POLITECHNIKA GDAŃSKA BIBLIOTEKA GŁÓWNA

ALGORYTMY

P. 2223/69

VOL. VI • No. 11 • 1969

INSTYTUT MASZYN MATEMATYCZNYCH

262 W

P. 2223 | 69

A L G O R Y T M Y

Vol. VI N° 11 1969

Stanisław WALIGÓRSKI

ALGEBRAICZNA TEORIA AUTOMATÓW

Copyright © 1969 - by Instytut Maszyn Matematycznych, Warszawa
Poland
Wszelkie prawa zastrzeżone

K o m i t e t R e d a k c y j n y

Antoni MAZURKIEWICZ /red. nacz./, Krzysztof MOSZYŃSKI /zast. red. nacz./,
Zdzisław PAWLAK, Jan WIERZBOWSKI, Andrzej WIŚNIEWSKI, Ryszard ZIELIŃSKI,
Witold WUDEL /sekr. red./

Adres redakcji: Warszawa, ul. Krzywickiego 34, tel. 28-37-29

PW 169/70

SPIS TREŚCI

Używane oznaczenia 4

WSTĘP 7

1. ALGEBRY, GRUPOIDY, PÓŁGRUPY I STRUKTURY 19

2. ALGEBRA PODZBIORÓW GRUPOIDU 33

3. ALGEBRY ZDARZEŃ 43

4. ZDARZENIA REGULARNE 49

5. AUTOMATY 67

6. NIEODRÓŻNIALNOŚĆ AUTOMATÓW I ICH UPRASZCZANIE 85

7. OBLICZANIE AUTOMATÓW NA PODSTAWIE ICH ZACHOWANIA 105

Literatura 125

Summary 127

Резюме 129

Używane oznaczenia:

$\{a,b,\ldots,c\}$	Zbiór, złożony z elementów a,b,...,c , albo /jeżeli to jest zaznaczone w tekście/ ciąg takich elementów.
$\{a\}$	Zbiór, którego jedynym elementem jest a . Uwaga: poczynając od pewnego miejsca niniejszej pracy, opuszcza się klamry $\{,\}$ i zbiór jednoelementowy jest oznaczany tak samo, jak jego jedyny element.
$\{x : \phi(x)\}$	Zbiór wszystkich takich x, które spełniają warunek $\phi(x)$.
$f: A \to B$	Funkcja f odwzorowuje zbiór A w /lub na/ zbiór B .
$x \in A$	x jest elementem A .
$A \subset B$	A jest podzbiorem B .
$A \cup B$	Suma zbiorów A i B .
$x \cup y$	Także: suma /złącze/ elementów struktury lub półstruktury.
$A \cap B$	Przecięcie /część wspólna/ zbiorów A i B .
$x \cap y$	Także: iloczyn /przecięcie/ elementów struktury lub półstruktury.
$-A$	Uzupełnienie zbioru A .
$-x$	Także: uzupełnienie elementu algebry Boole'a.
$\bigcup_{Z \in H} Z$	Suma wszystkich zbiorów, należących do rodziny H .
$\bigcap_{Z \in H} Z$	Przecięcie wszystkich zbiorów, należących do rodziny H .
0	Zbiór pusty albo liczba zero. Także: najmniejszy element struktury.

$A \times B$	Produkt /iloczyn kartezjański/ zbiorów A i B.
$\sim$ $\equiv$	Równoważność /oznaczenia ogólne/.
$\geqslant$	Quasiporządek /relacja przechodnia i zwrotna/, albo porządek /quasiporządek antysymetryczny/. W szczególności: słaba nierówność liczb.
$>$	Nierówność liczb.
$i + j$	Suma liczb i, j.
Z^*	Jeżeli Z jest zbiorem elementów jakiejś algebry: zbiór wszystkich elementów podalgebry, generowanej przez Z. Inaczej mówiąc: zamknięcie Z ze względu na wszystkie operacje tej algebry. W szczególności, gdy tą algebrą jest wolna półgrupa z jednością: iteracja Z.
$\cdot$	Operacja dwuargumentowa w grupoidzie /oznaczenie ogólne/. W szczególności, gdy mamy do czynienia z wolną półgrupą z jednością: złożenie słów lub zdarzeń /zbiorów słów/. Uwaga: we wzorach często tę kropkę się opuszcza.
$P /\!/ Q$	Iloraz lewostronny P przez Q.
$P \backslash\!\backslash Q$	Iloraz prawostronny P przez Q.
e	Jedność grupoidu lub półgrupy. W szczególności, w przypadku wolnej półgrupy z jednością: słowo puste.
ε	Funkcja określona w grupoidzie lub półgrupie z jednością: Jeżeli A jest jakimkolwiek zbiorem elementów grupoidu, to $\varepsilon(A) = e$, gdy $e \in A$, i $\varepsilon(A) = 0$ w przeciwnym przypadku.

$x_1x_2 \dots x_n$	Słowo złożone z liter $x_1, x_2, \dots, x_n$ /element wolnej półgrupy lub wolnej półgrupy z jednością, generowanej przez zbiór zawierający te litery/. Uwaga: słowo jednoliterowe oznacza się tak samo, jak literę, z której ono jest zbudowane.
$l(s)$	Jeżeli s jest słowem: ilość liter w s, czyli długość tego słowa.
$l(S)$	Jeżeli S jest zdarzeniem /jakimkolwiek zbiorem elementów wolnej półgrupy z jednością/: najmniejsza z długości słów należących do S, albo ∞, gdy S jest pusty.
d_R	Jeżeli R jest zdarzeniem regularnym: ilość jego ilorazów charakterystycznych.
δ	Funkcja przejść lub rozszerzona funkcja przejść automatu.
λ	Funkcja wyjść lub rozszerzona funkcja wyjść automatu.
μ	Ostatnia litera wartości funkcji λ dla tych samych wartości argumentów, albo e, gdy wartością funkcji λ jest e.
T_{pq}	Zbiór słów, przeprowadzających automat ze stanu p do stanu q.
R_{py}	Zbiór słów które podane na automat w stanie p, powodują ukazanie się na jego wyjściu słów, których ostatnią literą jest y.
A_{ij}	Element macierzy $\mathbb{A}$, leżący na przecięciu i- wiersza i j-kolumny.

Instytut Maszyn Matematycznych
Algorytmy N° 11
© 1969.5

ALGEBRAICZNA TEORIA AUTOMATÓW

Stanisław WALIGÓRSKI

Pracę złożono 10 lutego 1969 r.

Praca zawiera podstawowe wiadomości z zakresu teorii automatów w ujęciu algebraicznym, poprzedzone zestawem niezbędnych informacji z algebry ogólnej. Z elementarnych własności grupoidów, algebr ich podzbiorów i operacji dzielenia, określonych w tych algebrach, wyprowadza się twierdzenia, wykorzystane później przy badaniu algebr zdarzeń, /które można traktować jako szczególny przypadek algebr podzbiorów półgrup/. Wprowadza się definicję automatu /maszyny sekwencyjnej w sensie [8], automatu Mealy w sensie [9]/, omawia się różne sposoby jego przedstawienia oraz pokazuje ich związek z poprzednio wprowadzonymi pojęciami algebraicznymi. Ponadto omawia się szczegółowo algebraiczne metody analizy i obliczania automatów.

WSTĘP

Teoria automatów wykrystalizowała się jako odrębna dyscyplina w latach pięćdziesiątych. U jej podstaw legły wyniki badań naukowców różnych dziedzin, przede wszystkim matematyki i elektroniki, a w szczególności takich działów, jak logika, teoria i metody projektowania układów cyfrowych, lingwistyka matematyczna i inne. Ponieważ niektóre z prac, które powstały w tym wczesnym okresie, wywarły istotny wpływ na kształtowanie

się podstaw teorii automatów, warto im poświęcić nieco uwagi.

W roku 1951 ukazała się praca S.C.Kleene Representation of Events in Nerve Sets and Finite Automata, wykonana jako Project RAND Memorandum RM-704. Szerszemu gronu czytelników została ona udostępniona w roku 1956, po opublikowaniu jej w zbiorze Automata Studies [11]. Kleene wprowadza w niej pojęcie zdarzenia i wyrażenia regularnego i pokazuje, jak one mogą być wykorzystane do opisywania zachowania się automatów skończonych. Rozważania swe przeprowadził na przykładzie abstrakcyjnych sieci neuronowych McCullocha-Pittsa /McCulloch W.S., Pitts W.: A Logical Calculus of the Ideas Immanent in Neuron Activity. Bull. of Math. Biophysics, vol. 5, 1943, str. 115-133/. Jednakże uzyskane przez niego wyniki miały charakter ogólny. Copi, Elgot i Wright [5] uprościli wyniki Kleene i zbudowaną przez niego algebrę wyrażeń regularnych, wprowadzając do niej operacje iteracji, konkatenacji i sumowania w takiej formie, w jakiej są one stosowane dotychczas. W tak zmodyfikowanej postaci algebra wyrażeń regularnych jest do obecnej chwili jednym z podstawowych narzędzi teorii automatów. Różnice w przedstawianiu jej przez różnych autorów sprowadzają się do raczej drugorzędnych szczegółów.

Inni badacze oprócz wymienionych wyżej trzech operatorów wprowadzili dwa dodatkowe: przecięcia i uzupełniania, dopełniając tę algebrę do algebry Boole'a z dwoma operacjami dodatkowymi /iteracją i konkatenacją/. Tak jest na przykład w [14] i [3]. Jeszcze inni, jak na przykład [9] pozostają przy tych trzech operatorach. Niektórzy /np. [3],[14]/ jako zbiór generatorów tej algebry przyjmują $\{0, 1\}$ zakładając, że tylko te dwa symbole mogą pojawiać się na wejściach automatów, inni, jak [9], [21], przyjmują, że zbiorem generatorów może być dowolny zbiór niepusty /skończony albo nie/.

W tym samym zbiorze Automata Studies ukazała się praca E.F.Moore'a [17]. Autor podaje w niej formalny sposób opisywania automatów za pomocą tablic i wykresów, definiuje pojęcie "eksperymentu" z automatem i na tej podstawie wprowadza

takie pojęcia, jak izomorfizm automatów, nieodróżnialność stanów i automatów oraz podaje pewne podstawowe własności relacji nieodróżnialności. W tych rozważaniach automat jest traktowany jako "czarna skrzynka" - urządzenie z wejściem i wyjściem, którego budowa nie jest nam znana, ale możemy obserwować jego zewnętrzne zachowanie. W szczególności możemy badać zależności pomiędzy ciągami sygnałów, podawanych na jego wejście, a ciągami sygnałów na wyjściu. Takie potraktowanie automatu pozwala abstrahować od wielu cech szczególnych, które są nieistotne z punktu widzenia ogólnej teorii. Ostatecznie właśnie takie podejście doprowadziło do takiego pojęcia automatu abstrakcyjnego, jakie jest stosowane obecnie.

G.H. Mealy [16], opierając się na wcześniejszych pracach Huffmana /D.A.Huffman: The Synthesis of Sequential Switching Circuits, J. Franklin Inst. vol. 257, 1954, str. 161-190, 275-303. Artykuł ten znajduje się także w [18]/ oraz na wspomnianej pracy Moore'a, znanej mu przed opublikowaniem w [17], podał nieco inny sposób opisywania automatów. Jego praca dotyczy sekwencyjnych układów przełączających, to znaczy takich, że ich działanie zależy nie tylko od stanów wejść w danej chwili, ale także od ich historii, czyli sekwencji stanów wejść w poprzedzającym tę chwilę okresie czasu. Ta zdolność pamiętania jest istotną cechą tych układów, właściwą automatom. Sam sposób opisywania ich, zaproponowany przez Mealy'ego, jest na tyle ogólny, że może być stosowany do dowolnych automatów skończonych.

Różnice w podejściu Moore'a i Mealy'ego do pojęcia automatu i metod jego opisywania spowodowały później wyróżnienie dwu rodzajów automatów: automaty Moore'a, w których stan wyjścia zależy tylko od stanu automatu oraz automaty Mealy'ego, w których stan wyjścia zależy bezpośrednio zarówno od stanu automatu, jak od stanu jego wejścia. Rozróżnienie to jest ważne przede wszystkim z punktu widzenia zastosowań praktycznych, zwłaszcza w teorii układów cyfrowych i ich projektowaniu. Z teoretycznego punktu widzenia ten podział jest mniej

istotny, gdyż każdy automat Moore'a można zastąpić automatem Mealy'ego o takim samym działaniu i odwrotnie. Wobec tego w konkretnych rozważaniach można dobrać taką wersję, która jest akurat bardziej dogodna dla wysłowienia lub obliczeń. Bliższe szczegóły Czytelnik może znaleźć w [9].

Jeszcze inne pojęcie automatu wprowadzili Rabin i Scott w [21]. Praca ta jest poprawioną i zmienioną wersją wcześniejszej pracy, wykonanej pod tym samym tytułem w 1957 r. w IBM Research Center, Lamb Estate, Yorktown Heights, jako raport nr IR-00126. Automat Rabina-Scotta jest uproszczeniem koncepcji Moore'a [17]: zakłada się, że na jego wyjściu mogą się ukazywać tylko dwie wartości: "tak", albo "nie" . Ponieważ stan wyjścia zależy tylko od stanu automatu, na to, aby znać reakcję automatu w określonej sytuacji, wystarczy podać tylko ten podzbiór zbioru stanów, którego wszystkie elementy powodują ukazanie się na wyjściu sygnału "tak". Takie uproszczenie pojęcia automatu jest bardzo dogodne w pewnych rozważaniach teoretycznych, szczególnie w niektórych problemach lingwistyki, gdzie chodzi tylko o badanie, czy automat "akceptuje" podawane na jego wejście sekwencje symboli. W ten sposób automat może być wykorzystany jako narzędzie do sprawdzania, czy podawane na jego wejście słowa, czyli ciągi sygnałów wejściowych należą do jakiegoś danego języka /rozumianego jako ustalony zbiór takich słów/. Ale we wszystkich zagadnieniach, w których automaty traktuje się jako przetworniki informacji, przekształcające w określony sposób sekwencje sygnałów wejściowych w sekwencje sygnałów na wyjściu, automaty Rabina-Scotta są raczej nieużyteczne, bo ilość stanów wyjścia, ograniczona do dwu jest niewystarczająca. Tak samo we wszelkich zastosowaniach do teorii i projektowania układów cyfrowych stosuje się raczej automaty Mealy'ego lub Moore'a bez nałożonych ograniczeń na ilość stanów wyjścia, gdyż w tych przypadkach stosowanie automatów Rabina-Scotta byłoby związane ze zbyt wielkimi niedogodnościami.

Po 1960 roku zaczęły się ukazywać podręczniki i prace przeglądowe, podsumowujące dotychczasowy dorobek w zakresie teorii

automatów. Do takich podręczników i prac należą: monograficzne opracowanie Głuszkowa [9], podręcznik Ginsburga [8] i praca przeglądowa McNaughtona [15]. Od samego początku teoria automatów rozwijała się bardzo szybko, o czym świadczy duża ilość publikowanych prac. O ilości i tematyce prac, napisanych do 1964 roku można się zorientować z bibliografii, umieszczonych w [18] i [15]. Do chwili obecnej ilość ta znacznie się zwiększyła i stale rośnie.

W miarę rozwoju teorii automatów zaczęły wyłaniać się różne szkoły i sposoby podejścia, zależne od indywidualności autorów, ich upodobań, zastosowań, jakie mieli na względzie, lub problemów, jakie chcieli rozwiązać. Między innymi powstała tendencja do algebraizacji tej teorii, wyrażająca się dążeniem do maksymalnego zbliżenia jej metod do metod algebry ogólnej. W myśl tych tendencji wprowadzono takie pojęcia, jak homomorfizm i izomorfizm automatów analogicznie do homomorfizmu i izomorfizmu algebr oraz automaty wolne, będące w pewnym sensie odpowiednikiem algebr wolnych. Niektóre fragmenty teorii automatów miały ten algebraiczny charakter od samego początku - tak było z pojęciem zdarzenia i wyrażenia regularnego. Dla wielu problemów, które początkowo rozwiązywano sposobami dość specyficznymi, nie mającymi swych odpowiedników w algebrze ogólnej, znaleziono metody rozwiązywania, które sprowadzały się do wykonywania operacji algebraicznych. Dość charakterystycznym przykładem tego są dwa ważne problemy teorii automatów: obliczanie automatu na podstawie zadanego zachowania oraz zadanie odwrotne, polegające na tym, że mając dany automat, wyznacza się jego zachowanie. Aby dokładniej pokazać, o co w tych zadaniach chodzi, posłużymy się przykładem.

Przypuśćmy, że mamy do czynienia z szafą pancerną, opatrzoną zamkiem szyfrowym. Otwarcie szafy następuje po wykręceniu ustalonej sekwencji cyfr na umieszczonej na tej szafie tarczy numerowej, takiej, jakie są stosowane w zwykłych aparatach telefonicznych. Nakręcenie sekwencji cyfr, która zostanie przez zamek rozpoznana jako niewłaściwa, powoduje alarm.

Taki zamek szyfrowy można traktować jako automat. Jego wejściem jest tarcza numerowa, a sygnałami wejściowymi nakręcane na niej cyfry. Są trzy możliwe sygnały wyjściowe: otwarcie szafy, alarm i stan spoczynku, gdy szafa jest zamknięta i alarmu nie ma. Nakręcanie cyfr na tarczy jest wprowadzaniem na wejście automatu ciągu /czyli słowa/ zbudowanego z tych cyfr.

