoidami, można zastanawiać się nad związkami teorii grup z teorią monoidów.

Twierdzenie 2 (Schützenberger, McNaughton, Papert)**.** *Dla języka $L \subseteq A^*$ następujące warunki są równoważne:*

- *L można opisać w logice pierwszego rzędu (FO),*
- *L jest rozpoznawalny przez homomorfizm w monoid, który nie zawiera żadnej nietrywialnej grupy jako podmonoid,*
- *L jest rozpoznawalny przez automat bezlicznikowy,*
- *L można opisać wyrażeniem regularnym, nie korzystając z gwiazdki, ale być może – z dopełnienia.*

1.2.2 Zastosowania

Przykład. Powiedzmy, że mamy dane długie słowo w i chcemy szybko sprawdzić na maszynie równoległej czy należy ono do języka regularnego L. Automaty są sekwencyjne – musimy czytać słowo w czasie $O(n)$. Korzystając z monoidu, możemy każdemu procesorowi przydzielić infiks, co daje algorytm działający w czasie $O(\log n)$ na $O(n)$ procesorach.

Korzystając z omawianej teorii, można podać strukturę danych, która dla ustalonego języka regularnego L wczytuje w czasie $O(n)$ słowo długości n, a następnie w czasie $O(1)$ odpowiada na pytanie, czy $a_i a_{i+1} \dots a_j \in L$. $\square$

Rozdział 2

Teoria Greena

Spisali: Marcin Kotowski i Michał Kotowski

Na tym wykładzie zajmiemy się teorią Greena, czyli „nauką o spójnych składowych monoidu".

2.1 Relacje Greena

Definicja 3. *Niech M – monoid i $m, n \in M$.*

- m **jest prefiksem** n*, jeśli $mx = n$ dla pewnego $x \in M$ (oznaczenie: $m \geqslant_{\mathcal{R}} n$).*
- m **jest sufiksem** n*, jeśli $xm = n$ dla pewnego $x \in M$ (oznaczenie: $m \geqslant_{\mathcal{L}} n$).*
- m **jest infiksem** n*, jeśli $xmy = n$ dla pewnych $x, y \in M$ (oznaczenie: $m \geqslant_{\mathcal{J}} n$).*

Uwaga. Relację $m \geqslant_{\mathcal{R}} n$ można zapisać inaczej jako $n \in mM$, gdzie $mM = \{mx \mid x \in M\}$ nazywamy prawym ideałem m w M. Jeśli $m \geqslant_{\mathcal{R}} n$, to $nM \subseteq mM$, co uzasadnia kierunek nierówności w przyjętej notacji.

Fakt 3. *Relacje $\geqslant_{\mathcal{R}}$, $\geqslant_{\mathcal{L}}$, $\geqslant_{\mathcal{J}}$ są zwrotne i przechodnie.*

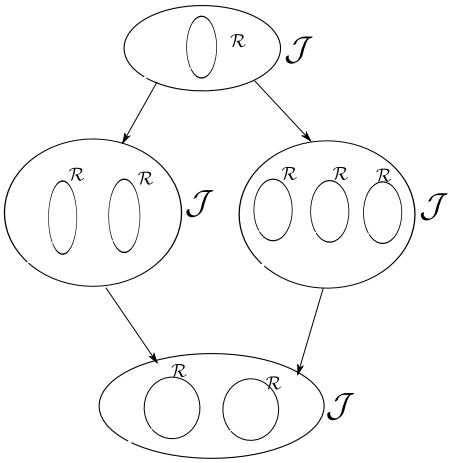
Uwaga. Powyższe relacje nie muszą być antysymetryczne (nie są więc porządkami) – na przykład w $\mathbb{Z}_2$ ze standardową strukturą dodawania mamy $0 \geqslant_{\mathcal{R}} 1$ i $1 \geqslant_{\mathcal{R}} 0$, ale $0 \neq 1$.

Definicja 4. *Wprowadzamy relację: $m \sim_{\mathcal{R}} n$ wtedy i tylko wtedy, gdy $m \geqslant_{\mathcal{R}} n$ i $n \geqslant_{\mathcal{R}} m$ (analogicznie dla $\geqslant_{\mathcal{L}}$, $\geqslant_{\mathcal{J}}$). Jest to relacja równoważności – jej klasy abstrakcji będziemy nazywać* $\mathcal{R}$**-klasami** *(dla $\geqslant_{\mathcal{L}}$ i $\geqslant_{\mathcal{J}}$ odpowiednio* $\mathcal{L}$**-klasami** *i* $\mathcal{J}$**-klasami**)*

Oznacza to, że cały monoid M możemy podzielić na rozłączne „spójne składowe", w obrębie których każdy element jest prefiksem (sufiksem, infiksem) każdego innego. Teoria Greena polega na badaniu struktury takich składowych (zdefiniowane powyżej relacje nazywa się relacjami Greena).

Dalej dowodzimy większości faktów dla relacji $\geqslant_{\mathcal{R}}$, sformułowania dla $\geqslant_{\mathcal{L}}$ są analogiczne.

Fakt 4. *Jeśli $m \geqslant_{\mathcal{R}} n$, to $m \geqslant_{\mathcal{J}} n$ (w szczególności każda $\mathcal{R}$-klasa jest zawarta w pewnej $\mathcal{J}$-klasie).*



Uwaga. Jeśli monoid M jest skończony, to istnieje w nim najmniejsza (w sensie relacji $\sim_{\mathcal{J}}$)$\mathcal{J}$-klasa (należy do niej np. element $n_1 \cdot \cdots \cdot n_k$, gdzie $M = \{n_1, \ldots, n_k\}$).

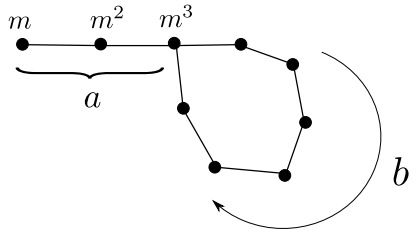
Jeśli nie będzie powiedziane inaczej, dalej będziemy zakładać, że M jest monoidem skończonym.

Definicja 5. *Element $m \in M$ nazywamy* **idempotentem**, *jeśli $m^2 = m$.*

Przyda nam się dalej następujący lemat:

Lemat 5. *Istnieje $i \in \mathbb{N}$ takie, że dla każdgo $m \in M$ element m^i jest idempotentem.*

Dowód
Rozpatrzmy ciąg elementów $m, m^2, m^3, \ldots$ Ponieważ monoid M jest skończony, to ciąg ten musi się w którymś momencie „zapętlić" (rysunek) – oznacza to, że istnieją takie $a, b \in \mathbb{N}$, że wszystkie elementy $m, m^2, \ldots, m^a$ są różne, a dla dalszych elementów zachodzi $m^j = m^k \Leftrightarrow j \equiv k \mod b$



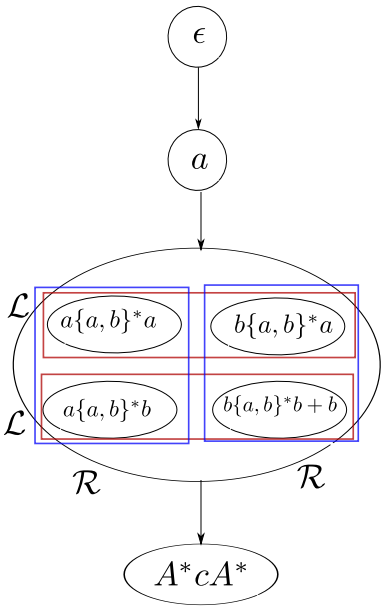
Jeśli m^i ma być idempotentem, to wystarczy, aby zachodziło $i > a$ oraz $m^i = m^{2i}$, czyli $i \equiv 0 \mod b$. Łatwo zobaczyć, że $i = |M|!$ spełnia te warunki, co kończy dowód. □

Uwaga. Liczbę i z powyższego lematu będziemy oznaczać przez ω, a potęgę elementu m, która jest idempotentem, przez m^ω. Łatwo jest zobaczyć, że każdy element ma dokładnie jedną taką potęgę, więc oznaczenie to jest jednoznaczne.

