Teoria automatów i języków formalnych
Błędy i uwagi

Kamil Ziemian

21 lipca 2022

Maria Foryś, Wit Foryś
Teoria automatów i języków formalnych, [FF05]

Uwagi

– Zawartość tej książeczki jest pod pewnym względami większa, zaś pod pewnymi względami mniejsza, niż kursu online *Języki, automaty i obliczania*, autorstwa, nota bene, Marii Foryś, Wita Forysia i Adama Romana, warto więc przerabiać go równolegle z tą książeczką. Można go znaleźć pod tym[1] linkiem.

– W tej książce używany jest cudzysłów w formie ”cytowany tekst”, ale polskie standardy typograficzna mówią, że powinno się stosować formę: „cytowany tekst”. Dodatkowo, wyjątek warto uczynić dla ciągów symboli (liter z danego alfabetu A), nazywanych napisami bądź stringami (ang. *strings*), które zgodnie z przyjętą w informatyce konwencją będziemy oznaczać jako `"abc"`.

Więcej o napisach powiemy przy okazji omawiania monoidów wolnych.

Uwagi do konkretnych stron

– **Str. 6.** Według mnie symbol mod_6 wygląda znacznie lepiej, niż używany w tej książce mod_6.

– **Str. 6.** Na tej stronie znajdujemy informację, że element $x \in M$ jest odwracalny w monoidzie M wtedy i tylko wtedy, gdy istnieje takie $y \in M$, że $x \cdot y = 1_M$. Jednak monoid nie musi być przemienny, więc nie widzę powodu, by zachodziła też równość $y \cdot x = 1_M$. Co więcej, wolne monoidy językowe, które zdefiniujemy dalej, a które są dla nas szczególnie interesujące, nie są przemienne, więc problem jest tym poważniejszy.

Wydaje mi, że jest to zwykłe przeoczenie ze strony autorów i trzeba po prostu przyjąć, że element $x \in M$ nazywamy odwracalny, gdy istnieje taki element $y \in M$, że zachodzi

$$x \cdot y = y \cdot x = 1_M. \tag{1}$$

– **Str. 6.** Na tej stronie znajdujemy stwierdzenia, że „zbiór elementów odwracalnych monoidu M stanowi podgrupę tego monoidu”. Zwykle przez podgrupę rozumie się podzbiór G_1 grupy G_0, taki że wraz z działaniem odziedziczonym z G_0 jest grupą. Tutaj jednak jest mowa, że grupa jedynki, oznaczmy ją U (od ang. *unity*), jest podgrupą monoidu, który nie musi być podgrupą.

Sens tego jest dość oczywisty. Mianowicie, że trójka uporządkowana $(U, \cdot, 1)$, gdzie $\cdot$ jest działaniem odziedziczonym po monoidzie M, zaś $1 \in U$, jest elementem neutralnym tego monoidu, jest grupą. Jednak czyni to cały system pojęciowy trochę mniej ścisłym.

Moglibyśmy doprecyzować ten formalizm za pomocą pojęcia algebry ogólnej (zob. [?]), lecz zamiast tego będziemy po prostu mówić, że U jest podzbiorem M i jest grupą. Pod tym ~~kontem~~ dokonamy pewnych poprawek w tekście.
kątem

[1] Pełna forma linku: https://wazniak.mimuw.edu.pl/index.php?title=J%C4%99zyki,_automaty_i_obliczenia.

– **Str. 6.** W dowodzie twierdzenia 1.1.1 brakuje mi zdania typu „Jeśli S nie jest monoidem, to rozszerzamy go do monoidu, za pomocą procedury którą zaprezentujemy poniżej.".

– **Str. 6.** Dowodu twierdzenia 1.1.1 zawiera dodatkową informację, nad którą warto się zatrzymać, mianowicie że każdą półgrupę można rozszerzyć do monoidu. Wymaga to jedynie oczywistego/nieoczywistego[2], czego? że istnieje element $1 \notin S$.