Nietrudno zauważyć, że nasz automat klasyfikuje te słowa, gdyż podanie jakiegokolwiek z nich na wejście zawsze powoduje określoną reakcję zamka. Podanie tej klasyfikacji, czyli zbiorów S_o, S_a, S_s, składających się odpowiednio ze słów powodujących otwarcie szafy, alarm lub pozostawienie szafy w stanie spoczynkowym, określa całkowicie i jednoznacznie zachowanie się urządzenia w każdej możliwej sytuacji. Na przykład, jeżeli kombinacją otwierającą jest 256092, to S_o może być zbiorem, zawierającym tylko to jedno słowo. Do zbioru S_s należą słowa 2, 25, 256, 2560, 25609, bo wykręcenie części poprawnej kombinacji nie powoduje alarmu. Do S_a należą wszystkie te słowa, które nie są elementami S_o ani S_s . Zakładamy, że wtedy, gdy szafa jest otwarta, tarcza jest zablokowana i nie można na niej nic wykręcić, a zamknięcie szafy powoduje sprowadzenie zamka do ustalonego stanu początkowego. Aby to wszystko stwierdzić, nie potrzeba znać wewnętrznej budowy zamka. Dla użytkownika te informacje są całkowicie wystarczające, przynajmniej do tego czasu, dopóki urządzenie się nie zepsuje. Gdybyśmy jednak chcieli taki zamek skonstruować, przerobić lub naprawić zepsuty, wtedy informacje o jego strukturze byłyby niezbędne. W szczególności, gdybyśmy musieli skonstruować nowy zamek o zadanym działaniu, nie mając do dyspozycji żadnych wzorów, musielibyśmy się posłużyć odpowiednimi metodami obliczeniowymi teorii automatów - to jest właśnie zadanie syntezy automatu, czyli obliczania automatu na podstawie zadanego zachowania. Odwrotnie, gdybyśmy mieli do czynienia z urządzeniem /takim, które można traktować jako automat/ i znali jego strukturę, ale nie wiedzieli jak działa, musielibyśmy rozwiązać problem analizy automatu, to znaczy wyznaczania jego zachowania na podstawie struktury.

Istnieje wiele metod rozwiązywania zadań analizy i syntezy, a wśród nich są także metody algebraiczne. Wyznaczanie zachowania automatu o zadanej strukturze można sprowadzić do rozwiązywania układów równań w algebrach zdarzeń /[3], [2]/. Obliczanie automatu na podstawie zadanego zachowania metodą Brzozowskiego [3] sprowadza się do wykonywania operacji algebraicznych na wyrażeniach regularnych, opisujących to zachowanie oraz badaniu równości wyników. Podobnie jest z innymi zagadnieniami teorii automatów, choć szczegółowe omawianie tego wykracza poza ramy niniejszej pracy.

Zbliżenie metod teorii automatów do metod algebry ogólnej powoduje jeszcze inny skutek: ułatwia uogólnienia. Automaty, rozumiane tak, jak to jest w większości prac, mogą przyjmować na wejście ciągi sygnałów i reagować na nie w określony sposób. Takie ciągi, czyli słowa, są w każdym przypadku elementami jakiejś wolnej półgrupy, czyli pewnej algebry abstrakcyjnej. Wobec tego nasuwa się pytanie: co by było, gdyby w tej koncepcji zastąpić elementy wolnej półgrupy elementami dowolnej innej algebry, nie koniecznie będącej półgrupą. Otrzymalibyśmy wtedy "automaty", które mogłyby reagować w określony sposób na podawane na ich "wejścia" dowolne elementy wybranej algebry. Takich prób uogólnienia było kilka, wśród nich chyba najdalej idzie w tym kierunku praca [7], która zresztą w istotny sposób wykorzystuje teorię kategorii dla definiowania i badania własności uogólnionych algebr i automatów.

Praca niniejsza zawiera podstawowe wiadomości z teorii automatów w ujęciu algebraicznym. Właściwe wiadomości o automatach zostały poprzedzone obszernymi informacjami o algebrach, grupoidach, półgrupach, strukturach /kratach/ i algebrach Boole'a. Celem tego jest wyprowadzenie w sposób aksjomatyczny i od samych podstaw pojęć, które będą odgrywały zasadniczą rolę w dalszych rozważaniach. Do nich należą półgrupy /w szczególności półgrupy wolne/, algebry zdarzeń, operacje, jakie mogą być wykonywane na zdarzeniach oraz własności tych operacji. Ponieważ we wszystkich rozważaniach tej pracy bardzo

ważną rolę odgrywają działania na zbiorach, takie jak sumy i przecięcia zbiorów /skończone i nieskończone/, uzupełnianie zbiorów, oraz własności tych operacji, podano także powtórzenie podstawowych wiadomości o algebrach Boole'a w ujęciu aksjomatycznym. W zasadzie te informacje pokrywają się z wiadomościami o działaniach na zbiorach podawanych w podręcznikach teorii mnogości lub podstaw matematyki /por. np. [12],[23], [22]/. Ujęcie algebr Boole'a w sposób abstrakcyjny, to znaczy bez zakładania, że ich elementami są zbiory, pomoże Czytelnikowi uświadomić sobie związki pomiędzy tymi algebrami i półgrupami, a poza tym pozwoli później wprowadzić bez dodatkowych wyjaśnień macierze zdarzeń.

Wszystkie twierdzenia, przytoczone w pracy, są formułowane w sposób możliwie najbardziej ogólny, to znaczy przy możliwie najsłabszych założeniach. Oczywiście posunięto to uogólnianie tylko tak daleko, jak to można było zrobić bez utraty elementarności i przejrzystości wywodów. Zasada ta istotnie zadecydowała o układzie całej pracy.

Rozdział 1 zawiera informacje najbardziej ogólne oraz te pojęcia, które można było wprowadzić dla dowolnych algebr: operację zamykania zbioru elementów algebry ze względu na jej wszystkie operacje /oznaczoną * / oraz algebrę podzbiorów danej algebry. To ostatnie pojęcie jest nieco zbliżone do pojęcia algebry relacyjnej, występującego w [7]. Algebry zdarzeń stosowane w teorii automatów są przy tych definicjach szczególnym przypadkiem takich algebr podzbiorów, podobnie jak iteracja w algebrze zdarzeń jest szczególnym przypadkiem tak wprowadzonej operacji * .

Zgodnie z wspomnianą zasadą operacje dzielenia lewo- i prawostronnego, które odgrywają dużą rolę przy obliczaniu automatów /metoda Brzozowskiego/, zostały zdefiniowane możliwie najogólniej, jako operacje w algebrach podzbiorów dowolnych grupoidów. W rozdziale 2 , traktującym o takich algebrach, poświęca się tym operacjom bardzo dużo miejsca. Podaje się tam własności, które one spełniają w dowolnych grupoidach,

a następnie te własności, które one mają tylko w grupoidach z jednością, półgrupach i półgrupach z jednością. Duża część rozdziału 2 jest oparta na wynikach, przedstawionych w [6]. W książce tej rozważa się półstruktury i struktury z dodatkową operacją dwuargumentową, łączną. Algebry podzbiorów grupoidów są szczególnym przypadkiem takich struktur. Ponieważ stosowanie tak ogólnych pojęć, jak to miało miejsce w [6], nie było tu potrzebne i mogło skomplikować wywody, wszystkie wzory i twierdzenia zostały sformułowane dla algebr podzbiorów grupoidów. Niektóre wzory, twierdzenia i ich dowody zostały przeniesione z [6] tylko z tą zmianą, niektóre zostały przerobione stosownie do potrzeb niniejszej pracy, inne wreszcie zostały sformułowane i udowodnione przez autora. Twierdzenie 2.1. o przenoszeniu własności operacji z grupoidu do jego algebry podzbiorów wywodzi się z ogólniejszej idei Eilenberga /o której wspomniał w swoim odczycie w Warszawie w 1967 r./.

W rozdziale 3 zostały podane pewne ogólne informacje o algebrach zdarzeń oraz te własności operacji dzielenia, które są spełnione tylko w tych algebrach: reguły dzielenia złożenia /konkatenacji/ dwu zdarzeń oraz iteracji zdarzenia przez literę. Wprowadzenie tych wzorów podał Brzozowski w [3]. Twierdzenie o rozwiązaniach równania z jedną niewiadomą i jego dowód są wzięte z [2].

Warto zauważyć, że Brzozowski w swej pracy stosował inne oznaczenie dla ilorazu lewostronnego, nazywając go pochodną /derivative/. Nazwa ta występuje nawet w tytule pracy. Jednak pochodna w sensie [3] jest szczególnym przypadkiem operacji zwanej po angielsku left residual i po francusku residuel à gauche, omawianej w [1], [6] i [26]. Tłumaczeniem tych nazw na polski jest właśnie termin "iloraz lewostronny", podobnie jak termin "iloraz prawostronny" jest tłumaczeniem right residual i residuel à droite.

Najważniejsze twierdzenia z [3], dotyczące regularności zostały przytoczone w rozdziale 4 z powyższą zmianą terminologiczną i pewnymi zmianami natury redakcyjnej, jako twierdze-

nia 4.1, 4.3 i 4.5. Metoda redukowania układów równań jest opracowana przez autora. Ostatnie twierdzenie tego rozdziału, 4.6 zawiera wyniki Myhill'a i Nerode'a, cytowane w [21], ale wyprowadzenie ich jest inne, gdyż korzysta się w nim z lewo- i prawostronnego dzielenia.

Definicja automatu, podana w tej pracy, pokrywa się z definicją maszyny sekwencyjnej Ginsburga [8] oraz z definicją automatu Mealy'ego, podaną przez Głuszkowa [9]. Aby niepotrzebnie nie rozbudowywać niniejszej pracy i nie rozpraszać uwagi Czytelnika, nie wprowadza się żadnych innych rodzajów automatów poza tym jednym, przyjmując, że dla wyłożenia elementów teorii to zupełnie wystarczy. O wyborze tego właśnie typu automatu zadecydowało to, że po pierwsze, automat Moore'a można uważać za szczególny przypadek automatu Mealy'ego, a po drugie, że zapis automatu Mealy'ego jest bardziej zwarty i oszczędny, gdyż przejście od skończonego automatu Mealy'ego do działającego tak samo automatu Moore'a jest na ogół związane z poważnym zwiększeniem ilości stanów automatu, ale nigdy ze zmniejszeniem /zob. [9]/. Czytelnik, który by się bardziej interesował automatami Moore'a, może skorzystać z prac [9], [3] oraz [17]. Wszystkie zawarte tam informacje dotyczą także automatów Rabina-Scotta, jako szczególnego przypadku automatów Moore'a. Poza tym Czytelnik, interesujący się automatami Rabina-Scotta ma jeszcze do dyspozycji [21] /lub [18]/.

Treść rozdziałów 5, 6 i 7 jest częściowo oparta na wynikach przedstawionych w [9] oraz, w mniejszym stopniu, na [3] i [25]. W szczególności z [9] pochodzi pojęcie homomorfizmu automatów i związki tego pojęcia z nieodróżnialnością, pojęcie funkcji sekwencyjnej, idea rozszerzenia automatu w ten sposób, żeby jego funkcja przejść była konkatenacją słów /odpowiednik automatu wolnego/, własności funkcji sekwencyjnych, konstruowanie automatu na podstawie zadanych funkcji sekwencyjnych, sprowadzanie dowolnej funkcji przekształcającej słowa na słowa do funkcji sekwencyjnej metodą wyrównywania długości słów oraz funkcja μ jako rozszerzenie funkcji wyjść, a także zbiory R_{py}

/zdarzenia opisujące zachowanie automatu/ i ich własności.

Z [3] pochodzi idea konstruowania automatu, którego stanami są zdarzenia lub ciągi zdarzeń /dokładniej: ich klasy abstrakcji/. Twierdzenie 7.6 jest nieznaczną modyfikacją twierdzenia z [3] o syntezie automatów Mealy'ego, lecz w odróżnieniu od [3] nie zakłada się, że obliczany automat ma stan początkowy. Ze względu na to, że ciągi wyrażeń regularnych /opisujących zdarzenia/ są najwygodniejszym sposobem opisywania zachowania automatów, podana w tym twierdzeniu metoda projektowania /zwana wyżej metodą Brzozowskiego/ ma dość duże znaczenie praktyczne. Metoda upraszczania automatów, opisana na końcu rozdziału 6 , jest uproszczonym wariantem metody upraszczania automatów częściowo określonych, podanej w [20] i [25].

Praca niniejsza jest przeznaczona przede wszystkim dla osób, które mają /lub mogą mieć/ coś do czynienia z teorią automatów i interesują się jej podstawami ujętymi w sposób sformalizowany. Do pełnego jej zrozumienia potrzebna jest znajomość podstaw teorii mnogości, w szczególności działań na zbiorach i ich własności, oraz umiejętność dość swobodnego operowania takimi pojęciami z tego zakresu, jak funkcja, relacja, równoważność itp. Dla ewentualnego uzupełnienia tych wiadomości można polecić [23] lub dowolny inny podręcznik o podobnym zakresie.

Materiał zaprezentowany w pracy niniejszej wchodził w zakres wykładów wygłaszanych przez autora na Wydziale Matematycznym Uniwersytetu Warszawskiego. Wydaje się jednak, że jej treść może być interesująca nie tylko dla matematyków, ale również dla szerszego grona osób związanych z maszynami cyfrowymi lub innymi dziedzinami, które wykorzystują teorię automatów.

Chciałbym wreszcie w tym miejscu podziękować Panom doc. dr A.W. Mostowskiemu i doc. dr Z. Pawlakowi za przejrzenie tej pracy i ich cenne uwagi.

1. ALGEBRY, GRUPOIDY, PÓŁGRUPY I STRUKTURY

Algebrą będziemy nazywać każdy ciąg postaci

$$\{A, o_1, \dots, o_s\}$$

złożony z niepustego zbioru A i skończonej ilości operacji /0 lub więcej argumentowych/, takich, że jeżeli ilość argumentów m_j operacji o_j jest dodatnia, to dla każdego ciągu $x_1, \dots, x_{m_j}$ elementów A $o_j(x_1, \dots, x_{m_j}) \in A$, a jeżeli $m_j = 0$, to o_j jest ustalonym elementem A.

Elementy zbioru A będziemy nazywać krótko elementami rozważanej algebry. Algebra jest skończona, o ile zbiór wszystkich jej elementów jest skończony.

Podalgebrą algebry $\{A, o_1, \dots, o_s\}$ będziemy nazywać każdy ciąg $\{A', o_1, \dots, o_s\}$ taki, że $A' \subset A$ i dla każdej operacji tej algebry o_j, jeśli $m_j = 0$, to $o_j \in A'$, a gdy $m_j > 0$, to dla każdego ciągu $x_1, \dots, x_{m_j}$ elementów A' $o_j(x_1, \dots, x_{m_j}) \in A'$.

Przecięciem dowolnego zbioru podalgebr algebry $\{A, o_1, \dots, o_s\}$ będziemy nazywać ciąg $\{B, o_1, \dots, o_s\}$, w którym B jest przecięciem zbiorów elementów wszystkich tych podalgebr.

Każde przecięcie podalgebr algebry $\{A, o_1, \dots, o_s\}$ jest jej podalgebrą. Stąd wynika, że dla dowolnego zbioru $Z \subset A$ istnieje najmniejsza podalgebra algebry $\{A, o_1, \dots, o_s\}$, zawierająca Z w zbiorze swoich elementów; będziemy ją nazywać podalgebrą generowaną przez Z, zaś Z będziemy nazywać zbiorem generatorów tej podalgebry. Zbiór wszystkich elementów podalgebry generowanej przez Z będziemy oznaczać Z^*. Jeżeli $Z^* = A$, czyli podalgebra generowana przez Z jest identyczna z algebrą $\{A, o_1, \dots, o_s\}$, to mówimy, że al-

gebra ta jest generowana przez Z, który jest wtedy zbiorem jej generatorów.

Podalgebra algebry $\{A, o_1, \ldots, o_s\}$ generowana przez zbiór pusty 0, jest przecięciem wszystkich jej podalgebr. $\{0^*, o_1, \ldots, o_s\}$ jest więc najmniejszą podalgebrą $\{A, o_1, \ldots, o_s\}$ i wszystkie zero-argumentowe operacje tej algebry /jeżeli istnieją/ należą do 0^*.

Algebry

$$\{A, o_1, \ldots, o_s\},$$
$$\{B, o_1', \ldots, o_s'\}$$

nazywamy podobnymi, o ile dla każdego j operacje o_j i o_j' mają te same ilości argumentów. Odpowiadające sobie operacje w algebrach podobnych możemy oznaczać tymi samymi symbolami.

Odwzorowanie h zbioru elementów algebry $\{A, o_1, \ldots, o_s\}$ w zbiór elementów podobnej algebry $\{B, o_1, \ldots, o_s\}$ nazywamy homomorfizmem, o ile zachowuje ono wszystkie operacje, tzn. dla każdego j, jeżeli $m_j > 0$, to dla dowolnego ciągu $x_1, \ldots, x_{m_j}$ elementów zbioru A jest

$$h\left(o_j\ (x_1, \ldots, x_{m_j})\right) = o_j\left(h(x_1), \ldots, h(x_{m_j})\right),$$

a jeśli $m_j = 0$, to

$$h\left(o_j\right) = o_j .$$

Jeżeli homomorfizm jest wzajemnie jednoznaczny, nazywamy go izomorfizmem.

Niech $\mathcal{K}$ będzie jakąś klasą algebr podobnych. Mówimy, że algebra $\{A, o_1, \ldots, o_s\} \in \mathcal{K}$ jest wolna w klasie $\mathcal{K}$, o ile istnieje zbiór $Z \subset A$ generujący tę algebrę i każde odwzorowanie $f: Z \to B$, gdzie $\{B, o_1, \ldots, o_s\}$ jest dowolną algebrą należącą do $\mathcal{K}$, może być rozszerzone do homomorfizmu $h: A \to B$. Z nazywamy wtedy zbiorem $\mathcal{K}$-wolnych generatorów algebry $\{A, o_1, \ldots, o_s\}$.