Lemat 6. *W obrębie każdej $\mathcal{J}$-klasy poszczególne $\mathcal{R}$-klasy są nieporównywalne (czyli jeśli $m \sim_{\mathcal{J}} n$ i $m \geqslant_{\mathcal{R}} n$, to $m \sim_{\mathcal{R}} n$).*

Dowód
Chcemy znaleźć takie $u \in M$, że $nu = m$. Niech $mx = n$ i $ynz = m$ dla pewnych $x, y, z \in M$. Z równości tych wynika, że $ymxz = m$. Możemy w ten sposób dopisać z lewej y, a z prawej xz, ω razy. Mamy wtedy $y^\omega m(xz)^\omega = m$. Gdy dopiszemy po obu stronach z prawej $(xz)^\omega$ i skorzystamy z równości $(xz)^{2\omega} = (xz)^\omega$, dostaniemy $m = y^\omega m(xz)^\omega = y^\omega m(xz)^\omega (xz)^\omega = m(xz)^\omega$. Zmieniwszy w równości $m = m(xz)^\omega$ sposób nawiasowania, otrzymamy $m = (mx)z(xz)^{\omega-1} = nz(xz)^{\omega-1}$ – przyjmując $u = z(xz)^{\omega-1}$, dostaniemy więc tezę. □

Przykład. Rozpatrzmy alfabet $A = \{a, b, c\}$ oraz język $L = a\{a, b\}^*a$. Przykładowy monoid rozpoznający ten język przedstawiony jest na rysunku:



Mamy tutaj 7 elementów i 4 $\mathcal{J}$-klasy ustawione w łańcuch. Przecięcia $\mathcal{R}$- i $\mathcal{L}$-klas są tu jednoelementowe, w szczególności są równoliczne i niepuste – za chwilę przekonamy się, że nie jest to przypadek i jest tak w każdym monoidzie. □

2.2 Struktura $\mathcal{H}$-klas

Definicja 6. **$\mathcal{H}$-klasą** *nazywamy przecięcie $\mathcal{R}$-klasy i $\mathcal{L}$-klasy.*

Twierdzenie 7. *W jednej $\mathcal{J}$-klasie wszystkie zawarte w niej $\mathcal{H}$-klasy są równoliczne. $\mathcal{H}$-klasy, które zawierają idempotent, są grupami.*

Dowód
Dla dowolnego $x \in M$ określamy funkcję $f_{\_x}\colon M \to M$, $f_{\_x}(m) = mx$ i analogicznie funkcję $f_{x\_}$.

Załóżmy, że $m \sim_{\mathcal{J}} n$ – wówczas istnieją takie $x, y \in M$, że $n = xmy$. Ponieważ $m \sim_{\mathcal{R}} my$ i $my \sim_{\mathcal{L}} xmy$ (z poprzedniego lematu), to widać, że przecięcie $\mathcal{R}$-klasy $[m]_{\mathcal{R}}$ i $\mathcal{L}$-klasy $[n]_{\mathcal{L}}$ jest niepuste – możemy dojść z m do n, idąc najpierw po $\mathcal{R}$-klasie, a potem po $\mathcal{L}$-klasie, $m \mapsto my \mapsto xmy = n$.

Dla ustalonych m,$n, m \sim_{\mathcal{J}} n$ pokażemy bijekcję pomiędzy $[m]_{\mathcal{R}}$ i $[n]_{\mathcal{R}}$. Niech x,y – jak wyżej,$n = xmy$. Łatwo widać,że $n \sim_{\mathcal{J}} xm$ – istnieją bowiem takie z,v, że $m = znv$, więc $xznv = xm$. Stąd $[n]_{\mathcal{R}} = [xm]_{\mathcal{R}}$.

Pokażemy teraz, że funkcja $f_{x\_}$ jest bijekcją pomiędzy $\mathcal{R}$-klasami $[m]_{\mathcal{R}}$ i $[xm]_{\mathcal{R}}$. Widać, że jest to funkcja „na” – niech $n' \in [xm]_{\mathcal{R}}, n' = xmz$. Wtedy $f_{x\_}(mz) = xmz = n'$ oraz $mz \sim_{\mathcal{R}} m$ (bo $xmz = n' \sim_{\mathcal{J}} xm \sim_{\mathcal{J}} m$, zatem $mz \sim_{\mathcal{J}} m$). Aby pokazać, że jest to bijekcja, wskażemy funkcję odwrotną. Ponieważ $xm \sim_{\mathcal{L}} m$, to istnieje takie $z \in M$, że $zxm = m$. Wobec tego złożenie funkcji $f_{z\_} \circ f_{x\_}$ jest identycznością na $[m]_{\mathcal{R}}$, czyli $f_{x\_}$ jest bijekcją.

$f_{x\_}$ jest też bijekcją $\mathcal{H}$-klas $[m]_{\mathcal{H}}$ i $[xm]_{\mathcal{H}}$. Aby to udowodnić, trzeba pokazać, że dowolnego $n \in [m]_{\mathcal{H}}$ mamy $xn \sim_{\mathcal{L}} xm$. Mamy jednak $n \sim_{\mathcal{L}} xn$ i $m \sim_{\mathcal{L}} xm$, a z założenia $n \in [m]_{\mathcal{H}}$, czyli w szczególności $n \sim_{\mathcal{L}} m$, skąd wynika, że istotnie $xn \sim_{\mathcal{L}} xm$.

Pokażemy teraz, że jeśli H jest $\mathcal{H}$-klasą zawierającą idempotent e, to jest grupą. Łączność mnożenia w H dziedziczy się w łączności w M. H jest zamknięta na mnożenie – jeśli $m, n \in H$, to $m = xe$ i $n = ey$ dla

pewnych x, y i $zm = e, nv = e$ dla pewnych z,v, skąd $xzmnv = xzme = xee = xe = m$, czyli $mn \sim_{\mathcal{J}} m$, skąd wynika $mn \sim_{\mathcal{R}} m$. Analogicznie $mn \sim_{\mathcal{L}} n$. Zatem $mn \in H$. Jedynką w H jest idempotent e – ponieważ $m \sim_{\mathcal{H}} e$, to $m = ex$ dla pewnego x, a zatem $em = eex = ex = m$ i analogicznie dla mnożenia przez e z prawej. Z faktu, że $m \sim_{\mathcal{R}} e$ i $m \sim_{\mathcal{L}} e$, wynika, że każdy element m posiada lewy i prawy element odwrotny, i łatwo widać, że są one sobie równe. Lewe i prawe odwrotności są jednoznaczne, bo jeśli $mx = e, my = e$, a $zm = e$, to $x = ex = zmx = zmy = ey = y$ i tak samo dla prawej odwrotności.

□

Wniosek 8. *Monoid, który ma tylko jedną $\mathcal{H}$-klasę, jest grupą.*

Rozdział 3

Języki rozpoznawane przez monoidy aperiodyczne

Spisali: Michał Bendowski i Katarzyna Krasnowska

3.1 Monoid syntaktyczny

Monoid syntaktyczny to algebraiczny odpowiednik automatu minimalnego. Rozważmy następującą relację $\sim_L$ na A^*: $w \sim_L w'$ wtw. gdy $\forall_{x,y \in A^*} xwy \in L \Leftrightarrow xw'y \in L$. Zauważmy podobieństwo tej relacji do relacji Myhilla-Nerode'a.

Przykład. Rozważmy język $L = (aa)^*$ and alfabetem $A = \{a\}$. Mamy wtedy dwie klasy abstrakcji, odpowiadające słowom $(aa)^*$ i $a(aa)^*$.

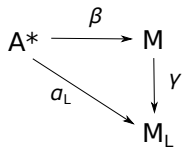
Zdefiniujmy działanie $\cdot$ w następujący sposób: $[w]_L \cdot [v]_L = [w \cdot v]_L$. Zauważmy, że tak określone działanie jest dobrze zdefiniowane: niech $[w']_L = [w]_L$ (czyli $w \sim_L w'$). Wtedy z definicji mamy, że dla dowolnego v zachodzi $wv \sim_L w'v$.

Z powyższego wynika, że zbiór klas abstrakcji relacji $\sim_L$ ma strukturę monoidu. Monoid ten nazywamy monoidem syntaktycznym.