W kontekście samego dowodu twierdzenia 1.1.1, warto się zastanowić nad tym dlaczego dokonujemy rozszerzenia półgrupy $(S, \cdot)$ do monoidu $(S^1, \cdot, 1)$. Dzięki temu mamy rodzinę odwzorowań $\rho_a : S^1 \to S^1$ i ponieważ S^1 jest monoidem, to mamy $\rho_a(1) = a$, ta zaś równość pozwala pokazać, że z $\rho_{a_1} = \rho_{a_2}$ wynika $a_1 = a_2$. Z tego zaś od razu wynika, że odwzorowanie $h : S \to (\{\rho_a\}_{a \in S})$, $h(a) = \rho_a$ jest iniektywne. Poza tym rozszerzenie półgrupy do monoidu nie wydaje się nigdzie indziej potrzebne.

Pytanie, czy istnieje sposób pokazania, że odwzorowanie h jest iniektywne, bez rozszerzania półgrupy S do monoidu S^1? Nawet jeżeli tak, to prostota przeprowadzonego w książce dowodu sprawia, że warto przy nim pozostać.

– **Str. 7.** Tak jak w przypadku symbolu mod_6, wydaje mi się, że lepiej wyglądałby symbol Ker_h.

– **Str. 8.** Rysunki na tej stronie są zrobione dość niechlujnie. Wystarczy zwrócić uwagę, że symbol h leży w różnych odległości od lewego marginesu, podczas, gdy powinien być w tej samej pozycji.

– **Str. 8.** Wedle podanej tu definicji wolny monoid M nad alfabetem A, który będziemy oznaczać również symbolem A^*, jest obiektem o pewnej bardzo konkretnej strukturze ontologicznej. Sprawa ta prowadzi do pewnych niejasności w dalszym wykładzie materiału.

Mianowicie bierzemy pewien zbiór A, którego elementy noszą nazwę „liter" lub „symboli" (patrz uwaga do str. 9) następnie tworzymy zbiór wszystkich ciągów tych symboli, który będziemy oznaczać symbolem A^*.

$$A^* = \{(a_1, a_2, a_3, \ldots, a_n) \ \ : \ \ n \geqslant 0,\ a_i \in A\}. \tag{2}$$

Wedle tej definicji do A^* należy ciąg pusty, oznaczany symbolem $1 \equiv$ "". Taki ciąg intuicyjnie jest prosty do pojęcia, zaś bardziej formalnie jest to odwzorowanie $f : \varnothing \to A$.

W zbiorze A^* wprowadzamy też działanie $\cdot$ wzorem

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_m) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m). \tag{3}$$

W dalszym ciągu książki dowiadujemy się, że klasycznym monoidem wolnym jest $(\mathbb{N}_0, +, 0)$. Powstaje teraz pytanie, czy aby móc powiedzieć, że zbiór liczb naturalnych z 0 jest monoidem wolnym, nie musimy go przedstawić jako zbioru ciągów jakiś symboli, tak jak jest to przedstawione w powyższej definicji? To jednak rodzi pewne problemy.

Zauważmy, że możemy wprawdzie przyjąć[3], że zbiór $A = \{|\}$, liczba 0 to pusty ciąg, $1 = (|)$, $2 = (|, |)$, $3 = (|, |, |)$, etc., jednak podstawowa intuicja matematyczna mówi, że wprowadzanie takiej konstrukcji nie powinno być konieczne. Zanim przejdziemy do dyskusji tego zagadnienia, zauważmy, że w tak podanym wolnym monoidzie A^* konkatenacja ciągów rzeczywiście prowadzi do tego co intuicyjnie rozpoznajemy jako dodawanie liczb naturalnych. Przykładowo

$$1 + 2 = (|) \cdot (|, |) = (|, |, |) = 3. \tag{4}$$

Wróćmy teraz do problemu, czemu takie podejście do liczby naturalnych jawi się intuicji matematycznej jako niekonieczne. Powinno być bowiem możliwe myślenie o liczbach naturalnych jako „po prostu o liczbach", jako autonomicznych bytach, nie zaś jako ciągach jakiegoś symbolu. Dodatkowo, taka definicji to błędne koło, samo bowiem pojęcie ciągu o skończonej długości wymaga uznania, że wiemy czym jest zbiór tw. sp.

[2] Zależy to od przekonań filozoficzno-matematycznych konkretnej osoby.