Relacja równoważności $\sim$, określona na zbiorze A elementów dowolnej algebry $\{A, o_1, \dots, o_s\}$ jest kongruencją, jeżeli dla dowolnej operacji o_j o dodatniej ilości argumentów m_j i dla dowolnych $x_1, y_1, \dots, x_{m_j}, y_{m_j}$, należących do A, z

$$x_1 \sim y_1, \dots, x_{m_j} \sim y_{m_j}$$

wynika

$$o_j(x_1, \dots, x_{m_j}) \sim o_j(y_1, \dots, y_{m_j}) .$$

Grupoid jest to algebra z jedną operacją dwuargumentową.

Element e grupoidu $\{A, .\}$ taki, że dla każdego $x \in A$ jest

$$e \cdot x = x ,$$

nazywamy jednością lewostronną. Analogicznie, jedność prawostronna jest to $i \in A$ taki, że dla każdego $x \in A$

$$x \cdot i = x .$$

Element grupoidu, będący jednością lewostronną i prawostronną nazywamy jednością tego grupoidu.

Jeżeli grupoid zawiera jedność lewostronną e i prawostronną i, to są one równe, bo

$$e = e \cdot i = i .$$

Stąd każdy grupoid może mieć co najwyżej jedną jedność.

Jedność e grupoidu nazywamy nierozkładalną, o ile dla dowolnych x, y $x \cdot y = e$ wtedy i tylko wtedy, gdy $x=y=e$.

Zerem lewostronnym grupoidu $\{A, \cdot\}$ nazywamy taki $q \in A$, że dla każdego $x \in A$ jest

$$q \cdot x = q .$$

Zerem prawostronnym jest taki $p \in A$, że dla każdego $x \in A$

$$x \cdot p = p .$$

Element będący jednocześnie zerem prawostronnym i lewostronnym, nazywamy krótko zerem. Każdy grupoid może mieć co

najwyżej jedno zero, bo jeżeli zawiera zero lewostronne q i prawostronne p, to one są równe

$$p = q \cdot p = q .$$

$\{A, \cdot\}$ jest grupoidem ze skracaniem lewostronnym, gdy dla dowolnych $x \in A$, $y \in A$, $z \in A$ jest spełniona implikacja

$$\text{jeśli } x \cdot y = x \cdot z \text{ , to } y = z .$$

$\{A, \cdot\}$ jest grupoidem ze skracaniem prawostronnym, o ile dla dowolnych $x \in A$, $y \in A$, $z \in A$ jest

$$\text{jeśli } x \cdot z = y \cdot z \text{ , to } x = y .$$

Grupoid $\{A, \cdot\}$, którego operacja jest łączna: dla dowolnych $x \in A$, $y \in A$, $z \in A$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad 1.1$$

nazywamy półgrupą.

Półgrupę nazywamy przemienną, jeżeli jej operacja jest łączna i oprócz tego przemienna: dla dowolnych $x \in A$, $y \in A$ jest

$$x \cdot y = y \cdot x . \qquad 1.2$$

Półstruktura /zwana także półkratą/ jest to półgrupa przemienna $\{A, \cdot\}$, w której operacja $\cdot$ jest idempotentna: dla każdego $x \in A$

$$x \cdot x = x . \qquad 1.3$$

Struktura /krata/ jest to algebra $\{A, \cup, \cap\}$ z dwoma operacjami dwuargumentowymi, z których każda jest łączna, przemienna i idempotentna, tzn dla dowolnych $x \in A$, $y \in A$, $z \in A$

$$x \cup (y \cup z) = (x \cup y) \cup z , \qquad 1.4$$

$$x \cap (y \cap z) = (x \cap y) \cap z , \qquad 1.5$$

$$x \cup y = y \cup x , \qquad 1.6$$

$$x \cap y = y \cap x , \qquad 1.7$$

$$x \cup x = x \quad , \qquad 1.8$$
$$x \cap x = x \quad , \qquad 1.9$$

a ponadto są w niej spełnione prawa pochłaniania: dla dowolnych $x \in A$, $y \in A$

$$x \cup (y \cap x) = x \quad , \qquad 1.10$$
$$x \cap (y \cup x) = x \quad . \qquad 1.11$$

Element $x \cup y$ nazywa się sumą lub złączem, a $x \cap y$ przecięciem lub iloczynem elementów x i y.

Z praw pochłaniania bezpośrednio wynika równoważność

$$x \cup y = x \text{ wtedy i tylko wtedy, gdy } y \cap x = y \quad . \qquad 1.12$$

Rzeczywiście, jeżeli $x \cup y = x$, to $y \cap x = y \cap (x \cup y) = y$, a jeżeli $y \cap x = y$, to $x \cup y = x \cup (y \cap x) = x$.

Pojęcie półstruktury i struktury można również wprowadzić w inny sposób.

Relacja $\leqslant$, określona na niepustym zbiorze P, jest quasiporządkiem, o ile jest przechodnia i zwrotna, tzn. dla dowolnych $x \in P$, $y \in P$, $z \in P$ jest

$$\text{jeżeli } x \leqslant y \text{ i } y \leqslant z \text{ , to } x \leqslant z \text{ ,} \qquad 1.13$$
$$x \leqslant x \quad . \qquad 1.14$$

Jeżeli quasiporządek jest symetryczny, tzn. dla dowolnych $x \in P$, $y \in P$

$$\text{jeśli } x \leqslant y \text{ , to } y \leqslant x \text{ ,}$$

to jest oczywiście równoważnością. Jeżeli natomiast ten quasiporządek jest słabo antysymetryczny: dla dowolnych $x \in P$, $y \in P$

$$\text{jeśli } x \leqslant y \text{ i } y \leqslant x \text{ , to } x = y \text{ ,} \qquad 1.15$$

to jest to porządek /częściowy/. Zbiór, na którym jest określony porządek, nazywamy zbiorem uporządkowanym /częściowo/.

Elementem minimalnym dowolnego zbioru /częściowo/ uporządkowanego P nazywamy każdy taki $x \in P$, że dla dowolnego $y \in P$ z $y \leqslant x$ wynika $x \leqslant y$. Najmniejszym elementem do-

wolnego zbioru uporządkowanego P nazywamy taki $a \in P$, że dla każdego $y \in P$ jest $a \leqslant y$. Analogicznie określamy element maksymalny i największy; elementem maksymalnym zbioru P jest każdy taki $x \in P$, że dla każdego $y \in P$ z $y \geqslant x$ wynika $x \geqslant y$, zaś największym elementem P jest taki $a \in P$, że dla każdego $y \in P$ jest $a \geqslant y$.

Jeżeli P jest zbiorem uporządkowanym i $X \subset P$, to ograniczeniem dolnym /w zbiorze P/ zbioru X nazywamy taki $a \in P$, że $a \leqslant x$ dla wszystkich $x \in X$. Kresem dolnym zbioru X nazywamy największe jego ograniczenie dolne. Ograniczeniem górnym /w zbiorze P/ zbioru X nazywamy taki $b \in P$, że $b \geqslant x$ dla wszystkich $x \in X$. Kresem górnym zbioru X nazywamy najmniejsze jego ograniczenie górne.

<u>Twierdzenie 1.1.</u> W dowolnej półstrukturze $\{A, \cap\}$ relacja $\leqslant$ określona w następujący sposób: $x \leqslant y$ wtedy i tylko wtedy, gdy $x = x \cap y$, jest porządkiem i $x \cap y$ jest w tym porządku kresem dolnym zbioru złożonego z elementów x i y.

Odwrotnie, jeżeli w uporządkowanym zbiorze P każdy zbiór, złożony z dwu elementów x, y posiada kres dolny $x \cap y$, to $\{P, \cap\}$ jest półstrukturą.

Dowód:

Przypuśćmy, że $\{A, \cap\}$ jest półstrukturą i relacja $\leqslant$ jest określona w sposób podany wyżej. Jeżeli $x \leqslant y$ i $y \leqslant z$, to $x = x \cap y$ oraz $y = y \cap z$, a stąd
$x = x \cap y = x \cap (y \cap z) = (x \cap y) \cap z = x \cap z$, czyli $x \leqslant z$.
Z $x = x \cap x$ wynika $x \leqslant x$. Jeżeli $x \leqslant y$ i $x \geqslant y$, to
$x = x \cap y = y \cap x = y$.

Niech c będzie dowolnym ograniczeniem dolnym zbioru złożonego z x i y; $c \leqslant x$ i $c \leqslant y$, czyli $c = c \cap x$ oraz $c = c \cap y$. Wtedy $c \cap (x \cap y) = (c \cap x) \cap y = c \cap y = c$, a więc $c \leqslant x \cap y$. Ale $x \cap y$ jest też ograniczeniem dolnym tego zbioru, bo $(x \cap y) \cap y = x \cap (y \cap y) = x \cap y$ oraz $(x \cap y) \cap x = (y \cap x) \cap x = y \cap (x \cap x) = y \cap x = x \cap y$, a stąd $x \cap y \leqslant x$, $x \cap y \leqslant y$, a więc $x \cap y$ jest kresem dolnym.

Odwrotnie, przypuśćmy, że P jest zbiorem uporządkowanym i że $x \cap y$ jest kresem dolnym zbioru złożonego z elementów x, y /lub z jednego elementu x=y/. Ponieważ kres dolny zbioru nie zależy od tego, w jakiej kolejności weźmiemy jego elementy, $x \cap y = y \cap x$. Kresem dolnym zbioru jednoelementowego jest jego jedyny element, a więc $x \cap x = x$. Z określenia kresu dolnego wynika, że $x \cap (y \cap z) \leqslant x$ i $x \cap (y \cap z) \leqslant y \cap z$, a więc także $x \cap (y \cap z) \leqslant y$ i $x \cap (y \cap z) \leqslant z$. Stąd $x \cap (y \cap z) \leqslant x \cap y$ i $x \cap (y \cap z) \leqslant (x \cap y) \cap z$. W podobny sposób wyprowadzamy nierówność odwrotną i wobec tego otrzymujemy $x \cap (y \cap z) = (x \cap y) \cap z$.

Koniec dowodu.

Twierdzenie pozostanie prawdziwe, jeżeli zastąpimy w nim znaki " $\leqslant$ ", " $\cap$ " odpowiednio przez " $\geqslant$ ", " $\cup$ " i słowa "kres dolny" przez "kres górny".

Uogólnieniem tych twierdzeń dla struktur jest

<u>Twierdzenie 1.2</u> W dowolnej strukturze $\{A, \cup, \cap\}$ relacja $\leqslant$ określona w następujący sposób: $x \leqslant y$ wtedy i tylko wtedy, gdy $y = y \cup x$ /lub, co jest równoważne, wtedy i tylko wtedy, gdy $x = x \cap y$/ jest porządkiem, w którym $x \cup y$ jest kresem górnym, a $x \cap y$ jest kresem dolnym zbioru, złożonego z elementów x i y.

Odwrotnie, jeżeli w zbiorze /częściowo/ uporządkowanym P każdy zbiór złożony z dwu elementów x, y posiada kres dolny $x \cap y$ i kres górny $x \cup y$, to $\{P, \cup, \cap\}$ jest strukturą.

Dowód:

W swej większej części twierdzenie to jest bezpośrednią konsekwencją poprzedniego twierdzenia. Pozostaje tylko udowodnić prawa pochłaniania dla algebry $\{P, \cup, \cap\}$.

Z definicji kresów wynika, że jeśli $a \leqslant b$, to $a \cap b = a$ oraz $a \cup b = b$, a także $y \cup x \geqslant x$ i $y \cap x \leqslant x$. Stąd $x \cap (y \cup x) = x$ i $x \cup (y \cap x) = x$.

Koniec dowodu.

Niżej, mówiąc o strukturach, będziemy zawsze zakładać, że związki pomiędzy porządkiem $\leqslant$ a operacjami $\cup$ i $\cap$ są takie, jak w tym twierdzeniu.

W każdej strukturze zachodzą prawa semirozdzielności: dla dowolnych x,y,z

$$x\cap(y\cup z)\geqslant(x\cap y)\cup(x\cap z)\ ,$$
$$x\cup(y\cap z)\leqslant(x\cup y)\cap(x\cup z)\ .$$

Rzeczywiście, $x\cap y\leqslant x$ i $x\cap z\leqslant x$, a więc $(x\cap y)\cup(x\cap z)\leqslant x$. Dalej, $x\cap y\leqslant y\leqslant y\cup z$ i $x\cap z\leqslant z\leqslant y\cup z$, a więc $(x\cap y)\cup(x\cap z)\leqslant y\cup z$. Stąd $(x\cap y)\cup(x\cap z)\leqslant x\cap(y\cup z)$. Dowód drugiej nierówności jest analogiczny - wystarczy zastąpić "$\cap$" "$\cup$", "$\leqslant$" odpowiednio przez "$\cup$", "$\cap$", "$\geqslant$".

Strukturę, w której zachodzą prawa rozdzielności: dla dowolnych x, y, z

$$x\cap(y\cup z)=(x\cap y)\cup(x\cap z)\ , \qquad 1.16$$
$$x\cup(y\cap z)=(x\cup y)\cap(x\cup z) \qquad 1.17$$

nazywamy strukturą rozdzielną /dystrybutywną/.

Jeżeli zachodzi jedno z tych praw, to zachodzi również drugie: np. jeżeli pierwsze prawo jest spełnione, to $(x\cup y)\cap(x\cup z)=((x\cup y)\cap x)\cup((x\cup y)\cap z)=x\cup((x\cap z)\cup(y\cap z))=$ $=(x\cup(x\cap z))\cup(y\cap z)=x\cup(y\cap z)$; podobnie można udowodnić implikację w drugą stronę.

Największy element struktury /o ile istnieje/ będziemy oznaczać I, najmniejszy element 0. Jeżeli struktura zawiera I i 0, to dla każdego jej elementu x jest $0\leqslant x\leqslant I$, a więc

$$0\cap x=0\ , \qquad 1.18$$
$$0\cup x=x\ , \qquad 1.19$$
$$I\cap x=x\ , \qquad 1.20$$
$$I\cup x=I\ . \qquad 1.21$$

Jeżeli x jest elementem struktury zawierającej 0 i I i istnieje jedyny element y taki, że jednocześnie

$$x\cap y=0\ , \qquad 1.22$$
$$x\cup y=I\ , \qquad 1.23$$

to y nazywamy uzupełnieniem elementu x. Oznaczając to uzupełnienie przez $-x$ możemy te równości przepisać w formie

$$x \cap -x = 0 , \qquad 1.24$$

$$x \cup -x = I \qquad 1.25$$

/zakładamy, że $-$ wiąże mocniej niż inne operacje/.
Elementy 0 i I mają zawsze uzupełnienia:

$$-0 = I , \qquad 1.26$$

$$-I = 0 . \qquad 1.27$$

<u>Twierdzenie 1.3.</u> Jeżeli struktura jest rozdzielna, to

1. dla każdego x istnieje co najwyżej jeden taki y, że

$$x \cap y = 0 ,$$
$$x \cup y = I ,$$

2. jeżeli istnieje $-x$, to istnieje $--x$ oraz

$$--x = x ,$$

3. jeżeli istnieją $-x$ i $-y$, to istnieją również $-(x \cup y)$, $-(x \cap y)$ oraz

$$-(x \cup y) = -x \cap -y ,$$
$$-(x \cap y) = -x \cup -y ,$$

a ponadto

$$x \leqslant y \text{ wtedy i tylko wtedy, gdy } -y \leqslant -x ,$$
$$x \leqslant y \text{ wtedy i tylko wtedy, gdy } x \cap -y = 0 .$$

Dowód:

1.: Przypuśćmy, że $x \cap y = 0$, $x \cap z = 0$, $x \cup y = I$, $x \cup z = I$. Wtedy $y = I \cap y = (x \cup z) \cap y = (x \cap y) \cup (z \cap y) = 0 \cup (z \cap y) = (x \cap z) \cup (y \cap z) = (x \cup y) \cap z = I \cap z = z$ a więc $y = z = -x$. Stąd także bezpośrednio wynika 2.

3.: Jeżeli $-x$ i $-y$ istnieją, to $(x \cup y) \cap (-x \cap -y) = (x \cap (-x \cap -y)) \cup (y \cap (-x \cap -y)) = ((x \cap -x) \cap -y) \cup ((y \cap -y) \cap -x) = 0 \cup 0 = 0$.
$(x \cup y) \cup (-x \cap -y) = ((x \cup y) \cup -x) \cap ((x \cup y) \cup -y) = I \cap I = I$.
Stąd wobec 1. $-(x \cup y)$ istnieje i jest równe $-x \cap -y$.
Drugą równość p. 3 możemy udowodnić analogicznie. Dalej, nas-

tępujące zależności są równoważne /i wszystkie występujące w nich uzupełnienia istnieją/: $x \leqslant y$, $x \cup y = y$, $-(x \cup y) = -y$, $-x \cap -y = -y$, $-x \geqslant -y$. Jeśli $x \leqslant y$, to $x \cap -y = (x \cap y) \cap -y = x \cap (y \cap -y) = x \cap 0 = 0$, a jeżeli $x \cap -y = 0$, to $x = x \cap I = x \cap (y \cup -y) = (x \cap y) \cup (x \cap -y) = (x \cap y) \cup 0 = x \cap y$ i stąd $x \leqslant y$.

Koniec dowodu.

Strukturę rozdzielną z uzupełnieniami /tzn. taką, w której każdy element ma uzupełnienie/ nazywamy algenrą Boole'a. Z tej definicji wynika, że każda algebra Boole'a ma swój element najmniejszy 0 i największy I.