Definicja 7. *Monoid syntaktyczny języka L to zbiór $M_L = \{[w]_L : w \in A^*\}$, wraz z działaniem zdefiniowanym powyżej.*

Od razu nasuwa się idea odpowiedniego homomorfizmu $\alpha_L : A^* \to M_L$, mianowicie $\alpha_L(w) = [w]_L$. Taki homomorfizm nazywamy homomorfizmem syntaktycznym.

Twierdzenie 9. *Niech $\beta : A^* \xrightarrow{na} M$ będzie homomorfizmem rozpoznającym język $L \subseteq A^*$. Wówczas istnieje dokładnie jeden homomorfizm $\gamma : M \xrightarrow{na} M_L$ taki, że dla każdego w mamy $\gamma(\beta(w)) = \alpha_L(w)$.*



Wniosek 10. *Jeśli istnieje homomorfizm $\beta : A^* \xrightarrow{na} M$, wówczas monoid M_L jest obrazem homomorficznym M.*

Z powyższego wniosku wynika, że jeśli M ma tyle samo elementów co M_L, to są one izomorficzne – innymi słowy M_L jest „najlepszy z dokładnością do izomorfizmu". Monoid syntaktyczny istnieje dla każdego języka. Istnieje wiele wyników postaci *„Język L ma własność $X \Leftrightarrow M_L$ ma własność Y"*, a dzisiejszy wykład jest poświęcony jednemu z nich. Zanim jednak do niego przejdziemy, zauważmy, że nie każda własność X ma odpowiadającą jej własność Y, na przykład:

Przykład. Niech $L = \emptyset$, wtedy M_L ma tylko jeden element – żadne słowo nie należy do L. Niech $K = A^*$, wtedy M_K też ma tylko jeden element – wszystkie słowa należą do K. Dla obu tych języków monoid syntaktyczny wygląda tak samo, różnią je zbiory akceptujące.

Na podstawie powyższego przykładu widać w szczególności, że własność X musi być zamknięta ze względu na negację.

Przykład. Niech $A = \{a\}$, $L = aA^*$. Wtedy $M_L = \{\{\varepsilon\}, L\}$. Niech $B = \{a,b\}$, $L' = b^*aA^*$ Wtedy $M_{L'} = \{b^*, L'\}$. Oba te języki mają taki sam monoid syntaktyczny.

Powyższy przykład pokazuje w szczególności, że nie można wskazać własności Y monoidu odpowiadającej własności X należenia do klasy **definite languages** (są to języki, dla których istnieje liczba $k \in \mathbb{N}$ taka, że przynależność do języka zależy wyłącznie od k pierwszych liter słowa).

Ogólnie rzecz biorąc, żeby dla pewnej własności X istniała odpowiadająca jej własność Y, wystarczy, aby X była zamknięta ze względu na:

- Operacje boolowskie
- Przeciwobrazy homomorficzne
- Pewne rodzaje ilorazów (więcej o tym później)

Spełnienie powyższych warunków jest wystarczające, ale niekonieczne — weźmy np. $Y =$ *„monoid syntaktyczny ma dokładnie 2 elementy"*.

3.2 Monoid aperiodyczny

Lemat 11. *Niech M — monoid skończony. Wówczas następujące warunki są równoważne:*

(a) M nie zawiera grupy nietrywialnej (czyli nie istnieje $G \subseteq M$, niekoniecznie zawierający jedność z M, który z działaniem w M i swoją jednością, tworzy grupę i $|G| > 1$),

(b) dla każdego $m \in M$ istnieje liczba $i \in \mathbb{N}$ taka, że $m^i = m^{i+1}$,

(c) wszystkie $\mathcal{H}$-klasy w M są trywialne.

*Taką własność monoidu nazywamy **aperiodycznością**.*

Dowód

$(a) \Rightarrow (b)$: Rozważmy element monoidu $m \in M$ oraz jego kolejne potęgi: m, m^2, m^3, ..., m^k, ... M jest skończony, zatem istnieją takie liczby $i, j \in \mathbb{N}$, że $m^i = m^j$. Wówczas elementy m^i, m^{i+1}, ..., m^{j-1}, m^j tworzą grupę. Zgodnie z założeniem (a), grupa ta jest trywialna, zatem wszystkie te elementy są sobie równe, w szczególności $m^i = m^{i+1}$.

$(b) \Rightarrow (c)$: Weźmy dowolne $m, n \in M$ takie, że $m \sim_{\mathcal{H}} n$. Istnieją wówczas $x, y \in M$ takie, że $mx = n$ oraz $yn = m$. Zgodnie z założeniem (b) istnieje również $i \in \mathbb{N}$ takie, że $x^i = x^{i+1}$. Mamy wówczas: $mx = n$,

$ymx = yn = m$, ..., $y^i m x^i = m$, $y^i m x^{i+1} = n$. Teraz widać, że $m = y^i m x^i = y^i m x^{i+1} = n$, zatem każda $\mathcal{H}$-klasa w M jest trywialna.

$(c) \Rightarrow (a)$: Każda grupa zawarta w M musi być zawarta w pewnej $\mathcal{H}$-klasie w M, zatem jest trywialna. □

Uwaga. Założenie o skończoności M jest istotne — prostym przykładem monoidu nieskończonego, dla którego lemat nie jest prawdziwy, jest $M = \mathbb{N}$.

3.3 Aperiodyczność monoidu a własności języka

Teraz przedstawimy twierdzenie mówiące o własnościach języka regularnego odpowiadających własności aperiodyczności monoidu syntaktycznego dla tego języka. W tym celu należy wprowadzić kilka pojęć.

Wyrażenia bezgwiazdkowe *(ang. star-free)* jest to odmiana wyrażeń regularnych, w której nie występuje operator domknięcia Kleene'ego (*), jest natomiast używane dopełnienie (w przeciwnym przypadku klasa języków star-free byłaby ograniczona do języków skończonych). Dozwolone operacje to zatem $+$, $\cdot$ oraz $\neg$; bazą wyrażeń są języki postaci $\{a\}$, gdzie a to symbol należący do alfabetu, oraz język pusty.

Przykład. Rozważmy alfabet $A = \{a, b\}$. Wówczas język A^* można opisać wyrażeniem bezgwiazdkowym $\neg\emptyset$, natomiast język b^* — wyrażeniem $\neg(\neg\emptyset a\neg\emptyset)$. Mamy również $A - B = \neg((\neg A) + B)$ i $A \cap B = (A + B) - (A - B) - (B - A)$.

Logika pierwszego rzędu (FOL) również może służyć jako mechanizm opisywania języków. Posługujemy się w tym celu:

- kwantyfikacją po pozycjach w słowie,
- predykatami mówiącymi o występowaniu na danej pozycji określonej litery alfabetu,
- porównywaniem pozycji pod względem kolejności występowania w słowie.

Przykład. Język A^*ab^* $(A = \{a, b\})$ można opisać formułą $\exists x(a(x) \wedge \forall y(y > x \Rightarrow b(y)))$.

Mówimy, że automat skończony ma **licznik**, jeżeli istnieje słowo w oraz ciąg stanów automatu q_1, q_2, ..., q_n $(n \geqslant 2)$ taki, że $q_1 \overset{w}{\rightsquigarrow} q_2 \overset{w}{\rightsquigarrow} \ldots \overset{w}{\rightsquigarrow} q_n \overset{w}{\rightsquigarrow} q_1$.

Możemy teraz sformułować następujące twierdzenie:

Twierdzenie 12. *Dla języka $L \subseteq A^*$ następujące warunki są równoważne:*

- *M_L jest aperiodyczny,*
- *L można opisać wyrażeniem bezgwiazdkowym,*
- *L można opisać zdaniem FOL,*
- *automat minimalny rozpoznający L nie ma licznika.*

Dowód

Dowodzimy implikacji: M_L jest aperiodyczny $\Rightarrow$ L można opisać wyrażeniem bezgwiazdkowym.

W dowodzie używamy indukcji po $\mathcal{J}$-klasach w M_L. Bazą indukcyjną będzie $\mathcal{J}$-klasa zawierająca 1 – wrócimy do niej pod koniec dowodu.

Definicja 8. $L_m = \{w \in A^* : \phi_L(w) = m\}$ *dla* $m \in M_L$.

Mamy $m \in J \subseteq M$, J — $\mathcal{J}$-klasa.