[3] Nie będziemy tu poruszać niezwykle interesującego i ważnego zagadnienie, tego mianowicie, że w pewnych teoriach typów „obiekty izomorficzne są identyczne" i tym samym, nie ma dwóch różnych „modeli liczb naturalnych" z zerem czy bez. Zawędrowalibyśmy tym sposobem zbyt daleko od właściwego tematu.

liczb $\{1, 2, \dots, n\}$. Skończony ciąg symboli to bowiem nic innego jak odwzorowanie $f : \{1, 2, \dots, n\} \to A$. Z tego powodu potrzebujemy definicji liczb naturalnych, która nie bazuje na pojęciu ciągu, jedną z nich jest ta, która bazuje na użyciu zbioru pustego.

Rozważmy teraz inny przykład. Zbiór wszystkich macierzy kwadratowych wymiaru n, który będziemy oznaczać symbolem $\mathrm{GL}(m)$, możemy rozpatrywać jako monoid $(\mathrm{GL}(m), \cdot, 1)$, gdzie $\cdot$ to mnożenie macierzy, zaś 1 to macierz jednostkowa $m \times m$. Czy jest więc w ogóle sens w zadawaniu pytania ~~się~~, czy ten monoid zawiera jakiś podmonoid wolny, rozumiany jako zbiór ciągów z działaniem konkatenacji? Wszak mając dwie macierze A i B należące do $\mathrm{GL}(m)$ musielibyśmy z jednej strony rozważać ich iloczyn $A \cdot B$, z drugiej ciąg dwuelementowy (A, B) i ustalić relację między tymi dwoma bytami. Nie jest powiedziane, że nie można utożsamić konkretnej macierzy kwadratowej, z ciągiem jakiejś zbioru macierzy, acz taka konstrukcja wydaje się znacznie mniej naturalna, niż przedstawiona powyżej dla liczb naturalnych.

W świetle tego proponuję następujące wyjście z sytuacji. **Wolnym monoidem językowym A^* nad alfabetem A** będziemy nazywać wcześniej określony zbiór ciągów wraz z działaniem konkatenacji. Jest więc to obiekt o konkretnej strukturze ontologicznej. Teraz ustalamy, że monoid $(M, \cdot, 1_M)$ jest monoidem wolnym, jeśli jest izomorficzny z pewnym wolnym monoidem językowym A^* nad alfabetem A. Zbiór A może być podzbiorem M lub nie. Jak pokazują twierdzenia udowodnione na stronach 9–12, jeśli istnieje dowolny zbiór A, taki że M jest izomorficzny z wolnym monoidem językowym A^*, to można znaleźć taki zbiór $B \subset M$, że M jest izomorficzny z wolnym monoidem językowym B^*. Jednak poprawne omówienie tej kwestii wymaga uporządkowania kilku pojęć.

Również z tych twierdzeń wynika wniosek, że jeśli dany monoid $(M, \cdot, 1_M)$ jest monoidem wolnym, to istnieje taki zbiór B, że każdy element $m \in M$, $m \neq 1_M$ można przedstawić w jeden i tylko jeden sposób jako

$$b_1 \cdot b_2 \cdot \ldots \cdot b_n, \quad b_i \in B. \tag{5}$$

Zauważmy, że w powyższym wyrażeniu może zachodzić $b_i = b_j$ dla $i \neq j$. W istocie ta własność jest równoważna przyjętej definicji i tym samym można by ją przyjąć w jej miejsce. Nie zrobiliśmy tego, bo zapisanie tej definicji w sposób precyzyjny „od zera" wymagało tyle miejsca, że nie wygląda na to, byśmy w ten sposób coś zyskiwali.

– **Str. 8.** Korzystając z wprowadzonych wcześniej pojęć, możemy teraz zająć się niejasnościami, jakie wynikają, z użycia w tej książce symbolu A^* w dwóch różnych znaczeniach. Jeżeli bowiem $A \subset M$, gdzie M jest pewnym monoidem, to symbol A^* może oznaczać zarówno wolny monoid językowy nad alfabetem A, jak i podmonoid monoidu M generowany przez A, są to więc dwa różne byty.