Przykładami algebr Boole'a mogą być znane z teorii mnogości ciała zbiorów, w szczególności ciała wszystkich podzbiorów danego zbioru. W tym przypadku oprócz dwuargumentowych operacji sumy i przecięcia wykorzystuje się także sumy i przecięcia nieskończone. Wtedy dla dowolnego zbioru P i dla dowolnej niepustej rodziny H zbiorów, należących do algebry Boole'a zbiorów jest

$$P \cup \bigcup_{Z \in H} Z = \bigcup_{Z \in H} (P \cup Z), \qquad 1.28$$

$$P \cap \bigcap_{Z \in H} Z = \bigcap_{Z \in H} (P \cap Z), \qquad 1.29$$

$$\text{jeśli } P \in H, \text{ to } P \cup \bigcap_{Z \in H} Z = P, \qquad 1.30$$

$$\text{jeśli } P \in H, \text{ to } P \cap \bigcup_{Z \in H} Z = P, \qquad 1.31$$

$$P \cap \bigcup_{Z \in H} Z = \bigcup_{Z \in H} (P \cap Z), \qquad 1.32$$

$$P \cup \bigcap_{Z \in H} Z = \bigcap_{Z \in H} (P \cup Z), \qquad 1.33$$

$$- \bigcup_{Z \in H} Z = \bigcap_{Z \in H} - Z, \qquad 1.34$$

$$- \bigcap_{Z \in H} Z = \bigcup_{Z \in H} - Z. \qquad 1.35$$

<u>Twierdzenie 1.4</u> Niech E będzie rodziną wszystkich podzbiorów dowolnego zbioru I. Jeżeli F jest jej dowolną podrodziną, zawierającą I i całkowicie multyplikatywną, tzn.

$$F \subset E \ , \qquad 1.36$$

$$I \in F \ , \qquad 1.37$$

$$\text{dla każdej rodziny } G \subset F \quad \bigcap_{X \in G} X \in F \qquad 1.38$$

oraz dla każdego $S \in E$, S^* oznacza najmniejszy ze zbiorów $X \in F$ takich, że $S \subset X$, czyli

$$S^* = \bigcap_{\substack{X \in F \\ S \subset X}} X \ , \qquad 1.39$$

to dla dowolnych $P \in E$, $Q \in E$, $H \subset E$

$$P \subset P^* \ , \qquad 1.40$$

$$\text{jeśli } P \subset Q \text{ , to } P^* \subset Q^* \ , \qquad 1.41$$

$$P^{**} = P^* \ , \qquad 1.42$$

a ponadto

$$(P^* \cup Q)^* = (P \cup Q)^* \ , \qquad 1.43$$

$$\left(\bigcup_{Z \in H} Z^*\right)^* = \left(\bigcup_{Z \in H} Z\right)^* , \qquad 1.44$$

$$\left(\bigcap_{Z \in H} Z^*\right)^* = \bigcap_{Z \in H} Z^* \ , \qquad 1.45$$

$$I^* = I \ . \qquad 1.46$$

Dowód:

1.40 wynika bezpośrednio z definicji. Jeżeli $P \subset Q$, to wobec $Q \subset Q^*$ jest $P \subset Q^* \in F$, a ponieważ P^* jest najmniejszym elementem F zawierającym P, to $P^* \subset Q^*$, czyli 1.41. Jeżeli $X \in F$, to $X^* = X$; stąd 1.42. Dalsze równości możemy wyprowadzić, korzystając tylko z 1.40 - 1.42. Z własności sumy i z 1.40 wynika

$$P \subset P \cup Q \subset P^* \cup Q \quad \text{oraz}$$

$$Q \subset P \cup Q \subset (P \cup Q)^* .$$

Stąd, korzystając z 1.41 otrzymujemy

$$P^* \subset (P \cup Q)^* \subset (P^* \cup Q)^*$$

i

$$P^* \cup Q \subset (P \cup Q)^* \subset (P^* \cup Q)^*$$

Z tego, z 1.40 i 1.41 wynika $(P^* \cup Q)^* \subset (P \cup Q)^* \subset (P^* \cup Q)^*$, czyli 1.43.

Niech Y będzie dowolnym elementem H. Wtedy

$$Y \subset \bigcup_{Z \in H} Z ,$$

$$Y \subset Y^* \subset (\bigcup_{Z \in H} Z)^* ,$$

$$\bigcup_{Y \in H} Y \subset \bigcup_{Y \in H} Y^* \subset (\bigcup_{Z \in H} Z)^* ,$$

$$(\bigcup_{Y \in H} Y)^* \subset (\bigcup_{Y \in H} Y^*)^* \subset (\bigcup_{Z \in H} Z)^* \quad \text{i stąd 1.44.}$$

Podobnie dla każdego $Y \in H$

$$\bigcap_{Z \in H} Z^* \subset Y^* ,$$

$$(\bigcap_{Z \in H} Z^*)^* \subset Y^* ,$$

$$(\bigcap_{Z \in H} Z^*)^* \subset \bigcap_{Y \in H} Y^* \subset (\bigcap_{Y \in H} Y^*)^* \quad \text{i stąd 1.45.}$$

Dalej, ponieważ I jest największym elementem E, $I^* \subset I$ oraz wobec 1.40 $I \subset I^*$ - stąd 1.46.

Koniec dowodu.

<u>Wniosek 1.5.</u> Jeżeli F jest przeciwdziedziną operacji $*$, określonej na rodzinie E wszystkich podzbiorów I i spełniającej 1.40 - 1.42, to są spełnione warunki 1.37 - 1.39.

Dowód:

1.37 i 1.38 wynikają odpowiednio z 1.46 i 1.45, które z kolei można wyprowadzić z 1.40 - 1.42. Jeżeli $S \in E$, $T \in F$ i $S \subset T$, to na mocy 1.41 i 1.40 $S \subset S^* \subset T^* = T$, a więc S^* jest najmniejszym elementem F, zawierającym S.

Koniec dowodu.

Przykład takiej operacji $*$, spełniającej warunki twierdzenia 1.4, mieliśmy już na początku tego rozdziału: branie zbiorów wszystkich elementów podalgebry generowanej przez dany zbiór.

Niech $\{I, o_1, \ldots, o_s\}$ będzie dowolną algebrą; oznaczmy przez E rodzinę wszystkich podzbiorów I. Na elementach E możemy wykonywać wszystkie działania algebry Boole'a; skończone i nieskończone sumy i przecięcia oraz uzupełnianie, a także możemy stosować opisaną wyżej operację $*$. Ponadto możemy dla każdej operacji o_j, dla $1 \leqslant j \leqslant s$, wprowadzić operację Θ_j o takiej samej ilości argumentów m_j, określoną w następujący sposób:

$$\text{jeśli } m_j = 0 \text{, to } \Theta_j = \{o_j\} \text{,} \tag{1.47}$$

$$\text{jeśli } m_j > 0 \text{, to } \Theta_j(X_1, \ldots, X_{m_j}) = \bigcup_{x_1 \in X_1} \cdots \bigcup_{x_{m_j} \in X_{m_j}} \{o_j(x_1, \ldots, x_{m_j})\} \tag{1.48}$$

dla dowolnych $X_1, \ldots, X_{m_j}$, będących podzbiorami I. W szczególności, jeżeli którykolwiek ze zbiorów X_i w wyrażeniu 1.48 jest pusty, to wartością całego wyrażenia jest również zbiór pusty.

Otrzymaliśmy w ten sposób algebrę podzbiorów algebry $\{I, o_1, \ldots, o_s\}$

$$\{E, \cup, \cap, -, *, \Theta_1, \ldots, \Theta_s\} \tag{1.49}$$

/gdzie suma $\cup$ i przecięcie $\cap$ są operacjami dwuargumentowymi/.

2. ALGEBRA PODZBIORÓW GRUPOIDU

Dla grupoidu $\{I, \cdot\}$ algebra 1.49 ma postać

$$\{E, \cup, \cap, -, *, \cdot\}, \qquad 2.1$$

gdzie E jest rodziną wszystkich podzbiorów I. Użycie w obu algebrach kropki jako symbolu operacji nie doprowadzi w tym przypadku do nieporozumień. We wzorach często będziemy tę kropkę opuszczać dla oszczędności zapisu.

W algebrze 2.1 są spełnione warunki 1.4 - 1.12, 1.16 - 1.35 i 1.40 - 1.46. Oprócz tego dla dowolnych $P \in E$, $Q \in E$ i dowolnej niepustej rodziny $H \subset E$ jest

jeśli $P \neq 0$ i $Q \neq 0$, to $P \cdot Q = \bigcup_{p \in P} \bigcup_{q \in Q} \{p \cdot q\}$, 2.2

$P \cdot 0 = 0$, 2.3

$0 \cdot P = 0$, 2.4

jeśli $P \cdot Q = 0$, to $P = 0$ lub $Q = 0$, 2.5

$I \cdot I \subset I$, 2.6

$P \cdot \bigcup_{Z \in H} Z = \bigcup_{Z \in H} (P \cdot Z)$, 2.7

$\left(\bigcup_{Z \in H} Z\right) \cdot Q = \bigcup_{Z \in H} (Z \cdot Q)$, 2.8

Z 2.3, 2.4 i własności zera grupoidu wynika, że zbiór pusty 0 jest jedynym zerem tej algebry ze względu na operację $\cdot$.

Z 2.7 i 2.8 wynika odpowiednio lewo- i prawostronna monotoniczność operacji $\cdot$:

jeśli $P \subset Q$, to $PR \subset QR$ i $RP \subset RQ$. 2.9

Rzeczywiście, jeśli $P \subset Q$, to, jak wynika z twierdzenia 1.2, $Q = P \cup Q$ i wobec 2.7 $QR = PR \cup QR$, czyli $PR \subset QR$. Podobnie wyprowadza się drugą nierówność.

Dla dowolnych $P \in E$, $Q \in E$ istnieje zawsze taki $X \in E$, że $PX \subset Q$ - jak widać z 2.3, zbiór pusty zawsze ten warunek speł-

nia. Z 2.7 wynika, że istnieje największy zbiór o tej własności; będziemy go oznaczać $Q/\!/P$ i nazywać ilorazem lewostronnym Q przez P. Tak samo z 2.4 i 2.8 wynika istnienie największego $Y \in E$ takiego, że $YP \subset Q$; będziemy go oznaczać $Q \backslash\!\backslash P$ i nazywać ilorazem prawostronnym Q przez P.

Bezpośrednio z definicji ilorazu lewostronnego wynika, że dla dowolnych $P \in E$, $Q \in E$, $R \in E$

$$P\,(Q/\!/P) \subset Q \qquad 2.10$$

i ogólniej

$$PR \subset Q \text{ wtedy i tylko wtedy, gdy } R \subset Q/\!/P\,, \qquad 2.11$$

$$Q \subset (PQ)/\!/P\,, \qquad 2.12$$

$$P/\!/0 = I\,, \qquad 2.13$$

$$\text{jeśli } Q \neq 0\,, \text{ to } 0/\!/Q = 0\,, \qquad 2.14$$

$$I/\!/Q = I\,. \qquad 2.15$$

Stąd dalej wynikają następujące własności tego ilorazu

$$\text{jeśli istnieje } S \in E \text{ taki, że } QS = P, \text{ to } Q(P/\!/Q) = P, \qquad 2.16$$

$$\text{jeśli } P \subset Q\,, \text{ to } P/\!/R \subset Q/\!/R\,, \qquad 2.17$$

$$\text{jeśli } Q \subset R\,, \text{ to } P/\!/R \subset P/\!/Q \qquad 2.18$$

oraz dla dowolnej rodziny niepustej $H \subset E$

$$\Big(\bigcap_{Z \in H} Z\Big)/\!/Q = \bigcap_{Z \in H} (Z/\!/Q)\,, \qquad 2.19$$

$$P/\!/\bigcup_{Z \in H} Z = \bigcap_{Z \in H} (P/\!/Z)\,. \qquad 2.20$$

Rzeczywiście, jeżeli $QS = P$, to $S \subset P/\!/Q$ i na mocy 2.9 i 2.10 jest $P = QS \subset Q\,(P/\!/Q) \subset P$; stąd 2.16. Jeżeli $P \subset Q$, to z 2.10 mamy $R\,(P/\!/R) \subset P \subset Q$, a więc także $P/\!/R \subset Q/\!/R$, czyli 2.17. Jeżeli $Q \subset R$, to wobec 2.9 i 2.10 $Q(P/\!/R) \subset R(P/\!/R)$ i wobec 2.10 $R(P/\!/R) \subset P$; stąd $Q(P/\!/R) \subset P$ i $P/\!/R \subset P/\!/Q$, czyli 2.18. Ponieważ $Q\big(\big(\bigcap_{Z \in H} Z\big)/\!/Q\big) \subset \bigcap_{Z \in H} Z \subset Y$ dla każdego $Y \in H$, to $\big(\bigcap_{Z \in H} Z\big)/\!/Q \subset Y/\!/Q$, a więc $\big(\bigcap_{Z \in H} Z\big)/\!/Q \subset \bigcap_{Y \in H}(Y/\!/Q)$. Ale $\bigcap_{Y \in H}(Y/\!/Q) \subset X/\!/Q$, czyli $Q \bigcap_{Y \in H}(Y/\!/Q) \subset X$ dla każdego $X \in H$, a więc $Q \bigcap_{Y \in H}(Y/\!/Q) \subset \bigcap_{X \in H} X$, to znaczy $\bigcap_{Y \in H}(Y/\!/Q) \subset \big(\bigcap_{X \in H} X\big)/\!/Q$;

stąd 2.19. Jeżeli oznaczymy $T = P /\!/ \bigcup_{Z\in H} Z$, to $\left(\bigcup_{Z\in H} Z\right) T \subset P$, a więc w szczególności $ZT \subset P$, czyli $T \subset P /\!/ Z$ dla każdego $Z \in H$ i stąd $T \subset \bigcap_{Z\in H} (P /\!/ Z)$. Dalej, $\bigcap_{Z\in H}(P /\!/ Z) \subset P /\!/ Y$, czyli $Y\left(\bigcap_{Z\in H}(P /\!/ Z)\right) \subset P$ dla każdego $Y \in H$. Biorąc sumę wszystkich Y i korzystając z rozdzielności 2.8 mamy $\bigcup_{Y\in H}\left(Y \cdot \bigcap_{Z\in H}(P /\!/ Z)\right) = \left(\bigcup_{Y\in H} Y\right) \cdot \bigcap_{Z\in H}(P /\!/ Z) \subset P$, a zatem $\bigcap_{Z\in H}(P /\!/ Z) \subset P /\!/ \bigcup_{Y\in H} Y$; stąd 2.20.

Podobnie można wyprowadzić własności ilorazu prawostronnego

$$(Q \backslash\!\backslash P)\, P \subset Q \,, \qquad 2.21$$

$RP \subset Q$ wtedy i tylko wtedy, gdy $R \subset Q \backslash\!\backslash P$, 2.22

$$Q \subset (QP) \backslash\!\backslash P \,, \qquad 2.23$$

$$P \backslash\!\backslash 0 = I \,, \qquad 2.24$$

jeśli $Q \neq 0$, to $0 \backslash\!\backslash Q = 0$, 2.25

$$I \backslash\!\backslash Q = I \,, \qquad 2.26$$

jeśli istnieje $S \in E$ taki, że $SQ = P$, to $(P \backslash\!\backslash Q) Q = P$, 2.27

jeśli $P \subset Q$, to $P \backslash\!\backslash R \subset Q \backslash\!\backslash R$, 2.28

jeśli $Q \subset R$, to $P \backslash\!\backslash R \subset P \backslash\!\backslash Q$ 2.29

oraz dla dowolnej niepustej rodziny $H \subset E$

$$\left(\bigcap_{Z\in H} Z\right) \backslash\!\backslash Q = \bigcap_{Z\in H} (Z \backslash\!\backslash Q) \,, \qquad 2.30$$

$$P \backslash\!\backslash \bigcup_{Z\in H} Z = \bigcap_{Z\in H} (P \backslash\!\backslash Z) \,. \qquad 2.31$$

Wobec 2.20 i 2.31 dzielenie lewostronne i prawostronne przez zbiory niepuste można sprowadzić do odpowiedniego dzielenia przez zbiory jednoelementowe. Wobec 2.11 jeśli $s \in I$, $t \in I$, $P \subset I$, to $t \in P /\!/ s$ wtedy i tylko wtedy, gdy $st \in P$, czyli

$$P /\!/ s = \{t : st \in P\} \,. \qquad 2.32$$

Podobnie

$$P \backslash\!\backslash s = \{t : ts \in P\} \,. \qquad 2.33$$

Dzielenie lewostronne i prawostronne przez zbiory jednoelementowe jest rozdzielne względem sumowania zbiorów: dla dowolnych $s \in I$, $H \subset E$

$$\left(\bigcup_{Z \in H} Z\right) /\!\!/ s = \bigcup_{Z \in H} (Z /\!\!/ s) \quad ; \qquad 2.34$$

$$\left(\bigcup_{Z \in H} Z\right) \backslash\!\!\backslash s = \bigcup_{Z \in H} (Z \backslash\!\!\backslash s) \quad . \qquad 2.35$$

Stosując wzór 2.32, można w następujący sposób wyprowadzić 2.34: $\left(\bigcup_{Z \in H} Z\right) /\!\!/ s = \{t: st \in \bigcup_{Z \in H} Z\} = \{t: \bigvee Z \in H\,(st \in Z)\} = \bigcup_{Z \in H} \{t: st \in Z\} = \bigcup_{Z \in H} (Z /\!\!/ s)$, gdzie $\bigvee$ oznacza kwantyfikator egzystencjalny. Podobnie wyprowadza się 2.35.

Z rozdzielności dzielenia przez zbiór jednoelementowy względem sumy i przecięcia zbiorów wynika, że dla dowolnych $P \subset I$, $s \in I$

$$P /\!\!/ s \cup -P /\!\!/ s = (P \cup -P) /\!\!/ s = I /\!\!/ s = I \ ,$$
$$P /\!\!/ s \cap -P /\!\!/ s = (P \cap -P) /\!\!/ s = 0 /\!\!/ s = 0 \ ,$$

a stąd

$$-P /\!\!/ s = -(P /\!\!/ s) \qquad 2.36$$

i podobnie

$$-P \backslash\!\!\backslash s = -(P \backslash\!\!\backslash s) \qquad 2.37$$

Równości 2.34 - 2.37 nie można jednak uogólnić na dzielenie przez dowolne zbiory; na przykład $-P /\!\!/ 0 = P /\!\!/ 0 = I \neq -(P /\!\!/ 0) = 0$.