Założenie indukcyjne Dla wszystkich $x >_{\mathcal{J}} m$ mamy wyrażenie bezgwiazdkowe, które będziemy oznaczać L_x, opisujące język L_x. Zakładamy ponadto, że $m \not\sim_{\mathcal{J}} 1$.

Krok indukcyjny Chcemy napisać L_m. Najpierw napiszemy wyrażenie K_m, które działa dobrze, o ile znajdujemy się w J. Intuicyjnie, K_m, wykrywa pierwszy moment, w którym „wpadamy" do J.

$$K_m = \Big(\bigcup_{\substack{x \in M \\ a \in A \\ x >_{\mathcal{J}} m \\ x \cdot \phi_L(a) \sim_{\mathcal{R}} m}} L_x a A^* \Big) \cap \Big(\bigcup_{\substack{y \in M \\ b \in A \\ y >_{\mathcal{J}} m \\ \phi_L(b) \cdot y \sim_{\mathcal{L}} m}} A^* b L_y \Big) \tag{3.1}$$

Fakt z poprzedniego wykładu Jeśli $x \leqslant_{\mathcal{R}} y$ oraz $x \sim_{\mathcal{J}} y$, to $x \sim_{\mathcal{R}} y$.

Obserwacja

(1) $\phi_L(w) = m \Rightarrow w \in K_m$

Znajdujemy najkrótszy v — prefiks w — taki, że $\phi_L(v) \sim_{\mathcal{J}} m$. Wiemy, że $\phi_L(v) \geqslant_{\mathcal{R}} m$. Z faktu wynika, że $\phi_L(v) \sim_{\mathcal{R}} m$.

$v \neq \epsilon$ (bo $\phi_L(\epsilon) = 1$), więc $v = v'a$, gdzie $\phi_L(v') >_{\mathcal{J}} m$.

Symetrycznie postępujemy dla drugiego podwyrażenia.

(2) $w \in K_m \Rightarrow$ mamy 2 możliwości: (1) $\phi_L(w) = m$, albo (2) $\phi_L(w) <_{\mathcal{J}} m$ oraz dla pewnego v — prefiksu w — zachodzi $\phi_L(v) \sim_{\mathcal{R}} m$.

- Jeśli $\phi_L(w) \not\sim_{\mathcal{J}} m$, to $\phi_L(w) <_{\mathcal{J}} m$, bo prefiks pasujący do $L_x a$ jest w $\mathcal{J}$-klasie m.
- Jeśli $\phi_L(w) \sim_{\mathcal{J}} m$, to prefiks v pasujący do $L_x a$ spełnia $\phi_L(v) \sim_{\mathcal{R}} m$, czyli $\phi_L(w) \leqslant_{\mathcal{R}} m$, czyli $\phi_L(w) \sim_{\mathcal{R}} m$ (z faktu). Analogicznie, $\phi_L(w) \sim_{\mathcal{L}} m$, czyli $\phi_L(w) \sim_{\mathcal{H}} m$, co znaczy, że $\phi_L(w) = m$ (bo M_L jest aperiodyczny, czyli każda $\mathcal{H}$-klasa jest trywialna).

Chcemy "poprawić" wyrażenie K_m:

$$L'_m = K_m - \bigcup_{\substack{x \sim_{\mathcal{J}} m \\ x \phi_L(a) <_{\mathcal{J}} m \\ x \in M, a \in A}} K_x a A^* \tag{3.2}$$

Teraz musimy udowodnić, że $L'_m = L_m$, którego szukamy.

Dowód

- $L_m \subseteq L'_m$ – proste.

  Załóżmy, że $\phi_L(w) = m$. $w \in K_m$ z obserwacji (1). Jeśli va — pewien prefiks w taki, że $v \in K_x$, to mamy 2 przypadki:

  - $\phi_L(v) = x$, wtedy $\phi_L(va) <_{\mathcal{J}} m$, czyli $\phi_L(w) <_{\mathcal{J}} m$
  - $\phi_L(v) <_{\mathcal{J}} m$, wtedy $\phi_L(w) <_{\mathcal{J}} m$.

- $L'_m \subseteq L_m$

  Weźmy $w \in L'_m$ (czyli $w \in K_m$). Jeśli $\phi_L(w) \neq m$, to mamy v — prefiks w taki, że $\phi_L(v) \sim_{\mathcal{J}} m$. Weźmy najdłuższy taki v.

  Niech a — kolejna litera w po v (taka istnieje, bo założyliśmy, że $\phi_L(w) <_{\mathcal{J}} m$ — $\phi_L(va) <_{\mathcal{J}} m$ z obserwacji (2), druga możliwość).

  Bierzemy $x = \phi_L(v)$. Otrzymujemy sprzeczność – takie w nie mogło należeć do L'_m.

To kończy dowód z wyłączeniem $\mathcal{J}$-klasy zawierającej 1. Ale $\mathcal{J}$-klasa z 1 jest jednoelementowa:
Załóżmy, że $xmy = 1$:

(1) $(mx)^\omega m(y)^\omega = m = (mx)^\omega m(y)^\omega y = my$

(2) $(x)^\omega m(ym)^\omega = m = x(x)^\omega m(ym)^\omega = xm$

Czyli $m \sim_{\mathcal{H}} 1 \Rightarrow m = 1$

Teraz widać, że:

$$L_1 = \Big(\bigcup_{\substack{a \in A \\ \phi_L(a)=1}} a \Big)^* = A^* - \bigcup_{\substack{b \in A \\ \phi_L(b)\neq 1}} A^* b A^* \tag{3.3}$$

□

Rozdział 4

Wyklad 4

Spisali: Michał Żak i Dariusz Leniowski

4.1 Logika, a języki regularne

Wprowadźmy następujące pojęcia logiki:

Definicja 9. *$FO_3(<)$ logika pierwszego rzędu, której formuły zawierają nie więcej niż trzy zmienne.*

Przykład. Formuła $\exists x\ \exists y{>}x\ \exists x{>}y\ \exists y{>}x$. `true` opisuje język $\{w \in A^* |\ 4 \leqslant |w|\}$ $\square$

Definicja 10 (`LTL`)**.** *Liniowa logika temporalna to logika, której formułami są relacje zeroargumentowe a dla $a \in A$ oraz wyrażenia postaci $\phi \vee \psi$, $\phi \wedge \psi$, $\neg\phi$, $X\phi$ i $\phi U \psi$ dla pewnych formuł ϕ oraz ψ.*

Wartość formuły w logice `LTL` *zależy od miejsca w którym formuła jest wyliczana. Prawdziwość formuły ϕ w słowie w na pozycji x będziemy oznaczać przez $w,x \models \phi$. Znaczenie poszczególnych operatorów określone jest poniżej:*

- *$w,x \models a$ wtw. w słowie w na pozycji x stoi litera a,*
- *$w,x \models \phi \vee \psi$ wtw. $w,x \models \phi$ lub $w,x \models \psi$,*
- *$w,x \models \phi \wedge \psi$ wtw. $w,x \models \phi$ i $w,x \models \psi$,*
- *$w,x \models \neg\phi$ wtw. nieprawda, że $w,x \models \phi$,*
- *$w,x \models X\phi$ wtw. $w,x+1 \models \phi$,*
- *$w,x \models \phi U \psi$ wtw. $\exists y \geqslant x\ (w,y \models \psi) \wedge \forall z{<}y.\ z \geqslant x \Rightarrow w,z \models \phi$.*

Dodatkowo stosuje się skróty

- *$w \models \phi$ dla $w,1 \models \phi$,*
- *$F\phi$ dla $\texttt{true}\,U\phi$,*
- *$G\phi$ dla $\neg F \neg \phi$,*
- *$\psi R \phi$ dla $\neg(\neg\psi U \neg phi)$.*

Przykład. Formuła aUb jest spełniana, przez wszystkie słowa z języka a^*bA* (i żadne inne). Język a^*b wyznaczany jest natomiast przez formułę $aU(b \wedge \neg X\,\texttt{true})$. $\square$

Możemy teraz rozszerzyć twierdzenie 12 o kolejne równoważne stwierdzenia:

Twierdzenie 13. *Następujące warunki dla języka $L \subset A^*$ są równoważne:*

- *L można opisać formułą $FO(<)$,*
- *L można opisać formułą $FO_3(<)$,*
- *L można opisać formułą* `LTL`*.*