Jeśli przyjmiemy, że M to omawiany już wcześniej monoid macierzy kwadratowych $(\mathrm{GL}(m), \cdot, 1)$, zaś $A = \{B_1, B_2, B_3, \dots, B_n\}$, to symbol A^* możne oznaczać zbiór ciągów macierzy kwadratowych, np. (B_1, B_2, B_3), jak i zbiór macierzy kwadratowych utworzonych jako iloczyny macierzowy macierzy ze zbioru A. W tym drugim przypadku do tego zbioru należy choćby macierz $B_1 \cdot B_2 \cdot B_3$.

By usunąć tego typu dwuznaczności przyjmiemy następującą konwencję. Jeżeli jest jawnie powiedziane, że A jest podzbiorem monoidu M, to przez symbol A^* będziemy rozumieli najmniejszy podmonoid M zawierający A. Jeżeli zbiór A jest podany, ale bez wskazania, że jest to podzbiór pewnego monoidu M, to przez symbol A^* będziemy rozumieć wolny monoid językowy nad alfabetem A. W przypadku gdy A jest podzbiorem monoidu M, ale rozważać będziemy wolny monoid językowy nad A, to zostanie to zaznaczone jawnie. Szczególny przypadkiem, acz nietrudnym do zrozumienia jest ten, gdy $A \subset M$ i M jest monoidem językowym. Wówczas obie definicje symbolu A^* się pokrywają.

W świetle powyższych ustaleń wprowadzimy odpowiednie poprawki do tej książeczki.

– **Str. 8.** Dysponując już tak uporządkowanym słownictwem, przeanalizujmy strukturę wolnego monoidu językowego A^* na alfabetem A. Jeśli potrzebny będzie nam przykład wolnego monoidu językowego, sięgniemy po niezwykle ważny w informatyce monoid $\{0, 1\}^*$. Łatwo spostrzec, że jest to monoid nieprzemienny, przykładowo jeśli $u = 00$, $b = 11$, to

$$uv = 0011 \neq 1100 = vu. \tag{6}$$

Nasuwa się naturalne pytanie: co można powiedzieć o zbiorze C taki, m że dla wszystkich $u, v \in C$ zachodzi

$$uv = vu. \tag{7}$$

Problem ten wymaga dalszej analizy.

Zauważmy, że dla monoidu językowego zachodzi równość

$$|uv| = |u| + |v|. \tag{8}$$

Wynika ona w prosty sposób z definicji konkatenacji. Z niej i z tego, że $|u| \geqslant 0, u \in M$, wynika, że grupa jedynki w wolnym monoidzie językowym jest trywialna. Choć wniosek ten jest prosty do zrozumienia, bardziej sformalizowany dowód wymagałby użycia nierówności

$$|uv| \geqslant |u|, \tag{9}$$

które wynika wprost z dwóch wspomnianych własności.

– **Str. 9.** Wedle przyjętej na tej stronie nomenklatury elementy alfabetu będziemy nazywać „literami” i będziemy mówić, że „słowa są ciągami liter”. Jednak ze względu na wygodę, warto przyjąć, że słowo „symbol” jest synonimem słowa „litera”, dzięki czemu będziemy mogli powiedzieć „elementami alfabetu są symbole” i „słowa są ciągami symboli”.

– **Str. 9.** Dowód twierdzenia 1.2.1 byłby znacznie prostszy do zrozumienia, gdyby został wskazane, że jeśli $h : A^* \to M$ jest rozszerzeniem odwzorowania $f : A \to M$ do homomorfizmu musi spełniać następujące trzy warunki

$$h(1) = 1_M, \tag{10a}$$
$$h(a) = f(a), \quad \forall\, a \in A, \tag{10b}$$
$$h(a_1 \ldots a_n) = f(a_1) \cdot \ldots \cdot f(a_n), \quad \forall\, a_i \in A^*. \tag{10c}$$

Dla większej przejrzystości działanie wewnętrzne w monoidzie M zapisaliśmy za pomocą symbolu $\cdot$. Równania te gwarantują nam, że może istnieć co najwyżej jedno odwzorowanie $h : A^* \to M$, dla których są one spełnione.

Możemy teraz użyć równań (10a)-(10c), do *zdefiniowania* homomorfizmu h. Z definicji A^* wynika, że odwzorowanie dane tymi wzorami ma za swoją dziedzinę cały zbiór A^*. Dla każdego $a \in A^*$ zachodzi też $h(a) \in M$ i podobnie można sprawdzić pozostałe warunki na to, by h było homomorfizmem monoidu A^* w monoid M. Ponieważ są to dość proste[4] opuścimy te rozważania.