<u>Twierdzenie 2.1</u> Jeżeli $\mathfrak{T}$ jest którąkolwiek z następujących własności operacji dwuargumentowej, takich jak:

przemienność,
łączność,
istnienie jedności lewostronnej,
istnienie jedności prawostronnej,
istnienie jedności,
istnienie i nierozkładalność jedności,

to w grupoidzie $\{I, \cdot\}$ operacja $\cdot$ ma własność $\mathfrak{T}$ wtedy i tylko wtedy, gdy tę samą własność ma operacja $\cdot$ w algeb-

rze podzbiorów tego grupoidu $\{E, \cup, \cap, -, *, \cdot\}$.

Dowód:

P r z e m i e n n o ś ć: Jeśli $p \cdot q = q \cdot p$ dla dowolnych $p \in I$, $q \in I$, to z 2.2 wynika przemienność operacji $\cdot$ na zbiorach niepustych, a więc wobec 2.3 i 2.4, także na zbiorach dowolnych. Odwrotnie, jeżeli operacja $\cdot$ na zbiorach jest przemienna i $p \in I$, $q \in I$, to $\{p \cdot q\} = \{p\} \cdot \{q\} = \{q\} \cdot \{p\} = \{q \cdot p\}$, a równość zbiorów jednoelementowych pociąga za sobą równość ich elementów.

Ł ą c z n o ś ć: Przypuśćmy, że dla dowolnych $p \in I$, $q \in I$, $r \in I$ $p \cdot (q \cdot r) = (p \cdot q) \cdot r$. Ponieważ zbiór pusty jest zerem, wystarczy udowodnić łączność operacji $\cdot$ dla zbiorów niepustych. Wobec 2.2, 2.7 i 2.8

$$P \cdot (Q \cdot R) = \Big(\bigcup_{p \in P} \{p\}\Big) \cdot \bigcup_{q \in Q} \bigcup_{r \in R} \{q \cdot r\} = \bigcup_{p \in P} \bigcup_{q \in Q} \bigcup_{r \in R} \{p \cdot (q \cdot r)\} =$$
$$= \bigcup_{p \in P} \bigcup_{q \in Q} \bigcup_{r \in R} \{(p \cdot q) \cdot r\} = (P \cdot Q) \cdot R.$$

Odwrotnie, z łączności operacji $\cdot$ na zbiorach wynika

$$\{p \cdot (q \cdot r)\} = \{p\} \cdot \{q \cdot r\} = \{p\} \cdot (\{q\} \cdot \{r\}) = (\{p\} \cdot \{q\}) \cdot \{r\} =$$
$$= \{p \cdot q\} \cdot \{r\} = \{(p \cdot q) \cdot r\}.$$

J e d n o ś ć l e w o s t r o n n a: Jeżeli e jest jednością lewostronną grupoidu, to dla dowolnego niepustego $P \subset I$ $\{e\} \cdot P = \bigcup_{p \in P} \{e \cdot p\} = P$; stąd i z 2.3 wynika, że $\{e\}$ jest jednością lewostronną algebry zbiorów ze względu na operację $\cdot$. Odwrotnie, jeżeli $A \in E$ i dla każdego $P \in E$ $AP = P$, to $A \neq 0$ i dla każdego $p \in I$ $A \cdot \{p\} = \{p\}$, czyli dla każdego $a \in A$ $a \cdot p = p$, to znaczy A jest zbiorem jedności lewostronnych grupoidu.

J e d n o ś ć p r a w o s t r o n n a i j e d n o ś ć: analogicznie.

N i e r o z k ł a d a l n o ś ć j e d n o ś c i: Jeżeli $P \in E$, $Q \in E$, to $P \cdot Q = \{e\}$, wtedy i tylko wtedy, gdy dla dowolnych $p \in P$, $q \in Q$ $p \cdot q = e$. Stąd jedność w grupoidzie jest nierozkładalna wtedy i tylko wtedy, gdy jest nierozkładalna w algebrze jego podzbiorów.

Koniec dowodu.

Jak wynika z tego dowodu, algebra podzbiorów grupoidu ma jedność wtedy i tylko wtedy, gdy ten grupoid ma jedność: jednością algebry podzbiorów jest w takim przypadku zbiór, mający jako swój jedyny element jedność grupoidu.

Dla uproszczenia zapisu będziemy niżej oznaczać jednakowo zbiory jednoelementowe i ich elementy. W ten sposób np. wzór 2.2 uzyska postać

$$PQ = \bigcup_{p \in P} \bigcup_{q \in Q} pq ,$$

a dla dowolnych $a \in I$, $A \subset I$ zapisy $a \in A$ i $a \subset A$ są równoważne. W szczególności będziemy zawsze jednakowo oznaczać jedność grupoidu i jedność /ze względu na operację $\cdot$ / algebry jego podzbiorów.

Grupoid z jednością e będziemy niżej oznaczać $\{I, \cdot, e\}$ /traktując e jako operację 0-argumentową/, zaś algebrę jego podzbiorów $\{E, \cup, \cap, -, *, \cdot, e\}$. Ta umowa wpływa zresztą tylko na interpretację operacji $*$: z niej wynika, że w każdym grupoidzie z jednością dla każdego zbioru P jest $e \in P^*$. Na własności innych operacji to założenie nie ma żadnego wpływu.

<u>Twierdzenie 2.2</u> W algebrze podzbiorów grupoidu z jednością $\{I, \cdot, e\}$ oprócz 1.4 - 1.12, 1.16 - 1.35, 1.40 - 1.46, 2.2 - 2.37 są spełnione warunki:

$$e^* = e , \qquad 2.38$$

$$0^* = e , \qquad 2.39$$

$$P^* P^* = P^* , \qquad 2.40$$

$$P /\!/ e = P , \qquad 2.41$$

$$e \subset P /\!/ Q \text{ wtedy i tylko wtedy, gdy } Q \subset P , \qquad 2.42$$

$$P = \bigcup_{s \in I} s \left(P /\!/ s \right) , \qquad 2.43$$

$$\text{jeśli } e \in P \text{ , to } P /\!/ P \subset P , \qquad 2.44$$

$$P \backslash\!\backslash e = P , \qquad 2.45$$

$$e \subset P \backslash\!\backslash Q \text{ wtedy i tylko wtedy, gdy } Q \subset P , \qquad 2.46$$

$$P = \bigcup_{s \in I} \left(P \backslash\!\backslash s \right) s , \qquad 2.47$$

$$\text{jeśli } e \in P \text{ , to } P \backslash\!\backslash P \subset P . \qquad 2.48$$

Dowód:

2.38 i 2.39 wynikają bezpośrednio z definicji. Dla dowolnego P zbiór P^* jest zamknięty ze względu na $\cdot$ i każdy $p \in P$ można przedstawić w formie $p = p \cdot e \in P^* P^*$; stąd 2.40. 2.41 i 2.45 wynikają z definicji ilorazów, 2,42 i 2.46 odpowiednio z 2.11 i 2.22 oraz z własności jedności. Na mocy 2.10 dla każdego $s \in I$ $s(P /\!/ s) \subset P$ i stąd $\bigcup_{s \in I} s(P /\!/ s) \subset P$. Odwrotnie, jeżeli $s \in P$, to $e \subset P /\!/ s$, czyli $s \subset s(P /\!/ s)$ a więc $P \subset \bigcup_{s \in P} s(P /\!/ s) \subset \bigcup_{s \in I} s(P /\!/ s) \subset P$; stąd 2.43 i analogicznie 2.47. Jeśli $e \in P$, to warunek $p \in P /\!/ P$ jest równoważny $Pp \subset P$, ale $P = e \cup P$ i $p \in p \cup PP = (e \cup P)p = Pp \subset P$; stąd 2.44 i podobnie 2.48.

Koniec dowodu.

W algebrze podzbiorów dowolnego grupoidu z jednością $\{I, \cdot, e\}$ można wprowadzić funkcję ε, określoną w następujący sposób:

$$\varepsilon(P) = \begin{cases} 0 & \text{gdy } e \notin P \subset I, \\ e & \text{gdy } e \in P \subset I. \end{cases} \qquad 2.49$$

Funkcja ta ma następujące oczywiste własności: dla dowolnych $P \in E$, $Q \in E$, $H \subset E$

$$\varepsilon(\varepsilon(P)) = \varepsilon(P), \qquad 2.50$$

$$\varepsilon\Big(\bigcup_{Z \in H} Z\Big) = \bigcup_{Z \in H} \varepsilon(Z), \qquad 2.51$$

$$\varepsilon\Big(\bigcap_{Z \in H} Z\Big) = \bigcap_{Z \in H} \varepsilon(Z), \qquad 2.52$$

$$\varepsilon(-P) = \begin{cases} 0 & \text{gdy } \varepsilon(P) = e, \\ e & \text{gdy } \varepsilon(P) = 0, \end{cases} \qquad 2.53$$

$$\varepsilon(P^*) = e, \qquad 2.54$$

$$\varepsilon(P /\!/ Q) = \varepsilon(P \backslash\!\backslash Q) = \begin{cases} 0 & \text{gdy } Q \not\subset P, \\ e & \text{gdy } Q \subset P. \end{cases} \qquad 2.55$$

Poza tym w każdym grupoidzie z jednością jest

$$\varepsilon(P)\varepsilon(Q) \subset \varepsilon(PQ) ,$$

ale

$$\varepsilon(P)\varepsilon(Q) = \varepsilon(PQ) , \qquad 2.56$$

wtedy i tylko wtedy, gdy jedność jest nierozkładalna.

Twierdzenie 2.3 W algebrze podzbiorów każdej półgrupy $\{I, \cdot\}$ /lub półgrupy z jednością $\{I, \cdot , e\}$/ dla dowolnych $P \subset I$, $Q \subset I$, $R \subset I$ jest

$$(P /\!\!/ Q) /\!\!/ R = P /\!\!/ QR , \qquad 2.57$$

$$(P \backslash\!\!\backslash Q) \backslash\!\!\backslash R = P \backslash\!\!\backslash RQ , \qquad 2.58$$

$$(P /\!\!/ Q) \backslash\!\!\backslash R = (P \backslash\!\!\backslash R) /\!\!/ Q \qquad 2.59$$

i wyrażenie 2.59 jest największym zbiorem X takim, że $QXR \subset P$.

Dowód:

Ponieważ mamy do czynienia z półgrupą, operacja $\cdot$ na zbiorach jest łączna /twierdzenie 2.1/, czyli dla dowolnych $Q \subset I$, $R \subset I$, $S \subset I$ następujące warunki są równoważne: $S \subset (P /\!\!/ Q) /\!\!/ R$, $RS \subset P /\!\!/ Q$, $Q(RS) \subset P$, $(QR)S \subset P$, $S \subset P /\!\!/ QR$. Rodziny wszystkich zbiorów S , spełniających te warunki, są identyczne, a zatem sumy elementów tych rodzin /będące ich elementami największymi/ są równe - stąd 2.57. Podobnie wyprowadza się 2.58. Dalej, równoważne są także następujące nierówności: $S \subset (P /\!\!/ Q) \backslash\!\!\backslash R$, $SR \subset P /\!\!/ Q$, $Q(SR) \subset P$, $(QS)R \subset P$, $QS \subset P \backslash\!\!\backslash R$, $S \subset (P \backslash\!\!\backslash R) /\!\!/ Q$. Zarówno rodziny wszystkich zbiorów S . spełniających dowolny z tych warunków, jak największe elementy tych rodzin są identyczne; stąd 2.59.

Koniec dowodu.

Lemat 2.4 $\{P, \cdot , e\}$ jest podgrupoidem grupoidu z jednością /czyli $P^* = P$/ wtedy i tylko wtedy, gdy $e \in P$ i $PP \subset P$.

Dowód:

Następujące zdania są równoważne:

$$PP \subset P \quad \text{i} \quad e \in P$$

dla dowolnych $p \in P$, $q \in P$ $pq \in P$ i $e \in P$, P jest zamknięty ze względu na operacje $\cdot$ i e.

Koniec dowodu.

Twierdzenie 2.5 W algebrze podzbiorów dowolnej półgrupy z jednością $\{I, \cdot, e\}$ dla każdego $P \subset I$

$$P^* = \bigcup_{i=0}^{\infty} P^i , \qquad 2.60$$

gdzie

$$P^0 = e ,$$

$$P^{i+1} = PP^i .$$

Dowód:

Z własności operacji $\cdot$ i * wynika, że jeśli $R \subset P^*$, $S \subset P^*$, to $RS \subset P^*$. Stąd $P^i \subset P^*$ dla $i=0, 1, 2, \ldots$. Dalej, $\left(\bigcup_{i=0}^{\infty} P^i\right)\left(\bigcup_{j=0}^{\infty} P^j\right) = \bigcup_{i=0}^{\infty}\left(P^i \bigcup_{j=0}^{\infty} P^j\right) = \bigcup_{i=0}^{\infty} \bigcup_{j=0}^{\infty} P^i P^j =$ $= \bigcup_{i=0}^{\infty} \bigcup_{j=0}^{\infty} P^{i+j} = \bigcup_{k=0}^{\infty} P^k$, a więc na mocy lematu 2.4 $\bigcup_{i=0}^{\infty} P^i$ jest podpółgrupą półgrupy $\{I, \cdot, e\}$, no i oczywiście zawiera P; stąd $\bigcup_{i=0}^{\infty} P^i \supset P^*$ i 2.60.

Koniec dowodu.

Wniosek 2.6 W algebrze podzbiorów dowolnej półgrupy z jednością $\{I, \cdot, e\}$ dla dowolnego $P \subset I$

$$PP^* = P^*P , \qquad 2.61$$

$$e \cup PP^* = P^* , \qquad 2.62$$

Twierdzenie 2.7 Niech $\{I, \cdot, e\}$ będzie dowolną półgrupą z jednością. Wtedy dla każdego $P \subset I$ i dla każdego $s \in I$ następujące warunki są równoważne:

$$P = P^* , \qquad 2.63$$

istnieje taki $R \subset I$, że $P = R^*$, 2.64

$$e \in P \text{ i } P^2 \subset P , \qquad 2.65$$

$e \in P$ i $P = P^2$, 2.66

$s \in P$ wtedy i tylko wtedy, gdy $P \subset P /\!/ s$, 2.67

$e \in P$ i $P \subset P /\!/ P$, 2.68

$P = P /\!/ P$, 2.69

istnieje taki $R \subset I$, że $P = R /\!/ R$, 2.70

$s \in P$ wtedy i tylko wtedy, gdy $P \subset P \backslash\!\backslash s$, 2.71

$e \in P$ i $P \subset P \backslash\!\backslash P$, 2.72

$P = P \backslash\!\backslash P$, 2.73

istnieje taki $R \subset I$, że $P = R \backslash\!\backslash R$, 2.74

Dowód:

Równoważność 2.63 - 2.66 wynika bezpośrednio z lematu 2.4 i własności * . Załóżmy teraz, że 2.65. Jeśli $s \in P$, to $sP \subset P$, czyli $P \subset P /\!/ s$, a jeśli $s \notin P$, to $e \notin P /\!/ s$ i wobec $e \in P$ jest $P \not\subset P /\!/ s$; stąd 2.67. Jeżeli 2.67 , to $e \in P$, bo $P \subset P = P /\!/ e$, a także $P \subset P /\!/ s$ dla każdego $s \in P$; stąd $P \subset \bigcap_{s \in P} P /\!/ s = P /\!/ \bigcup_{s \in P} s = P /\!/ P$, czyli 2.68. Jeżeli 2.68, to wobec 2.44 jest 2.69, a więc i 2.70. Jeżeli 2.70 , to ponieważ $R = Re$, jest $e \subset R /\!/ R = P$ i wobec 2.16 $R = R\,(R /\!/ R)$, a zatem na mocy 2.57 $P = R /\!/ R = R /\!/ R\,(R /\!/ R) = (R /\!/ R) /\!/ (R /\!/ R) = P /\!/ P$ czyli $P^2 \subset P$, a więc 2.65. Podobnie dowodzi się, że wszystkie warunki 2.71 - 2.74 są równoważne 2.65.

Koniec dowodu.

3. ALGEBRY ZDARZEŃ

Niech X będzie dowolnym zbiorem niepustym. Dla ułatwienia dalszego wysłowienia nazwijmy go alfabetem a jego elementy literami. Słowem w alfabecie X nazywamy każdy skończony ciąg, powstający przez napisanie obok siebie dowolnych elementów zbioru X; ilość tych elementów nazywamy długością słowa. Słowo złożone z jednego elementu zbioru X będziemy utożsamiać z tym elementem.

Dopisując obok dowolnego słowa inne słowo otrzymamy nowe słowo; w ten sposób np. ze słów $x_1x_2\ldots x_m$ oraz $y_1y_2\ldots y_n$ możemy otrzymać słowo $x_1x_2\ldots x_my_1y_2\ldots y_n$. Taką operację dopisywania będziemy nazywać złożeniem lub konkatenacją i oznaczymy kropką $\cdot$, ale w słowach i wzorach będziemy z zasady tę kropkę opuszczać.

Złożenie jest operacją łączną; jeżeli więc oznaczymy przez W_X zbiór wszystkich słów w alfabecie X, to algebra $\{W_X, \cdot\}$ będzie półgrupą.

X jest zbiorem generatorów półgrupy $\{W_X, \cdot\}$, gdyż każda półgrupa, zawierająca wszystkie słowa utworzone z elementów X, zawiera W_X w zbiorze swoich elementów.