Dowód

- L można opisać formułą $FO_3(<) \Rightarrow L$ można opisać formułą $FO(<)$
  — oczywiste.
- L można opisać formułą `LTL` $\Rightarrow L$ można opisać formułą $FO_3(<)$
  — także dość łatwo. Dowodzimy implementując definicję `LTL` za pomocą formuł $FO_3(<)$ móc wyrazić następną pozycję, co czynimy określając $y = x + 1$
  $\exists y{>}x.\ (\neg\exists z.\ x < z < y) \wedge \phi(y)$.
- L można opisać formułą $FO(<) \Rightarrow L$ można opisać formułą `LTL`
  wystarczy pokazać, że każdą formułę $FO(<)$ możemy zapisać używając co najwyżej trzech zmiennych. Czynimy to w nastepujący sposób:
  1. przepisujemy formułę, aż musimy użyć czwartej zmiennej;
  2. zamiast nowej zmiennej możemy użyć jednej z już użytych, możemy założyć, że mamy ustalony porządek na wprowadzonych zmiennych — na przykład dla $x < y < z$, jeśli zachodzi potrzeba wprowadzenia $q > z$ to równie dobrze możemy wprowadzić $x > z$, a dla r takiego, że $x < r < y$ moglibyśmy kwantyfikować po nowym z, dla którego $x < z < y$; analogicznie w pozostałych przypadkach.
- Część $FO(<) \Rightarrow$ `LTL` wynika z lematu 15 i twierdzenia 12.

□

Definicja 11. *Niech f będzie dowolną funkcją częściową $f : A^* \to X$, dla pewnego skończonego zbioru X. Powiemy, że f należy do logiki* `LTL` *($f \in$ `LTL`) jeżeli dla każdego możliwego wyniku $x \in X$ istnieje formuła $\phi_x \in$ `LTL` taka, że dla każdego słowa $w \in A^*$ zachodzi $w \models \phi_x$ wtedy i tylko wtedy gdy $f(w) = x$.*

Lemat 14. *Niech M będzie monoidem aperiodycznym i $a \in A$ będzie dowolną literą alfabetu A. Wtedy $f_{a\_} : M \to M$ jest surjektywna wtedy i tylko wtedy gdy jest identycznością.*

Dowód
Jeżeli f jest surjekcją, to jest też bijekcją, a wtedy ze skończoności M wynika, że kolejne iteracje f tworzą grupę symetryczną. Niech k będzie rzędem tej grupy, wtedy $f^{(k+1)} \equiv f$ i z aperiodyczności M mamy $k = 1$.
□

Lemat 15. *Niech $\alpha : A^* \to M$, gdzie M jest monoidem aperiodycznym, wtedy każdy język rozpoznawany przez α jest definiowalny w* `LTL`*.*

Dowód
Dowód będzie polegał na indukcji po rozmiarze monoidu i rozmiarze alfabetu (ściśle po parach $\langle|M|,|A|\rangle$ w porządku leksykograficznym).

Baza indukcji: [[nie było]]

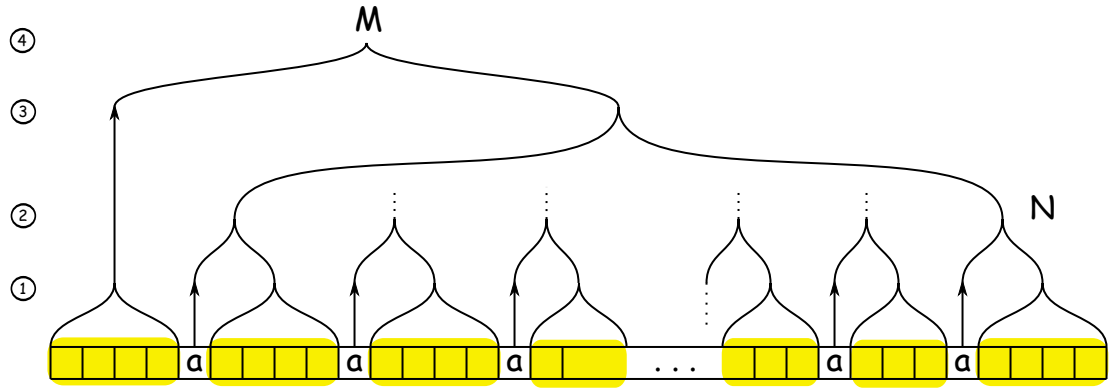
Rozważmy zbiór liter A', taki, że $\forall b \in A'\ f_{b\_} \equiv id$, wtedy dla $A' = A$ zachodzi $\forall w \in A^*\ \alpha(w) = 1$ i oczywiście teza lematu jest prawdziwa. W przeciwnym wypadku, istnieje litera a, dla której na mocy lematu 14 $\forall m \in M\ \alpha(a)m \in N \subsetneq M$. Oznaczmy $B = A - \{a\}$.

Zauważmy, że N jest półgrupą (połączenie dwóch słów zaczynających się na a również zaczyna się na a). Niech N^1 oznacza monoid, taki, że $N^1 = N$, jeżeli N jest monoidem (zawiera element neutralny), lub $N^1 = N \cup 1'$, gdzie $1'$ będzie sztucznie dodaną jednością.

$|N^1| < |M|$, bo ... [[nie było]]

Schemat dowodu $\alpha \in$ `LTL` ma cztery kroki, będziemy pokazywać kolejno, że do `LTL` kolejno należą:

1. $\alpha|_{B^*}$ — z założenia indukcyjnego,
2. $\alpha|_{aB^*}$ — z lematu 16, gdzie $f = \alpha|_B$, $g = \alpha|_a$ i $\phi = X(a \wedge \neg X\texttt{true})$.
3. $\alpha|_{(aB^*)^*}$ — lemat **??**,
4. $\alpha|_{B^*(aB^*)^*} = \alpha$ — analogicznie do kroku drugiego.



□

Definicja 12. *Niech, f,$g : A^* \to M$ i f,$g \in$ LTL oraz ϕ - formuła* LTL. *Wtedy jeśli i jest ostatnią pozycją to $f \circ_\phi g(a_1a_3 \dots a_n) = f(a_1 \dots a_i)g(a_{i+1} \dots a_n)$*

Lemat 16. *Niech f,$g : A^* \to M$ należą do* LTL. *Niech $\phi \in$ LTL będzie pewną formułą. Wtedy $f \circ_\phi g$ też należy do* LTL.

Dowód
Niech $m \in M$. Trzeba pokazać, że zbiór słów $L_m = \{w \in A^* : (f \circ_\phi g)(w) = m\}$ należy do LTL. Niech ψ_1 i ψ_2 będą pewnymi formułami Określmy:

$$przed(\psi_1,\psi_2) = \{w \in A^* : c_1, \dots, c_i \models \psi_2, \text{ gdzie } i \text{ to pierwsza pozycja spełniająca } \psi_1$$

$$po(\psi_1,\psi_2) = \{w \in A^* : c_{i+1}, \dots, c_n \models \psi_2, \text{ gdzie } i \text{ to ostatnia pozycja spełniająca } \psi_1$$

Funkcje te można skonstruować za pomocą zależności $przed(\psi,c) = c \wedge F\psi$, $przed(\psi_1,\psi_2 \wedge \psi_3) = przed(\psi_1,\psi_2) \wedge przed(\psi_3)$ i analogicznych dla sumy i negacji. [[co z X i U?]]
Wtedy

$$L_m = \bigvee_{m_1,m_2 : m_1m_2 = m} przed(\phi, f^{-1}(m_1) \wedge po(\phi, g^{-1}(m_2)))$$

[[czy to wszystko?]]
□

Lemat 17. *Niech C będzie pewnym alfabetem i niech $\{\phi_c\}_{c \in C}$ będzie rodziną wzajemnie wykluczających się formuł logiki* LTL. *Określmy $f : A* \to C*$ przez $f(a_1 \dots a_n) = c_1 \dots c_n$, gdzie $c_i = c$ jeżeli $a_i \dots a_n \models \phi_c$ lub $c_i = \epsilon$ w przeciwnym wypadku.*

Wtedy dla dowolnej $g : C^* \to X$ należącej do LTL *złożenie $(f;g) : A^* \to X$ też należy do* LTL.