Błędy Razem z następnym

[4] Jak to niektórzy powiadają „Nie ma czego dowodzić”.

Strona	Wiersz		Jest	Powinno być
	Od góry	Od dołu		
5	11		$\forall x, y, z \in S$	$\forall x, y, z \in S,$
5	15		$\forall x \in M$	$\forall x \in M,$
5		13	$(\mathbf{S}, \cdot)$	$(S, \cdot)$
5		12	$(\mathbf{M}, \cdot, 1_{\mathbf{M}})$	$(M, \cdot, 1_M)$
5		1	$x \in \mathbf{M}$	$x \in M$
5		1	$\exists b \in B\ ,$	$\exists b \in B,$
6	9		$(S, \cdot)\ ,\quad (S', *)$	$(S, \cdot), (S', *)$
6	11		$\forall x, y \in S$	$\forall x, y \in S,$
6	14		$\forall x, y \in M$	$\forall x, y \in M,$
6		14	$x \cdot y = 1$	$x \cdot y = 1_M$
6		13	Podgrupa	Grupa
7		12	$\forall x, y, z \in S$	$\forall x, y, z \in S,$
7		10	$\forall x, y, z \in S$	$\forall x, y, z \in S,$
7		8	$\forall x, y, z \in S$	$\forall x, y, z \in S,$
7		4	S/ρ	$S_{/\rho}$
7		3	M/ρ	$M_{/\rho}$
8		10	$n \geqslant 0\ ,$	$n \geqslant 0,$
8		7	n=0	$n = 0$
9		9	$\to \mathbf{M}$	$\to M$

Str. 6, wiersz 13 (od dołu).
Jest: jest podgrupą M.
Powinno być: jest grupą zawartą, jako zbiór, w M. Grupa ta dziedziczy po M działanie i element neutralny.
Str. 6, wiersz 1 (od dołu).
Jest: *dla* $x \in S^1$ $\rho_a(x) = ax$.
Powinno być: $\rho_a(x) = ax$ *dla* $x \in S^1$.
Str. 8, pierwszy rysunek.
Jest: $S/_{Ker_h}$
Powinno być: $S_{/Ker_h}$
Str. 8, drugi rysunek.
Jest: $A^*/_{Ker_h}$
Powinno być: $M_{/Ker_h}$
Str. 9, wiersz 1.
Jest: wolną półgrupę
Powinno być: wolną półgrupę językową
Str. 9, wiersz 2.
Jest: wolny monoid
Powinno być: wolny monoid językowy
Str. 9, wiersz 2.
Jest: wolna półgrupa
Powinno być: wolna półgrupa językowa
Str. 9, wiersz 3.

Jest: nazywamy
Powinno być: językowego nazywamy
Str. 9, wiersz 4.
Jest: nazywamy
Powinno być: językowego nazywamy
Str. 9, wiersz 6.
Jest: nazywamy
Powinno być: językowego nazywamy
Str. 9, wiersz 6.
Jest: monoid wolny
Powinno być: językowy monoid wolny
Str. 9, wiersz 6.
Jest: półgrupa wolna
Powinno być: językowa półgrupa wolna
Str. 9, wiersz 12.
Jest: wolnych monoidów
Powinno być: wolnych monoidów językowych
Str. 9, wiersz 12.
Jest: wolnych półgrupach
Powinno być: wolnych półgrupach językowych
Str. 9, wiersz 14.
Jest: monoidzie
Powinno być: monoidzie językowym
Str. 9, wiersz 6 (od dołu).
Jest: *monoidu*
Powinno być: *monoidu językowego*
Str. 9, wiersz 25.
Jest: *homomorfizm*
Powinno być: *homomorfizm z wolnego monoidu językowego w dowolny monoid*

Literatura

[FF05] Maria Foryś, Wit Foryś. *Teoria automatów i języków formalnych.* Problemy współczesnej nauki, teoria i zastosowania. Informatyka. Akademicka Oficyna Wydawnicza EXIT, Warszawa, wydanie i, 2005.