Niech $\{A, \cdot\}$ będzie dowolną półgrupą i niech $K \subset A$ będzie zbiorem o mocy nie większej od mocy X. Niech f będzie odwzorowaniem X na K. Odwzorowanie to możemy rozszerzyć do homomorfizmu w następujący sposób: jeżeli $f(x_1)$, $f(x_2)$, ..., $f(x_m)$ są obrazami dowolnych elementów zbioru X, to jako obraz słowa $s = x_1x_2\ldots x_m$ przyjmujemy złożenie $h(s) = f(x_1)\,f(x_2)\ldots f(x_m)$. h jest funkcją, bo dowolne dwa słowa, należące do W_X są równe tylko wtedy, gdy mają tę samą formę; w tej algebrze nie ma innej reguły utożsamiania słów poza prawem łączności i wobec tego jeżeli $s = t$, to $h(s) = h(t)$. Oczywiście $h(s) \in A$ dla każdego $s \in W_X$, a więc h jest homomorfizmem odwzorowującym W_X w A. Stąd wynika, że półgrupa $\{W_X, \cdot\}$ jest wolna w każdej klasie półgrup.

Prawdziwe jest również twierdzenie odwrotne: każda półgrupa, wolna w dowolnej klasie półgrup, jest izomorficzna z półgrupą wszystkich słów w pewnym alfabecie; jednak dowodu nie będziemy tu podawać /zob. np. [13] /.

Półgrupa $\{W_X, \cdot\}$ nie zawiera jedności: dla dowolnych $s \in W_X$, $t \in W_X$ jest $st \neq s \neq ts$. Dla dalszych rozważań wygodnie będzie dołączyć do W_X dodatkowy element, który stanie się jednością półgrupy: nazwiemy go "słowem pustym", tzn. słowem nie zawierającym żadnego elementu zbioru X. Oznaczymy go e; dla dowolnego $s \in W_X$ $es = s = se$ oraz $ee = e$. Przyjmujemy, że długość słowa pustego jest równa zeru.

Zbiór, złożony ze wszystkich słów w alfabecie X i ze słowa pustego e będziemy oznaczać I_X. Jak łatwo pokazać, $\{I_X, \cdot, e\}$ jest półgrupą. Jest ona wolna w każdej klasie półgrup z jednością; dowód przebiega podobnie, jak dla $\{W_X, \cdot\}$. Także każda półgrupa z jednością, wolna w każdej klasie półgrup z jednością, jest izomorficzna z $\{I_X, \cdot, e\}$ dla pewnego X, ale nie będziemy tego tu dowodzić /zob. [13]/.

Ze sposobu dołączenia jedności do W_X wynika, że jest ona nierozkładalna w I_X.

Oznaczmy przez E_X rodzinę wszystkich podzbiorów I_X; podzbiory te będziemy także nazywać zdarzeniami w alfabecie X. Algebrę podzbiorów półgrupy z jednością $\{I_X, \cdot, e\}$ będziemy także nazywać algebrą zdarzeń w alfabecie X /lub algebrą zdarzeń nad alfabetem X/, PQ złożeniem lub konkatenacją zbiorów P i Q, zaś P^* iteracją P. Jak wynika z poprzednich rozważań, w tej algebrze istnieją także iloraz lewostronny, iloraz prawostronny i operacja ε, czyli można również tu rozważać algebrę

$$\{E_X, \cup, \cap, -, *, \cdot, e, /\!/, \backslash\!\backslash, \varepsilon\} \quad . \qquad 3.1$$

Jednak specjalnie wyróżnianie tych trzech dodatkowych operacji nie będzie nam potrzebne, mimo że one będą bardzo użyteczne w dalszych rozważaniach, i wobec tego pozostaniemy

przy definicji algebry zdarzeń, przyjętej wyżej .

W przypadkach, w których alfabet X będzie ustalony, będziemy opuszczać wskaźniki przy oznaczeniach I_X i E_X .

Algebry zdarzeń mają pewną istotną cechę, której na ogół nie mają algebry podzbiorów dowolnego grupoidu: nie tylko każde niepuste zdarzenie można przedstawić jako sumę wszystkich swoich elementów, ale każdy z tych elementów, różny od słowa pustego, można w jedyny sposób przedstawić jako skończone złożenie elementów alfabetu. To wpływa istotnie na metodykę rozważań i obliczeń związanych z algebrami zdarzeń oraz z teorią automatów, która w istotny sposób posługuje się tymi zdarzeniami. W szczególności wpływa to na sposób obliczania ilorazów, który odgrywa istotną rolę przy projektowaniu automatów skończonych.

Z 2.20 wynika, że dzielenie lewostronne przez dowolne zdarzenie niepuste da się sprowadzić do dzielenia przez wszystkie słowa należące do tego zdarzenia i następnie obliczenie odpowiedniego przecięcia. Dzielenie przez słowo niepuste można /na mocy 2.57/ sprowadzić do dzielenia przez kolejne litery, wchodzące w skład tego słowa: jeżeli $x_1, x_2, \ldots, x_m$ są literami, to

$$P /\!/ x_1 x_2 \ldots x_m = (\ldots((P /\!/ x_1) /\!/ x_2) \ldots /\!/ x_m) \qquad 3.2$$

Wzory na złożenie dzielenia lewostronnego przez literę z innymi operacjami algebry zdarzeń będą miały następującą postać: dla dowolnej litery a , dowolnych zdarzeń P , Q i dla dowolnej niepustej rodziny zdarzeń H jest

$$\Big(\bigcup_{Z \in H} Z\Big) /\!/ a = \bigcup_{Z \in H} (Z /\!/ a) \quad , \qquad 3.3$$

$$\Big(\bigcap_{Z \in H} Z\Big) /\!/ a = \bigcap_{Z \in H} (Z /\!/ a) \quad , \qquad 3.4$$

$$(-P) /\!/ a = -(P /\!/ a) \quad , \qquad 3.5$$

$$P^* /\!/ a = (P /\!/ a) P^* \quad , \qquad 3.6$$

$$(PQ) /\!/ a = (P /\!/ a) Q \cup \varepsilon(P) Q /\!/ a \quad , \qquad 3.7$$

$$e /\!/ a = 0 \quad . \qquad 3.8$$

Równości 3.3 - 3.5 są trawestacją odpowiednio 2.34, 2.19, 2.36. Pozostałe można uzasadnić w następujący sposób: $e /\!/ a = \{t: at \in e\}$, ale ponieważ e jest nierozkładalne, zbiór ten jest pusty, czyli 3.8. Dalej, P można rozłożyć na sumę dwu zdarzeń rozłącznych: $P = P_0 \cup \varepsilon(P)$, $P_0 \cap \varepsilon(P) = 0$ i teraz $(PQ)/\!/a = ((P_0 \cup \varepsilon(P))Q)/\!/a = P_0Q/\!/a \cup \varepsilon(P)Q/\!/a =$ $= \{t: at \in P_0Q\} \cup \{t: at \in \varepsilon(P)Q\} = \{u_1u_2: au_1 \in P_0, u_2 \in Q\} \cup \varepsilon(P) \cdot$ $\cdot \{t: at \in Q\} = \{u_1: au_1 \in P_0\} Q \cup \varepsilon(P)Q/\!/a = (P_0/\!/a)Q \cup \varepsilon(P)Q/\!/a$. Ale $\varepsilon(P)/\!/a = 0$ wobec 3.8 i 2.14, a więc $P_0/\!/a =$ $= P_0/\!/a \cup \varepsilon(P)/\!/a = P/\!/a$; stąd 3.7. Dalej na mocy 2.60 i 3.3 $P^*/\!/a = \bigcup_{i=0}^{\infty} P^i/\!/a = e/\!/a \cup \bigcup_{i=1}^{\infty} P^i/\!/a = \bigcup_{i=1}^{\infty}(PP^{i-1})/\!/a =$ $= \bigcup_{i=1}^{\infty}((P/\!/a)P^{i-1} \cup \varepsilon(P)P^{i-1}/\!/a) = \bigcup_{i=1}^{\infty}(P/\!/a)P^{i-1}$, ponieważ $\varepsilon(P)P^{i-1}/\!/a$ jest równe 0 lub $P^{i-1}/\!/a$, tzn. innemu składnikowi sumy, o mniejszym wykładniku. Stąd 3.6.

Warto tu podkreślić, że wzory 3.6 i 3.7 nie byłyby prawdziwe, gdyby w nich zamiast litery a wziąć dowolne słowo o długości różnej od 1; widać to zresztą z przebiegu dowodu.

Z tego, że każde słowo niepuste, wchodzące w skład dowolnego zdarzenia, można jednoznacznie przedstawić jako skończone złożenie liter, wynika, że dla każdego zdarzenia P

$$P = \varepsilon(P) \cup \bigcup_{a \in X} a(P/\!/a). \qquad 3.9$$

Rzeczywiście, P może zawierać e lub nie - fakt ten jest uwzględniony przez dodanie $\varepsilon(P)$. Każde niepuste słowo $s \in P$ zaczyna się od jakiejś litery. Jak widać z definicji ilorazu, $a(P/\!/a)$ jest zbiorem wszystkich słów należących do P i zaczynających się od litery a, a więc $\bigcup_{a \in X} a(P/\!/a)$ jest zbiorem wszystkich niepustych słów, zawartych w P. Składniki tej sumy są oczywiście rozłączne; każdy zawiera słowa, zaczynające się od innej litery alfabetu X.

<u>Twierdzenie 3.1</u> Jeżeli A, B, P są zdarzeniami, to

$$P = AP \cup B ,$$

wtedy i tylko wtedy, gdy

$$P = A^*(B \cup \varepsilon(A) K) ,$$

gdzie K jest dowolnym zdarzeniem.

Dowód:

Zauważmy najpierw, że dla dowolnego zdarzenia A $AA^* \varepsilon(A) = A^* \varepsilon(A)$, bo $\varepsilon(A) = 0$ lub $\varepsilon(A) = e$ i $e \in A$, $e \cup A = A$, $AA^* = (e \cup A) A^* = A^*$.

Jeśli $P = AP \cup B$, to istnieje takie zdarzenie K, że

$$P = K \cup B ,$$

a więc także

$$P = AK \cup AB \cup B ,$$

$$P = A^2K \cup A^2B \cup AB \cup B$$

i ogólnie

$$P = A^nK \cup A^nB \cup \ldots \cup AB \cup B$$

dla każdego naturalnego n. Stąd

$$P = A^*K \cup A^*B .$$

Rozważmy teraz dwa przypadki:

1. $\varepsilon(A) = e$.

Wtedy $AA^* = A^*$ i jeśli $P = AP \cup B$, to $P = AA^*K \cup A^*B = A^*K \cup A^*B$ dla dowolnego K.

2. $\varepsilon(A) = 0$.

Oznaczmy przez $l(s)$ długość słowa s i niech dla dowolnego zdarzenia niepustego S będzie $l(S) = \min_{s \in S} l(s)$ oraz $l(0) = \infty$. Dla dowolnych zdarzeń S, T będzie wtedy $l(ST) = l(S) + l(T)$.

Istnieje takie zdarzenie D, że $D \cup A^*B = A^*K \cup A^*B$ i $D \cap A^*B = 0$. Wobec tego jeśli $P = AP \cup B$, to $P = D \cup A^*B$ oraz $P = AD \cup AA^*B \cup B = AD \cup A^*B$. Stąd $D \subset AD \cup A^*B$ czyli $D \subset AD$. Gdyby było $D \neq 0$, to istniałby taki $s \in D$, że $l(s) = l(D)$ i wtedy $s \in AD$ i $l(s) = l(D) \geqslant l(AD) = l(A) + l(D)$, to znaczy $l(A) = 0$ wbrew założeniu $e \notin A$. Zatem jest $D = 0$, czyli $P = A^*B$.

Odwrotnie, jeżeli $P = A^*(B \cup \varepsilon(A)\, K)$, to

$$AP \cup B = AA^* B \cup AA^* \varepsilon(A)\, K \cup B = A^* B \cup A^* \varepsilon(A)\, K = P$$

Koniec dowodu.

Analogicznie dowodzi się

<u>Wniosek 3.2</u> Jeżeli A, B, P, są zdarzeniami, to

$$P = PA \cup B \quad ,$$

wtedy i tylko wtedy, gdy

$$P = (B \cup \varepsilon(A)\, K)A^* \quad ,$$

gdzie K jest dowolnym zdarzeniem.

4. ZDARZENIA REGULARNE

Pojęcie zdarzenia regularnego w zadanym alfabecie X określimy rekurencyjnie w następujący sposób:

1. Zdarzenie puste 0, słowo puste e i każdy element alfabetu X jest zdarzeniem regularnym.
2. Jeśli P, Q są zdarzeniami regularnymi, to $P \cup Q$, $P \cap Q$, $-P$, P^*, PQ są również zdarzeniami regularnymi.
3. Żadne zdarzenie, którego regularności nie można udowodnić przez zastosowanie skończoną ilość razy reguł 1. i 2. nie jest regularne.

Z tej definicji wynika, że jeżeli zdarzenie jest regularne, to istnieje przedstawiające je wyrażenie algebry zdarzeń, zawierające prócz symboli operacji $\cup, \cap, -, *, \cdot$ i nawiasów tylko elementy zbioru X oraz symbole 0 i e.

Wyrażenia takie będziemy nazywać wyrażeniami regularnymi. Oczywiście każde wyrażenie regularne jest zdarzeniem regularnym, ale zdarzenia regularne, jak zobaczymy niżej, mogą być zapisywane w formie wyrażeń, które nie są regularne.

<u>Twierdzenie 4.1</u> Jeżeli P jest zdarzeniem regularnym i s jest dowolnym słowem w alfabecie X, to $P/\!/s$ jest zdarzeniem regularnym.

Dowód:

Jeżeli P jest zdarzeniem regularnym, to istnieje równe mu wyrażenie regularne. Z wzorów 3.3 - 3.8 widać, że dzielenie lewostronne przez dowolną literę nie wprowadza nowych operacji, poza ε, której wynik jest regularny niezależnie od wartości argumentu. Stąd iloraz dowolnego wyrażenia regularnego przez literę jest wyrażeniem regularnym. Dzielenie przez słowo puste nie zmienia dzielonego zdarzenia. Jeżeli $P/\!/s$ jest regularne dla wszystkich słów o długości $n > 1$, to jest także regularne dla wszystkich słów o długości $n+1$,

bo dzielenie przez nie można sprowadzić do dzielenia przez słowa krótsze i przez litery.

Koniec dowodu.

Twierdzenie 4.2 Układ równań

$$R_1 = A_{11}R_1 \cup A_{12}R_2 \cup \ldots \cup A_{1n}R_n \cup B_1 ,$$
$$R_2 = A_{21}R_1 \cup A_{22}R_2 \cup \ldots \cup A_{2n}R_n \cup B_2 ,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$R_n = A_{n1}R_1 \cup A_{n2}R_2 \cup \ldots \cup A_{nn}R_n \cup B_n ,$$

w którym A_{ij} , B_i są regularne oraz $\varepsilon(A_{ij}) = 0$ dla wszystkich i, j, $1 \leq i \leq n$, $1 \leq j \leq n$, ma jeden układ rozwiązań $R_1, R_2, \ldots , R_n$, i wszystkie te rozwiązania są regularne.

Dowód:

Korzystamy z twierdzenia 3.1. Dla $n=1$ mamy równanie $R_1 = A_{11}R_1 \cup B_1$; wobec regularności A_{11} i B_1 jego rozwiązanie $R_1 = A_{11}^* B_1$ jest też regularne. Załóżmy, że $n > 1$ i że twierdzenie jest prawdziwe dla $n-1$.

Rozwiązując ostatnie równanie ze względu na R_n otrzymujemy

$$R_n = A_{nn}^* \left(A_{n1}R_1 \cup A_{n2}R_2 \cup \ldots \cup A_{n,n-1}R_{n-1} \cup B_n\right) .$$

Podstawiając do pozostałych $n-1$ równań mamy

$$R_i = \left(A_{i1} \cup A_{in}A_{nn}^*A_{n1}\right) R_1 \cup \ldots \cup \left(A_{i,n-1} \cup A_{in}A_{nn}^*A_{n,n-1}\right) R_{n-1}$$
$$\cup \left(B_i \cup A_{in}A_{nn}^*B_n\right) .$$

Dla każdego i, j jest

$$\varepsilon\left(A_{ij} \cup A_{in}A_{nn}^*A_{nj}\right) = \varepsilon(A_{ij}) \cup \varepsilon(A_{in})\varepsilon(A_{nn}^*)\varepsilon(A_{nj}) = 0$$

i wobec tego istnieje jedyny ciąg rozwiązań tego nowego układu równań, $R_1, \ldots , R_{n-1}$, i wszystkie rozwiązania są regularne. Zatem R_n jest też określone jednoznacznie i regularne, czyli cały nasz układ n równań ma jedyny ciąg rozwiązań /które są regularne/.

Koniec dowodu.

Twierdzenie 4.3 Zdarzenie R w dowolnym skończonym alfabecie X jest regularne wtedy i tylko wtedy, gdy ilość d_R różnych ilorazów postaci $R/\!/s$, gdzie s są słowami w tym alfabecie, jest skończona. Jeżeli R jest regularne, to dla każdego słowa $s \in I$ istnieje $t \in I$ o długości nie większej od $d_R - 1$, takie, że $R/\!/s = R/\!/t$.

Dowód:

Przypuśćmy, że R jest zdarzeniem regularnym; wtedy istnieje równe mu wyrażenie regularne. Dowód skończoności d_R przeprowadzimy przez indukcję ze względu na ilość operatorów algebry zdarzeń występujących w tym wyrażeniu.

Jeżeli ta ilość operatorów $n = 0$, to $R = 0$ lub $R = e$ lub R jest literą. Dla każdego słowa s $0/\!/s = 0$ i stąd $d_0 = 1$. $e/\!/e = e$ i jeśli $s \neq e$, to $e/\!/s = 0$; stąd $d_e = 2$. Dla dowolnej litery a $a/\!/a = e$, $a/\!/e = a$ i jeśli $s \neq a$ i $s \neq e$, to $a/\!/s = 0$; stąd $d_a = 3$.