Dowód
Zamiast pytać się o literę, pytamy się o wynik przetwornika, czyli wszytksie formuły w g typu a, gdzie $g \in C$ zastępujemy przez formuły które są równoważne f daje wynik a na tej pozycji. Co jest definiowalne w LTL, bo $f \in$ LTL. [[tutaj jeszcze cos]] □

Lemat 18. *Funkcja* $f : (aB^*)^* \to N*$ *taka, że* $f(aw_1aw_2 \dots aw_k) = \alpha(aw_1)\alpha(aw_2) \dots \alpha(aw_k)$ *należy do* LTL.

Dowód
Oczywiste. □

Rozdział 5

Wykład 5

Spisał: Adam Witkowski

Poznaliśmy już algebraiczną charakteryzację monoidów aperiodycznych, czyli $\mathcal{H}$-trywialnych. Kontynuując badania monoidów skończonych, chcemy poznać również charakteryzacje monoidów X-trywialnych dla różnych relacji X. Przypomnijmy, że

Definicja 13. *Monoidem X-trywialnym dla $X = \mathcal{R}$, $\mathcal{L}$, $\mathcal{J}$, $\mathcal{H}$ nazywamy monoid w którym klasy abstrakcji relacji X są jednoelementowe.*

Nasz aktualny stan wiedzy na temat tych klas monoidów podsumowuje poniższy diagram:

$$\begin{array}{rcl} \text{Monoidy } \mathcal{H}\text{-trywialne} & = & FO,\ LTL \\ \cup\!| & & \\ \text{Monoidy } \mathcal{L}\text{-trywialne} & = & ? \\ \cup\!| & & \\ \text{Monoidy } \mathcal{J}\text{-trywialne} & = & ? \end{array}$$

5.1 Hierarchia logiczna pierwszego rzędu

Ponieważ chcemy opisać za pomocą logiki coraz mniejsze (w sensie zawierania) klasy monoidów, będziemy potrzebowali logik słabszych od logiki pierwszego rzędu. Każda formuła FO jest równoważna formule w postaci preneksowej normalnej:

$$\phi = \exists^* \forall^* \cdots \exists^* \psi(x_1, \cdots, x_n)$$

gdzie ψ nie zawiera kwantyfikatorów, a $\exists^*$ oznacza pewną skończoną ilość kwantyfikatorów egzystencjalnych. Naturalnym rozwiązaniem jest ograniczenie liczby alternacji pomiędzy kwantyfikatorami $\forall$ i $\exists$. W ten sposób otrzymujemy hierarchię logiczną pierwszego rzędu:

Definicja 14. *Hierarchią logiczną pierwszego rzędu nazywamy klasy formuł $\Pi_n, \Sigma_n, \Delta_n$ i $Bool(\Sigma_n)$, gdzie*

- Σ_1 *to zbiór formuł FO postaci $\exists x_1 \cdots \exists x_n \phi(x_1, \cdots, x_n)$ gdzie ϕ nie zawiera kwantyfikatorów.*
- Π_1 *to zbiór formuł FO postaci $\forall x_1 \cdots \forall x_n \phi(x_1, \cdots, x_n)$ gdzie ϕ nie zawiera kwantyfikatorów.*
- $\Sigma_n = \{\exists^* \psi \mid \psi \in \Pi_{n-1}\}$, $n > 1$
- $\Pi_n = \{\forall^* \psi \mid \psi \in \Sigma_{n-1}\}$, $n > 1$
- $\Delta_n = \Pi_n \cap \Sigma_n$.
- $Bool(\Sigma_n) = Bool(\Pi_n)$ *to boole'owskie kombinacje formuł z Σ_n.*

Bardzo łatwo można przekonać się, jakie języki należą do Σ_1, zachodzi bowiem następujący fakt:

Fakt 19. *Niech $L \subset A^*$. Zachodzi*

$$L \in \Sigma_1 \iff L \text{ zamknięty na dodawanie liter.} \tag{5.1}$$

Dowód
$\Rightarrow$ Oczywiste.
$\Leftarrow$ Niech L zamknięty na dodawanie liter. Rozpatrzmy częściowy porządek na $A^* \leqslant_p$ zdefiniowany następująco:

$$w \leqslant_p v \iff w \text{ jest podciągiem } v$$

Łatwo sprawdzić, że rzeczywiście jest to częściowy porządek. Podstawową własnością $\leqslant_p$ jest lemat Higmana:

Lemat 20 (Higmana)**.** *Niech $X \subseteq A^*$ antyłańcuch względem $\leqslant_p$. X jest skończony.*

Na mocy lematu Higmana, zbiór $min(L) = \{w \in L | \neg \exists v \in Lv \leq_p w\}$ jest skończony. Oczywiście, $w \in L \iff \exists v \in min(L)\ v \leqslant_p w$. Skoro tak, to $L \in \Sigma_1$ - odpowiednia formuła to:

$$\phi_L = \bigvee_{v \in min(L)} \exists x_1 \cdots \exists x_{|v|} (\bigwedge_{i<j} x_i < x_j) \wedge (\bigwedge_i x_i = v(i))$$

□

Analogicznie, Π_1 to języki zamknięte na usuwanie liter. Łatwo widać, że Δ_1 to języki zamknięte jednocześnie na dodawanie i usuwanie liter. Są tylko 2 takie języki: A^* i $\emptyset$.

Krok wyżej w hierarchii znajduje się $Bool(\Sigma_1)$ czyli boole'owskie kombinacje formuł Σ_1. Oczywiście to ta sama klasa co $Bool(\Pi_1)$. Zachodzi następujące:

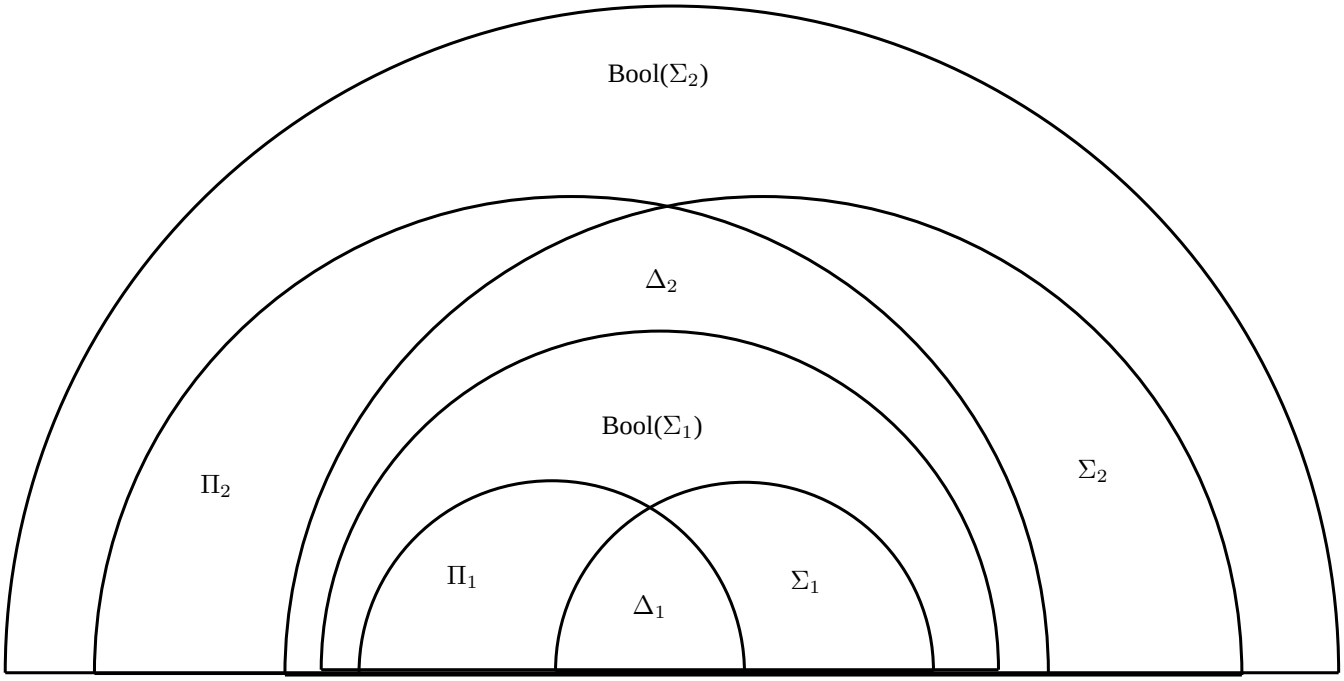
Twierdzenie 21. *Niech $L \subseteq A^*$ język regularny. Następujące warunki są równoważne:*

- *M_L jest $\mathcal{J}$-trywialny.*
- *L jest definiowalny za pomocą formuły $Bool(\Sigma_1)$.*

Twierdzenie to podajemy bez dowodu.