Załóżmy, że $n > 0$ i że wszystkie zbiory regularne, równe wyrażeniom regularnym o ilości operatorów mniejszej od n, mają skończone ilości różnych ilorazów. Jeżeli R można przedstawić przy pomocy wyrażenia regularnego, zawierającego n operatorów, to możliwe są, zależnie od głównego operatora wyrażenia, następujące przypadki:

$R = P \cup Q$. Wtedy dla każdego słowa s $R/\!/s = P/\!/s \cup Q/\!/s$ i wobec tego $d_R \leq d_P d_Q$. Ale P i Q są wyrażeniami regularnymi o ilości operatorów mniejszej od n, czyli d_P i d_Q są skończone - z tego wynika skończoność d_R.

$R = P \cap Q$. Wtedy $R/\!/s = P/\!/s \cap Q/\!/s$ i podobnie jak poprzednio $d_R \leq d_P d_Q$.

$R = -P$. Wtedy dla każdego słowa s $R/\!/s = -(P/\!/s)$ i $d_R = d_P$.

$R = PQ$. Wtedy dla dowolnego słowa $s = a_1 a_2 \ldots a_m$ mamy

$$PQ /\!/ a_1 = (P /\!/ a_1)\, Q \cup \varepsilon(P)\, Q /\!/ a_1 \quad ,$$

$$PQ /\!/ a_1 a_2 = (PQ /\!/ a_1) /\!/ a_2 = (P /\!/ a_1 a_2) Q \cup \varepsilon (P /\!/ a_1)(Q /\!/ a_2) \cup \varepsilon(P) Q /\!/ a_1 a_2 ,$$

.....

$$PQ /\!/ s = (P /\!/ a_1 \ldots a_m) Q \cup \varepsilon (P /\!/ a_1 \ldots a_{m-1})\, Q /\!/ a_m \cup \ldots \cup$$
$$\cup \varepsilon (P /\!/ a_1)\, Q /\!/ a_2 \ldots a_m \cup \varepsilon(P)\, Q /\!/ a_1 \ldots a_m \quad .$$

Dla dowolnego niepustego s iloraz $R /\!/ s$ jest sumą $(P /\!/ s) Q$ i co najwyżej d_Q różnych ilorazów zdarzenia Q, przy czym suma ich może być utworzona na co najwyżej 2^{d_Q} różnych sposobów. Jeżeli $s = e$, to $R /\!/ s = PQ$. Stąd $d_R \leqslant d_P \; 2^{d_Q}$.

$R = P^*$. Przyjmijmy jak poprzednio $s = a_1 a_2 \ldots a_m$

$$P^* /\!/ a_1 = (P /\!/ a_1)\, P^* \quad ,$$

$$P^* /\!/ a_1 a_2 = (P /\!/ a_1 a_2)\, P^* \cup \varepsilon (P /\!/ a_1)(P^* /\!/ a_2) =$$
$$= (P /\!/ a_1 a_2)\, P^* \cup \varepsilon (P /\!/ a_1)(P /\!/ a_2)\, P^* \quad ,$$

$$P^* /\!/ a_1 a_2 a_3 = (P /\!/ a_1 a_2 a_3)\, P^* \cup \varepsilon (P /\!/ a_1 a_2)(P /\!/ a_3)\, P^* \cup$$
$$\varepsilon (P /\!/ a_1)(P /\!/ a_2 a_3)\, P^* \cup \varepsilon (P /\!/ a_1) \varepsilon (P /\!/ a_2)(P /\!/ a_3) P^* ,$$

.....

Widać, że dla dowolnego słowa s długości $m > 0$ $P^* /\!/ s$ będzie sumą co najwyżej d_P różnych składników postaci $(P /\!/ t)\, P^*$, przy czym suma ta może być tworzona na co najwyżej 2^{d_P} różnych sposobów. Jeżeli $s = e$, to $R /\!/ s = (P /\!/ e)\, P^*$, a więc mamy wyrażenie tej samej postaci, co w przypadku słów niepustych. Stąd $d_R \leqslant 2^{d_P}$. Jak z tego wynika, w każdym wypadku d_R jest ograniczone z góry, a więc jest skończone. To kończy krok indukcyjny.

Odwrotnie, przypuśćmy, że jakieś zdarzenie R ma skończoną ilość ilorazów postaci $R /\!/ s$. Numerując odpowiednio słowa, możemy je ustawić w ciąg

$$R /\!/ s_1 \; , \; R /\!/ s_2 \; , \; \ldots \; , \; R /\!/ s_{d_R} \quad . \qquad 4.1$$

W ciągu tym występuje m.in. $R = R /\!/ e$. Dla każdego j , $1 \leqslant j \leqslant d_R$ zgodnie z 3.9 mamy

$$R/\!/s_j = \varepsilon\left(R/\!/s_j\right) \cup \bigcup_{a\in X} a\left(R/\!/s_{\alpha(j,a)}\right), \quad 4.2$$

gdzie wartość wskaźnika $\alpha(j,a)$ jest wyznaczona zależnością

$$R/\!/s_{\alpha(j,a)} = R/\!/s_j a \ .$$

W układzie wszystkich równań 4.2 współczynniki przy ilorazach są literami lub skończonymi sumami liter, a więc są regularne i żaden z nich nie zawiera e ; stąd wynika regularność wszystkich elementów ciągu 4.1, a więc także regularność R .

Przyjmijmy teraz, że R jest regularne i że obliczamy wszystkie ilorazy $R/\!/s$ najpierw dla słów s długości 0 , potem 1 , 2 itd. Jeżeli dla słów o długości m nie otrzymaliśmy żadnego ilorazu różnego od ilorazów przez słowa krótsze, to dzieląc przez słowa o długości większej od m również żadnego nowego ilorazu nie otrzymamy. Wynika to stąd, że w tym przypadku dla każdego słowa s o długości m istnieje słowo t o mniejszej ilości liter, takie, że $R/\!/s = R/\!/t$. Każde słowo o długości m+1 można przedstawić jako konkatenację sa , gdzie s ma długość m i a jest literą . Ale $R/\!/sa = R/\!/ta$, a długość słowa t jest mniejsza od m+1 . To samo jest dla słów o długości m+k , gdzie k jest dowolną liczbą naturalną. Oczywiście jeżeli ilorazy są uporządkowane według długości słów, przez które dzielimy, to w ostatnim ilorazie różnym od wszystkich poprzednich słowo może mieć długość co najwyżej $d_R - 1$ /bo pierwszym elementem tego ciągu ilorazów będzie iloraz R przez słowo 0-literowe/.

Koniec dowodu.

Z ostatniego fragmentu dowodu wynika również metoda obliczania wszystkich różnych parami ilorazów dowolnego zdarzenia regularnego R /będziemy je niżej nazywać ilorazami charakterystycznymi R /; sposób ten można stosować wtedy, gdy alfabet jest skończony. Jako pierwszy element ciągu 4.1 bierzemy $R = R/\!/e$. Numerujemy wszystkie elementy alfabetu

i dzielimy kolejno przez nie zdarzenie R. Wybieramy te ilorazy, które są różne od wszystkich poprzednich; tworzą one część $R//s_2, \ldots, R//s_{i_1}$ ciągu 4.1. Dalej bierzemy wszystkie ilorazy $R//s_2$ przez kolejne litery, te z nich, które są różne od poprzednio otrzymanych, dodajemy jako nowe elementy ciągu 4.1 i tak dalej aż do momentu, gdy dzielenie nie daje już nowych ilorazów.

Układ 4.2 będziemy nazywać układem równań charakterystycznych zdarzenia regularnego R.

Dla każdego alfabetu istnieją zdarzenia, które nie są regularne. Na przykład niech $a \in X$ i niech

$$S = \bigcup_{n=0}^{\infty} a^{n^2} .$$

Wtedy

$$S // a^k = \bigcup_{n=0}^{\infty} a^{n^2} // a^k = \bigcup_{n=F(\sqrt{k})}^{\infty} a^{n^2 - k} ,$$

gdzie $F(\sqrt{k})$ jest najmniejszą liczbą całkowitą x taką, że $x > \sqrt{k}$. Przypuśćmy, że $S // a^k = S // a^j$, czyli

$$\bigcup_{n=F(\sqrt{k})}^{\infty} a^{n^2 - k} = \bigcup_{n=F(\sqrt{j})}^{\infty} a^{n^2 - j} .$$

Najkrótsze słowa z obu zbiorów oraz słowa bezpośrednio od nich dłuższe powinny być jednakowej długości, a więc

$$\left(F(\sqrt{k})\right)^2 - k = \left(F(\sqrt{j})\right)^2 - j ,$$

$$\left(F(\sqrt{k}) + 1\right)^2 - k = \left(F(\sqrt{j}) + 1\right)^2 - j .$$

Po odjęciu stronami pierwszej równości od drugiej i po prostych przekształceniach otrzymujemy

$$F(\sqrt{k}) = F(\sqrt{j}) .$$

Podstawiając to do pierwszej równości otrzymujemy $k = j$. Ilorazy $S // a^k$ są różne dla różnych k, a więc S nie jest regularny.

Z twierdzenia 4.3 wynika

Wniosek 4.4 Dla każdego zdarzenia regularnego w dowolnym skończonym alfabecie istnieje wyrażenie regularne przedstawiające to zdarzenie, w którym jako operacje występują tylko sumy, złożenia i iteracje.

Dowód:

Układ równań charakterystycznych dowolnego zdarzenia regularnego /w skończonym alfabecie/ jest skończony. Współczynnikami są litery lub skończone sumy liter. Istnieje tylko jeden ciąg rozwiązań; na mocy twierdzeń 3.1 i 4.2 każde z nich można zapisać przy użyciu sumy, złożenia, iteracji i operacji ε . Ale tę ostatnią można usunąć, gdyż wszystkie wyrażenia postaci $\varepsilon(P)$, otrzymywane w takim obliczeniu, będą równe 0.

Koniec dowodu.

Opisana metoda może służyć do likwidowania przecięć i uzupełnień w wyrażeniach regularnych, a także, w pewnych przypadkach, do upraszczania takich wyrażeń /choć nie zawsze obliczone w ten sposób wyrażenia będą prostsze od początkowych/. Rozwiązania układu równań charakterystycznych mogą mieć różną postać - zależy to m.in. od kolejności, w jakiej ruguje się niewiadome, wykonywania dodatkowych przekształceń wyrażeń itd. W każdym razie, aby otrzymać układ równań charakterystycznych, trzeba obliczyć wszystkie ilorazy charakterystyczne danego wyrażenia; to wymaga dzielenia go przez różne słowa i badania równości otrzymywanych wyrażeń. Sprawdzanie równości jest tu niezbędne - inaczej nie moglibyśmy nawet ustalić ilości różnych ilorazów.

Jeżeli nasze zdarzenie jest zapisane w formie wyrażenia regularnego i badanie równości ilorazów /które też można przedstawić w formie wyrażeń regularnych/ sprawia nam trudności, możemy przeprowadzić te obliczenia przy słabszych założeniach: badać nie równość, a podobieństwo wyrażeń.

Dwa wyrażenia regularne nazywamy podobnymi, jeżeli jedno można otrzymać z drugiego, stosując tylko prawa łączności, przemienności i idempotencji sumy.

Wyrażenia są niepodobne, jeżeli nie są podobne.

Twierdzenie 4.5 Jeżeli będziemy obliczać ilorazy dowolnego wyrażenia regularnego przez słowa w ten sposób, że dzielenie przez słowa o długości większej od 1 sprowadzamy do superpozycji dzieleń przez litery, a wszystkie dzielenia przez litery wykonujemy zgodnie z 3.3 - 3.8 bez żadnych dodatkowych przekształceń /poza obliczaniem wartości funkcji ε i redukcjami wynikającymi z własności 0 i e/, to otrzymamy tylko skończoną ilość wyrażeń niepodobnych.

Dowód:

Przeprowadzimy go analogicznie jak dowód twierdzenia 4.3, przez indukcję ze względu na ilość operatorów w wyrażeniu R.

Jeżeli ta ilość operatorów $n = 0$, podobieństwo sprowadza się do równości. Załóżmy wobec tego, że $n > 0$ i że nasze twierdzenie jest prawdziwe dla wyrażeń regularnych o ilości operatorów mniejszej od dowolnie wybranej liczby n i rozważmy wszystkie możliwe przypadki.

$R = P \cup Q$. Wtedy $R/\!/s = P/\!/s \cup Q/\!/s$ dla każdego s, a ponieważ ilości operatorów w P i Q są mniejsze od n, istnieje tylko skończona ilość ilorazów postaci $P/\!/t$ niepodobnych do $P/\!/s$ i tak samo jest dla Q, a więc także dla R.

$R = P \cap Q$ lub $R = -P$. Analogicznie.

$R = PQ$. Ogólna postać ilorazu $R/\!/s$ jest podana w dowodzie twierdzenia 4.3. Ilość składników tego wyrażenia rośnie nieograniczenie z długością s. Prawo łączności pozwala usunąć nawiasy na poziomie sumy. Prawo przemienności pozwala identyfikować sumy, różniące się tylko kolejnością składników. Zauważmy jednak, że wyprowadzone dla tego przypadku

w dowodzie twierdzenia 4.3 oszacowanie $d_R \leq d_P\, 2^{d_Q}$ nie zależy od długości s ; wzrost ilości składników sumy dla długich słów s będzie przerwany dzięki działaniu prawa idempotencji, ponieważ pewne składniki zaczną się powtarzać. Podobne oszacowanie można wykonać teraz - wystarczy tylko zastąpić d_P, d_Q, d_R przez ilość ilorazów niepodobnych dla P, Q i R . Stąd wynika praktyczna wskazówka: przy takich obliczeniach trzeba najpierw upraszczać wyrażenia, korzystając z tego, że suma jest łączna, przemienna i idempotentna, a potem dopiero porównywać je ze sobą.

$R = P^*$. Analogicznie, jak dla złożenia.

Koniec dowodu.

Zaletą tej metody, opartej na badaniu podobieństw, jest jej łatwość, wadą jest to, że ilość otrzymanych w ten sposób wyrażeń może być o wiele większa od ilości ilorazów charakterystycznych. Istnieje jednak sposób, pozwalający na redukowanie zbioru wszystkich ilorazów niepodobnych do zbioru ilorazów charakterystycznych, tzn. na utożsamianie ilorazów, które są równe, ale niepodobne.

Przykład:

Niech alfabet $X = \{a, b\}$ i niech $S = -a^* \cap (a \cup b)^* b$. Wtedy

$$S /\!/ a = -((a /\!/ a)\, a^*) \cap (((a \cup b) /\!/ a)(a \cup b)^* b \cup \varepsilon((a \cup b)^*)(b /\!/ a)) =$$
$$= -a^* \cap (a \cup b)^* b = S \quad ,$$

$$S /\!/ b = -((a /\!/ b)\, a^*) \cap (((a \cup b) /\!/ b)\, (a \cup b)^* b \cup \varepsilon((a \cup b)^*)\, (b /\!/ b)) =$$
$$= -0 \cap ((a \cup b)^* b \cup e) \; .$$

Przechodzimy teraz do dzielenia S przez słowa dwuliterowe; wobec $S /\!/ a = S$ wystarczy ograniczyć się do słów, zaczynających się od litery b .

$$S /\!/ ba = -0 \cap ((a \cup b)^* \cup 0) = -0 \cap (a \cup b)^* b \quad ,$$
$$S /\!/ bb = -0 \cap ((a \cup b)^* b \cup e) = S /\!/ b \; .$$

Dalej

$$S /\!/ baa = -0 \cap (a \cup b)^* b = S /\!/ ba \ ,$$
$$S /\!/ bab = -0 \cap ((a \cup b)^* b \cup e) = S /\!/ b \ .$$

W ten sposób otrzymaliśmy trzy niepodobne ilorazy: S , $S /\!/ b$, $S /\!/ ba$. Korzystając z 3.9 /lub 4.2/ możemy ułożyć trzy równania

$$S = a(S /\!/ a) \cup b(S /\!/ b) \cup \varepsilon(S) = aS \cup b(S /\!/ b) \ ,$$
$$S /\!/ b = a(S /\!/ ba) \cup b(S /\!/ bb) \cup \varepsilon(S /\!/ b) = a(S /\!/ ba) \cup b(S /\!/ b) \cup e,$$
$$S /\!/ ba = a(S /\!/ baa) \cup b(S /\!/ bab) \cup \varepsilon(S /\!/ ba) = a(S /\!/ ba) \cup b(S /\!/ b).$$

Stąd

$$S /\!/ b = S /\!/ ba \cup e \ ,$$
$$S /\!/ ba = a(S /\!/ ba) \cup b(S /\!/ ba) \cup b = (a \cup b)^* b \ ,$$
$$S /\!/ b = (a \cup b)^* b \cup e \ ,$$
$$S = aS \cup b((a \cup b)^* b \cup e) = a^* b((a \cup b)^* b \cup e) \ .$$

Zastanówmy się teraz, jak można by, nie rozwiązując tego układu równań, zbadać, którego z jego rozwiązań są równe. Dla skrócenia zapisu możemy oznaczyć $T = S /\!/ b$, $U = S /\!/ ba$ i wtedy nasz układ przybierze postać

$$S = aS \cup bT \ ,$$
$$T = aU \cup bT \cup e \ ,$$
$$U = aU \cup bT \ .$$

Jak widać, $\varepsilon(S) \neq \varepsilon(T) \neq \varepsilon(U)$, a więc $S \neq T \neq U$. Zbadajmy, czy $S = U$.

Przypuśćmy, że $S \neq U$. Wtedy istnieje słowo s takie, że $s \in S$ i $s \notin U$ lub $s \notin S$ i $s \in U$. Nie jest to słowo puste, bo $\varepsilon(S) = \varepsilon(U) = 0$. Zatem istnieje takie słowo t , że $s = at$ lub $s = bt$. Przypuśćmy, że $s \in S$ i $s \notin U$. W takim razie jeżeli $s = at$, to $t \in S$ i $t \notin U$, a jeżeli $s = bt$, to $t \in T$ i $t \notin T$.