Kolejną klasą w hierarchii jest Δ_2. Okazuje się, że $\Delta_2 = FO_2(<)$, czyli logika pierwszego rzędu z 2 zmiennymi. Do tej pory odkryto algebraiczne charakteryzacje Σ_2 i Π_2, problemem otwartym pozostaje charakteryzacja $Bool(\Sigma_2)$, jak i wszystkich klas znajdujących się wyżej w hierarchii (oczywiście poniżej FO). Okazuje się, że monoidy $\mathcal{L}$-trywialne nie są równoważne żadnej klasie naszej hierarchii. Do ich charakteryzacji trzeba wykorzystać logikę temporalną.

Poniżej diagram obrazujący zawieranie klas logicznych aż do $Bool(\Sigma_2)$:



Rysunek 5.1: Hierarchia logiczna pierwszego rzędu

5.2 Monoidy $\mathcal{L}$-trywialne

Chcemy zcharakteryzować monoidy $\mathcal{L}$-trywialne. W tym celu musimy lepiej zrozumieć, co to znaczy, że monoid jest $\mathcal{L}$-trywialny. Posłuży nam do tego następujący lemat:

Lemat 22. *Skończony monoid M jest $\mathcal{L}$-trywialny $\iff$, $\forall x,y \in M$ zachodzi $(xy)^\omega = y(xy)^\omega$*

Dowód
Dla dowodu $\Rightarrow$ zauważmy, że $(xy)^\omega \sim_{\mathcal{L}} y(xy)^\omega$. Zależność $y(xy)^\omega \leqslant_{\mathcal{L}} (xy)^\omega$ jest oczywista, a ponieważ $xy(xy)^\omega = (xy)^\omega$, to również $(xy)^\omega \leqslant_{\mathcal{L}} y(xy)^\omega$. Skoro $\mathcal{L}$-klasy są trywialne, to $(xy)^\omega \sim_{\mathcal{L}} y(xy)^\omega$ implikuje $(xy)^\omega = y(xy)^\omega$.

Dla dowodu $\Leftarrow$ potrzebny będzie następujący fakt:

Fakt 23. $\forall m,n \in M \quad \exists x,y$

$$\begin{aligned} m \sim_{\mathcal{L}} n \iff & m = (xy)^\omega m \\ & n = y(xy)^\omega m \end{aligned}$$

Dowód (Faktu)
Implikacja w lewo jest oczywista, dla wykazania implikacji w prawo wystarczy zauważyć, że istnieją x,y

$$\begin{aligned} n = ym \quad m = xn \\ m = (xy)m = \cdots = (xy)^\omega m \\ n = ym = y(xy)^\omega m \end{aligned}$$

□

Niech $m \sim_{\mathcal{L}} n$. Z faktu 23 i założenia, wiemy że:

$$m = (xy)^\omega m = y(xy)^\omega m = n$$

□

5.3 Logika LTL(F)

Zdefiniujemy teraz logikę, którą wykorzystamy do charakteryzacji monoidów $\mathcal{L}$-trywialnych. Logika, która nas interesuje to właściwy podzbiór LTL - z operatorów temporalnych można korzystać tylko z F (Finally).

Definicja 15. *Formułą LTL(F) nazywamy każdą formułę zdefiniowaną zgodnie z poniższymi regułami:*

$$\phi ::= a(a \in A) \mid \phi_1 \vee \phi_2 \mid \neg\phi_1 \mid F\phi_1 \tag{5.2}$$

gdzie ϕ_1, ϕ_2 są formułami LTL(F).
Semantyka LTL(F) jest następująca:

- $w \models a$ *gdy* a *jest pierwszą literą* w
- $w \models F\phi$ *gdy istnieje* v *będące* właściwym *sufiksem* w *t. że* $v \models \phi$

Semantyka operacji logicznych jest standardowa.

Na przykład, $abb \not\models Fa$, ale $baa \models Fa$. Zdefiniujmy jeszcze pomocniczy operator $F^*\phi := \phi \vee F\phi$. $w \models F^*\phi$ jeśli istnieje v będące sufiksem w takie, że $v \models \phi$. Ponieważ w LTL(F) nie ma operatora X, operator F^* jest istotnie słabszy od F.

5.4 Logiczna charakteryzacja monoidów $\mathcal{L}$-trywialnych

Niestety, LTL(F) nie do końca odpowiada naszym potrzebom: aby się o tym przekonać wystarczy rozpatrzyć język $L = \{aA^*\}$. $M_L = \{\epsilon, aA^*, bA^*\}$ i $aA^* \sim_{\mathcal{L}} bA^*$, więc M_L nie jest $\mathcal{L}$-trywialny. Okazuje się, że aby uzyskać dokładną charakteryzację monoidów $\mathcal{L}$-trywialnych, trzeba ograniczyć się do boole'owskich kombinacji formuł postaci $F^*\phi$, gdzie ϕ jest formułą LTL(F). Główne twierdzenie tego wykładu jest zatem następujące:

Twierdzenie 24 (Logiczna charakteryzacja monoidów $\mathcal{L}$-trywialnych)**.** *Niech $L \subset A^*$ język regularny. Następujące warunki są równoważne:*

1. *M_L jest $\mathcal{L}$-trywialny.*
2. *L jest definiowalny poprzez boole'owską kombinację formuł postaci $F^*\phi*$, gdzie $\phi \in LTL(F)$.*

Zanim udowodnimy powyższe twierdzenie, potrzebny będzie nam następujący lemat:

Lemat 25. *Niech $\phi \in LTL(F)$.*

$$\exists n \in \mathbb{N}\ \forall x,y,u,v\ \in A^* \quad u(xy)^n v \models F^*\phi \iff uy(xy)^n v \models F^*\phi \tag{5.3}$$

Dowód
$\Rightarrow$
Prosta indukcja po rozmiarze formuły.
$\Leftarrow$
Również indukcja po rozmiarze ϕ. n to właśnie rozmiar formuły. □

Możemy przejść do dowodu głównego twierdzenia.
Dowód (Twierdzenia 24)
$1 \Rightarrow 2$ Działa standardowy logiczny argument.
$1 \Leftarrow 2$ Przyjrzyjmy się warunkowi $\mathcal{L}$-trywialności monoidu M z lematu 23 :

$$\forall x,y\ \in M(xy)^\omega = y(xy)^\omega$$

Równoważnie:

$$\exists n \in \mathbb{N}\ \forall x,y \in M\ (xy)^n = y(xy)^n$$
$$\exists n \in \mathbb{N}\ \forall x,y \in A^*\ (xy)^n \sim_L y(xy)^n$$
$$\exists n \in \mathbb{N}\ \forall u,v,x,y \in A^* u(xy)^n v \in L \iff uy(xy)^n v \in L$$

Skoro tak, to z lematu 25 wynika teza. □

Można też podać algebraiczną charakteryzację LTL(F)

Twierdzenie 26 (algebraiczna charakteryzacja LTL(F))**.** *Niech $L \subset A^*$ język regularny. Następujące warunki są równoważne:*

- *W M_L spełnione jest równanie $z(xy)^\omega = zy(xy)^\omega$, gdzie z jest obrazem słowa niepustego przy α_L*
- *L jest definiowalny poprzez formułę LTL(F).*

Dowód tego twierdzenia pomijamy. Warto zauważyć, że algebraiczny warunek z twierdzenia 26 jest nałożony na monoid syntaktyczny wraz z homomorfizmem. Jest to pierwszy przykład sytuacji w której sam monoid syntaktyczny nie wystarcza do określenia, czy badany język ma pewną własność (w tym wypadku - definiowalność za pomocą LTL(F)).

Możemy teraz uzupełnić diagram klasyfikacji monoidów $\mathcal{H}$, $\mathcal{L}$ i $\mathcal{J}$-trywialnych:

$$\begin{aligned} \mathcal{H}\text{-trywialne} &= FO,\ LTL && (5.4)\\ \cup\!| & \\ \mathcal{L}\text{-trywialne} &= Bool(F^* LTL(F)) && (5.5)\\ \cup\!| & \\ \mathcal{J}\text{-trywialne} &= Bool(\Sigma_1) && (5.6) \end{aligned}$$

Rozdział 6

Wyklad 6

Spisali: Michal Jastrzebski i Bartosz Lewinski

DRAFT
Celem tego wykladu jest pokazanie, ze dla slow nieskonczonych zachodzi nastepujaca rownosc

$$\text{Bool(DBA)} = \text{NBA} \tag{6.1}$$

Gdzie

$$\begin{aligned} \text{DBA} &= \text{Deterministyczny automat z warunkiem Buchiego} \\ \text{NBA} &= \text{Niedeterministyczny automat w warunkiem Buchiego} \end{aligned}$$

Konieczna bedzie nam nastepujaca

Definicja 16. *Automatem z warunkiem Buchiego (dla slow nieskonczonych) nazywamy automat o takiej samej skladni jak klasyczne automaty. Inny jest jedyne warunek akceptacji.*
Powiemy, ze automat akceptuje dane slowo nieskonczone jezeli istnieje taki bieg mu odpowiadajacy w ktorym pewien stan koncowy pojawia sie nieskonczenie wiele razy.

Przejdzmy do glownego twierdzenia wykladu.

Twierdzenie 27. *Dla slow nieskonczonych zachodzi Bool(DBA) = NBA*

Dowód

Pokazmy najpierw prostsze zawieranie: NBA $\supseteq$ Bool(DBA) - majac dana kombinacje boolowska jezykow rozpoznawanych DBA, zasymulujemy jej wykonywanie jednym automatem niedeterministycznym. Pokazemy, jak symulowac kazdy spojnik, co w sumie da nam dowolne wyrazenie:
Oczywiscie pojedynczy automat DBA mozna doskonale symulowac automatem niedeterministycznym.
By zasymulowac dopelnienie jezyka, automat niedeterministyczny zgaduje miejsce, od ktorego nie ma juz stanu akceptujacego. (tzn. od pewnego miejsca przechodzimy do drugiej kopii automatu, w ktorej wyciete sa stany, ktore byly poprzednio akceptujace, a wszystkie pozostale zaznaczamy jako akceptujace)
By zasymulowac alternatywe, wystarczy zgadnac do ktorego skladnika alternatywy nalezy badane slowo.
By zasymulowac koniunkcje, rownolegle idziemy po dwoch automatach, ale akceptujemy naprzemiennie - to znaczy za pierwszym razem akceptujemy dopiero jak pierwszy automat zaakceptuje, potem czekamy az drugi automat zaakceptuje, i tak dalej, naprzemiennie.

Skupimy sie teraz na pokazaniu zaleznosci NBA $\subseteq$ Bool(DBA) - to znaczy w jaki sposob automat niedeterministyczny zasymulowac boolowska kombinacja automatow deterministycznych. Rozwazmy automat NBA o stanach Q. Wezmy dowolne slow nieskonczone w i przyporzadkujmy mu zbior trojek postaci

$$\alpha(w) = \{(p, i, q) | p \in Q, q \in Q, i \in \{0,1\}\}$$

takich, ze istnieje bieg po slowie w od stanu p do stanu q przechodzacy przez stan akceptujacy dla $i = 1$, badz tez nie (dla $i = 0$). W ten sposob otrzymujemy przeksztalcenie

$$\alpha : A^* \to P(\{Q \times \{0,1\} \times Q\})$$

Zauwazmy, ze zbior w ktory prowadzi α jest monoidem (oznaczmy do M). Istotnie, mozemy dla m,$n \subseteq M$ mozemy okreslic dzialanie

$$m \cdot n = \{(p,i,q) \text{ dla ktorych istnieja} (p,j,r) \in m, (r,k,q) \in n, i = max(j,k)\}$$

. Dzialanie to zadaje strukture monoidu z jedynka rowna $\{(p, 0, p)|p \in Q\}$. Nasze α staje sie wowczas homomorfizmem. Wprowadzmy teraz nastepujaca definicje:

Definicja 17. *$\mathcal{J}$-klasa J jest ogonowa $\mathcal{J}$-klasa dla slowa $w \in A^\infty$ jezeli istnieje podzial $w = w_0w_1w_2 \cdots$ t.ze dla kazdych $1 \leqslant i \leqslant j$ zachodzi $\alpha(w_i \cdots w_j) \in J$*

Lemat 28. *Kazde slowo nieskonczone posiada dokladnie jedna $\mathcal{J}$-klase ogonowa.*

Dowód
□

Lemat 29. *Dla kazdej $\mathcal{J}$-klasy J zachodzi $L_J = \{w \in A^\infty | J ogonowe\ dla\ w\} \in Bool(DBA)$.*

Dowód
Wprowadzmy oznaczenie $K_J = \{w \in A^*$ t.ze J wystepuje nieskonczenie czesto $\}$. Wowczas widzimy, ze

$$L_J = K_J \cap \bigcap_{\neg K \leqslant J} \neg K_K$$

. Mamy natomiast $K_J \in DBA$ poniewaz mozemy skonstruowac automat stwierdzajacy czy dana $\mathcal{J}$-klasa wystepuje nieskonczenie czesto. □

Wezmy zatem $w \in A^\infty$ o $\mathcal{J}$ -klasie ogonowej J. Daje to nam rozbicie w jako $m_1m_2m_3 \cdots$ (przy czym jako m_k rozumiemy $m_k = \alpha(w_k)$). Rozwazamy infiksy i zauwazamy, ze

- $\mathcal{L}$-klasa $m_i \cdots m_j$ jest taka sama jak $\mathcal{L}$-klasa m_j
- $\mathcal{R}$-klasa $m_i \cdots m_j$ jest taka sama jak $\mathcal{R}$-klasa m_i

Zatem $\mathcal{H}$-klasa infiksu jest wyznaczona jednoznacznie przez poczatek i koniec. Nastepnie z kazdym miejscem i w naszym podziale mozemy skojarzyc

$$profil(i) = (m_i, m_{i+1}, m_0m_1 \cdots m_i)$$

Pewien profil wystepuje zatem nieskonczenie czesto - oznaczmy go przez (x, y, z). Zauwazmy tez, ze infiksy pomiedzy wystapieniami tego samego profilu naleza do tej samej $\mathcal{H}$-klasy. Udowodnimy teraz nastepujacy:

Lemat 30. *Niech J bedzie $\mathcal{J}$-klasa ogonowa slowa nieskonczonego w. Zalozmy, ze profil (x, y, z) wystepuje nieskonczenie czesto. Wowczas*

- *Niech H bedzie $\mathcal{H}$-klasa do ktorej naleza infiksy pomiedzy wystapieniami profilu. Wowczas H zawiera idempotent e (wynika z tego, ze H jest grupa)*
- *Istenieje podzial slowa $w = v_0v_1v_2 \cdots$ t.ze $\alpha(v_0) = z$ oraz $\alpha(v_i) = e$ dla $i \geqslant 1$*

Dowód
□

Widzimy teraz, zdajac sobie sprawe z istnienia takiego podzialu, ze jezeli dla pewnego $p \in Q, i \in \{0,1\}$ i stanu startowego q_0 mamy $(q_0, i, p) \in z$ oraz $(p, 1, p) \in e$ to akceptujemy slowo w poniewaz generuje to nam bieg akceptujacy. Co wiecej, jest to warunek konieczny.

Wystarczy nam zatem skonstruowac automat sprawdzajacy czy dany profil wystepuje nieskonczenie czesto. Zauwazmy, ze konstrukcje mozemy przeprowadzac przy znanej $\mathcal{J}$-klasie ogonowej J - poniewaz jak wiemy z lematu $L_J \in Bool(DBA)$. Konstrukcje przeprowadzamy odcinajac kolejne przefiksy w, czekajac w odcieciem az prefiks nie bedzie prostszy niz J. Od pewnego momentu nasze przefiksy beda wpadac wciaz do $\mathcal{J}$-klasy J. Konstrukcja taka wyznaczy nam rowniez dekompozycje w.

□