Badanie warunków dla s sprowadziło się do badania warunków dla słowa krótszego. Założenie $s = bt$ doprowadziło od razu do sprzeczności. Jeżeli $s = at$ i t jest słowem pustym, to też otrzymamy sprzeczność, a jeśli t jest niepusty, to możemy dalej zmniejszać długość słów, aż dojdziemy do

warunków na słowa puste. W rezultacie w każdym przypadku dojdziemy do sprzeczności, a więc $S = U$ i

$$S = aS \cup bT \ ,$$
$$T = aS \cup bT \cup e \ .$$

Stąd

$$T = S \cup e \ ,$$
$$S = aS \cup bS \cup b = (a \cup b)^* b \ .$$

Koniec przykładu.

Przytoczone w przykładzie rozważania można uogólnić na dowolne układy równań postaci

$$R_i = \bigcup_{l=1}^{k} a_l R_{\alpha(i,l)} \cup \varepsilon(R_i) \ , \qquad 4.3$$

gdzie $a_1, \ldots, a_k$ jest ciągiem wszystkich elementów skończonego alfabetu X, $1 \leqslant i \leqslant n$ oraz α jest dowolną funkcją, określoną dla $1 \leqslant i \leqslant n$, $1 \leqslant l \leqslant k$ i taką, że dla jakichkolwiek i, l spełniających te warunki, jest $1 \leqslant \alpha(i,l) \leqslant n$.

Ogólna zasada badania równości rozwiązań takiego układu równań wygląda następująco:

Należy narysować kwadratową tablicę $n \times n$ kratek, przyporządkowując kolejnym wierszom i kolumnom odpowiednio zdarzenia $R_1, \ldots, R_n$. Ponieważ ta tablica ma opisywać relację symetryczną i zwrotną, wystarczy wiąć tylko trójkąt: wszystkie pola pod główną przekątną.

Należy wpisać X na przecięciu każdego wiersza, odpowiadającego R_i i kolumny, odpowiadającej R_j, dla których $\varepsilon(R_i) \neq \varepsilon(R_j)$. W polach, w których nie ma znaku X, trzeba wpisać na przecięciu wiersza R_i i kolumny R_j wszystkie pary $R_{\alpha(i,l)}$, $R_{\alpha(j,l)}$ dla $1 \leqslant l \leqslant k$, z tym, że nie warto powtarzać par jednakowych lub różniących się tylko kolejnością elementów, a także nie warto wypisywać par R_i, R_j oraz R_j, R_i oraz takich, dla których $\alpha(i,l) = \alpha(j,l)$.

Jeżeli po wykonaniu tych czynności pozostaną jeszcze wolne pola, wpisać w nich znak V .

W polach, w których nie ma X ani V trzeba wpisywać znak X wszędzie tam, gdzie jest wpisana para R_i, R_j taka, że na przecięciu wiersza R_i i kolumny R_j jest X . Czynność tę należy powtarzać dopóty, aż nie będzie można już wpisać żadnego nowego X .

W rezultacie otrzymamy tablicę relacji równości zdarzeń, będących rozwiązaniami układu 4.3 , w której X oznacza 0, zaś brak X oznacza 1 .

Przykład:

$$R = aY \cup bS \cup cY \cup e \quad ,$$
$$S = aT \cup bU \cup cY \cup e \quad ,$$
$$T = aU \cup bT \cup cY \quad ,$$
$$U = aW \cup bS \cup cY \cup e \quad ,$$
$$W = aS \cup bT \cup cY \quad ,$$
$$Y = aY \cup bY \cup cY \quad .$$

utworzenie tablicy i wpisanie X :

R						
S						
T	X	X				
U			X			
W	X	X		X		
Y	X	X		X		
	R	S	T	U	W	Y

Wpisywanie par $R_\alpha(i,1)$, $R_\alpha(j,1)$

R						
S	TY SU					
T	X	X				
U	WY	TW	X			
W	X	X	SU	X		
Y	X	X	UY	X	SY TY	
	R	S	T	U	W	Y

Dopisywanie X :

R						
S	TY SU					
T	X	X				
U	WY	TW	X			
W	X	X	SU	X		
Y	X	X	UY X	X	SY X TY	
	R	S	T	U	W	Y

i dalej:

R						
S	TY X SU					
T	X	X				
U	WY X	TW	X			
W	X	X	SU	X		
Y	X	X	UY X	X	SY X TY	
	R	S	T	U	W	Y

Teraz już żadnego X dopisać nie można, a więc $S = U$ i $T = W$.

$$R = aY \cup bS \cup cY \cup e \ ,$$
$$S = aT \cup bS \cup cY \cup e \ ,$$
$$T = aS \cup bT \cup cY \ ,$$
$$Y = aY \cup bY \cup cY$$

i stąd

$$Y = 0 \ ,$$
$$T = b^*aS \ ,$$
$$S = ab^*aS \cup bS \cup e = (ab^*a \cup b)^* \ ,$$
$$T = b^*a(ab^*a \cup b)^* \ ,$$
$$R = bS \cup e = b(ab^*a \cup b)^* \cup e \ .$$

Koniec przykładu.

Wszystkie dotychczas podane własności zdarzeń, w których było wykorzystywane dzielenie lewostronne, mają swoje odpowiedniki w warunkach z dzieleniem prawostronnym. Można więc wykazać, że iloraz prawostronny zdarzenia regularnego przez dowolne słowo jest zdarzeniem regularnym i że zdarzenie R w skończonym alfabecie jest regularne wtedy i tylko wtedy, gdy ilość g_R różnych ilorazów prawostronnych tego zdarzenia przez słowa jest skończone. Opierając się na tym i na twierdzeniu 4.3 można dowieść, że jeżeli zdarzenie R jest regularne, to ilość ilorazów postaci $(R \backslash\backslash s) /\!/ t$, gdzie s, t są słowami, jest skończona /bo każdy iloraz $R \backslash\backslash s$ jest regularny i jest ich skończona ilość/ i odwrotnie, jeżeli zdarzenie R w alfabecie skończonym ma skończoną ilość takich ilorazów, to jest regularne /bo w zbiorze tych ilorazów są wszystkie ilorazy charakterystyczne wszystkich ilorazów prawostronnych $R \backslash\backslash s$, które w ten sposób można odtworzyć, a mając wszystkie ilorazy prawostronne można otrzymać R, znajdująo go bezpośrednio lub z układu równań, analogicznego do 4.2/.

Czasami badanie zdarzeń i ich regularności wygodnie jest sprowadzić do badania pewnych równoważności, związanych z tymi zdarzeniami.

Weźmy na przykład dowolne zdarzenie R i równoważność $\equiv_R$:

$$s \equiv_R t \text{ wtedy i tylko wtedy, gdy } R/\!/s = R/\!/t. \quad 4.4$$

Mamy z nią do czynienia zawsze, gdy obliczamy ilorazy charakterystyczne. Ilość jej klas abstrakcji jest równa d_R. Warunek $R/\!/s = R/\!/t$ można też wyrazić inaczej:

dla każdego u $u \in R/\!/s$ jest równoważne $u \in R/\!/t$,

dla każdego u $su \in R$ jest równoważne $tu \in R$.

Stąd 4.4 jest równoważny warunkowi

$$s \equiv_R t \text{ wtedy i tylko wtedy, gdy dla każdego } u \ su \in R \text{ jest równoważne } tu \in R. \quad 4.5$$

Stąd także wynika, że jeśli $s \equiv_R t$, to dla każdego słowa u mamy $su \equiv_R tu$.

Odwróćmy teraz sytuację: przypuśćmy, że $\equiv$ jest taką dowolną równoważnością, że z $s \equiv t$ wynika $su \equiv tu$ dla dowolnego u. Niech K będzie jedną z jej klas abstrakcji. Jeśli $su \equiv tu$, to $su \in K$ jest równoważne $tu \in K$, czyli $u \in K/\!/s$ jest równoważne $u \in K/\!/t$. Zatem jeśli $s \equiv t$, to $K/\!/s = K/\!/t$. Jak z tego widać, ilość ilorazów d_K dowolnej klasy abstrakcji K tej równoważności jest nie większa od ilości wszystkich klas. Jeżeli ta ilość jest skończona, to wszystkie klasy są regularne.

Zanim przejdziemy do dalszych rozważań, przypomnijmy pewne pojęcia, związane z równoważnościami.

Podziałem dowolnego zbioru niepustego I nazywamy taką rodzinę jego podzbiorów, że wszystkie jej elementy są niepuste, parami rozłączne i ich suma jest równa I.

Jak wiadomo, każdy podział zbioru I określa równoważność, dla której elementy podziału są klasami abstrakcji.

Niech $\mathcal{R}$ będzie dowolną rodziną podzbiorów I. Podziałem, wyznaczonym przez tę rodzinę, $\pi(\mathcal{R})$, będziemy nazywać taki podział, że dla każdego $P \in \pi(\mathcal{R})$ i dowolnych $s \in I$, $t \in I$ $s \in P$ i $t \in P$ wtedy i tylko wtedy, gdy dla każdego $R \in \mathcal{R}$ $s \in R$ jest równoważne $t \in R$.

Podział $\pi(\mathcal{R})$ jest skończony wtedy i tylko wtedy, gdy rodzina $\mathcal{R}$ jest skończona. Rzeczywiście, każdy zbiór $R \in \mathcal{R}$ jest sumą pewnych elementów $\pi(\mathcal{R})$, a więc ze skończoności $\pi(\mathcal{R})$ wynika skończoność $\mathcal{R}$; odwrotnie, jeżeli $\mathcal{R}$ ma n elementów, to ilość elementów $\pi(\mathcal{R})$ nie przekracza 2^n.

Wróćmy teraz do równoważności $\equiv_R$. Warunek 4.5 jest równoważny warunkowi

$$s \equiv_R t \text{ wtedy i tylko wtedy, gdy dla każdego } u \quad s \in R\backslash\backslash u \text{ jest równoważne } t \in R\backslash\backslash u . \qquad 4.6$$

Jak z tego widać, zbiór wszystkich klas abstrakcji $\equiv_R$ jest równocześnie podziałem, wyznaczonym przez zbiór wszystkich ilorazów prawostronnych zdarzenia R przez słowa. Stąd natychmiast wynika związek pomiędzy ilością d_R ilorazów charakterystycznych /lewostronnych/ zdarzenia regularnego R oraz ilością g_R różnych ilorazów prawostronnych R przez słowa

$$d_R \leqslant 2^{g_R} .$$

Zupełnie analogicznie można otrzymać nierówność

$$g_R \leqslant 2^{d_R} ,$$

wprowadzając równoważność, definiowaną przy pomocy prawostronnych ilorazów zdarzenia R. Stąd dla każdego zdarzenia regularnego R jest

$$\lg_2 g_R \leqslant d_R \leqslant 2^{g_R} , \qquad 4.7$$

$$\lg_2 d_R \leqslant g_R \leqslant 2^{d_R} . \qquad 4.8$$

Dowolna równoważność $\sim$ jest kongruencją, o ile dla dowolnych słów s, t, u, w z równoważności $s \sim t$ i $u \sim w$ wynika $su \sim tw$. Nietrudno sprawdzić, że warunek ten jest równoważny następującemu: jeśli $s \sim t$, to dla dowolnych u, w $usw \sim utw$.

Równoważność $\equiv_R$ tego warunku nie spełnia, ale można dla każdego zdarzenia R określić kongruencję $\sim_R$:

$s \sim_R t$ wtedy i tylko wtedy, gdy dla dowolnych u , w $usw \in R$ jest równoważne $utw \in R$. 4.9

Z 4.9 natychmiast wynika, że jeśli $s \sim_R t$, to $usw \sim_R utw$, a więc $\sim_R$ jest rzeczywiście kongruencją. 4.9 jest równoważny warunkowi

$s \sim_R t$ wtedy i tylko wtedy, gdy dla dowolnych u , w $s \in (R \setminus w) /\!/ u$ jest równoważne $t \in (R \setminus w) /\!/ u$. 4.10

Stąd widać, że zbiór klas abstrakcji $\sim_R$ jest podziałem, wyznaczonym przez zbiór wszystkich różnych ilorazów postaci $(R \setminus w) /\!/ u$, gdzie w, u są słowami.

Z tych wszystkich rozważań dochodzimy do następującego wyniku:

<u>Twierdzenie 4.6</u> Niech R będzie zdarzeniem w skończonym alfabecie. Następujące warunki są równoważne:

1. R jest regularny .
2. Zbiór klas abstrakcji $\equiv_R$ jest skończony .
3. Zbiór klas abstrakcji $\sim_R$ jest skończony .
4. Istnieje równoważność $\equiv$ o skończonej ilości klas abstrakcji, taka, że z $s \equiv t$ wynika $su \equiv tu$ dla dowolnego u i R jest sumą pewnych jej klas abstrakcji.
5. Istnieje kongruencja $\sim$ o skończonej ilości klas abstrakcji i R jest sumą niektórych /lub wszystkich/ takich klas.

5. AUTOMATY

Automatem /maszyną sekwencyjną/ będziemy nazywać uporządkowaną piątkę

$$\{Q, X, Y, \delta, \lambda\} , \qquad 5.1$$

gdzie Q, X, Y, są zbiorami niepustymi, zaś δ i λ są odwzorowaniami

$$\delta : Q \times X \rightarrow Q ,$$
$$\lambda : Q \times X \rightarrow Y . \qquad 5.2$$

Automat częściowo określony, lub krócej, częściowy /częściowo określona maszyna sekwencyjna/ jest to uporządkowana piątka 5.1, w której funkcje δ i λ są określone na pewnych podzbiorach zbioru $Q \times X$.

Ponieważ $Q \times X$ jest swoim własnym podzbiorem, każdy automat jest automatem częściowym, ale istnieją automaty częściowe, które nie są automatami. W obu przypadkach elementy zbiorów Q, X, Y nazywa się odpowiednio stanami /wewnętrznymi/, stanami wejść i stanami wyjść, zaś δ i λ odpowiednio funkcją przejść i funkcją wyjść tego automatu /lub automatu częściowego/. Zbiór X będziemy nazywać alfabetem wejściowym, Y alfabetem wyjściowym zaś Q alfabetem stanów.

Automat /lub automat częściowy/ nazywamy skończonym, jeżeli wszystkie trzy zbiory, Q, X i Y są skończone.

Automat ze stanem początkowym jest to szóstka uporządkowana

$$\{Q, X, Y, \delta, \lambda, q\} \qquad 5.3$$

gdzie Q, X, Y, δ, λ są takie same, jak w definicji automatu, zaś $q \in Q$ jest wyróżnionym stanem, który nazywamy początkowym.

Analogicznie definiuje się automat częściowy ze stanem początkowym.

Automat skończony /ze stanem początkowym lub bez/, w którym ilość stanów i stanów wejść są stosunkowo niewielkie, można opisać przy pomocy tabelek funkcji δ i λ, które będziemy nazywać odpowiednio tablicami przejść i wyjść.

Przykład:

Niech

$$X = \{a, b\},$$
$$Y = \{u, v, w, t\},$$
$$Q = \{1, 2, 3, 4\}$$

i niech δ, λ mają następujące tabelki

δ	a	b
1	2	3
2	2	3
3	4	1
4	4	1

λ	a	b
1	u	u
2	u	v
3	u	w
4	u	t

Z tych tablic widać np., że

$$\delta(1,a) = \delta(2,a) = 2,$$
$$\delta(3,b) = \delta(4,b) = 1,$$
$$\lambda(1,a) = \lambda(1,b) = u,$$
$$\lambda(3,b) = w.$$

Tablice przejść i wyjść można połączyć w jedną tablicę automatu:

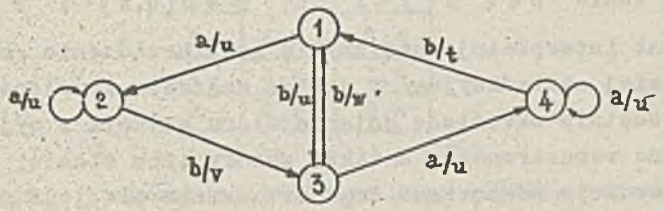
δ,λ	a	b
1	2,u	3,u
2	2,u	3,v
3	4,u	1,w
4	4,u	1,t

Stan automatu i stan wyjścia wewnątrz tablicy oddzielamy dowolnym znakiem przestankowym, np. przecinkiem lub dwukropkiem.

Inną formą opisu automatu skończonego jest wykres Mealy'ego. Tworzy się go w następujący sposób: wypisujemy

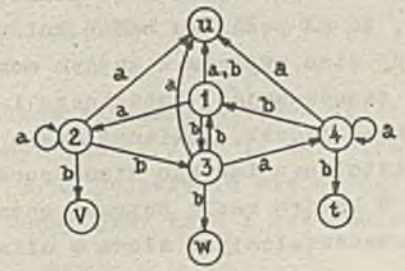
w kółkach wszystkie elementy zbioru Q . Każdą parę kółek z wpisanymi w środku stanami q , p , takimi, że dla pewnej litery $x \in X$ jest $p = \delta(q,x)$, łączymy strzałką, wychodzącą z kółka q do kółka p /w szczególności, gdy q = p, rysujemy strzałkę wracającą do tego samego kółka/. Samą strzałkę oznaczamy parą x , $y = \lambda(q,x)$, przedzieloną skośną kreską.

Dla naszego przykładu wykres Mealy'ego wygląda tak:



Automaty skończone można również opisywać przy pomocy tzw. grafów przepływu. Wypisujemy w kółkach wszystkie elementy zbiorów Q i Y . Kółka te będą wierzchołkami naszego grafu. Każdą parę kółek z wpisanymi stanami q i p takimi, że dla pewnego $x \in X$ jest $p = \delta(q,x)$, łączymy strzałką, wychodzącą z kółka q do kółka p i oznaczoną tą literą x . Podobnie łączymy strzałką oznaczoną literą $x \in X$ każdą parę kółek z wpisanym stanem q i stanem wyjścia $y \in Y$, takich, że $y = \lambda(q,x)$. Strzałka w tym przypadku prowadzi z kółka q do kółka y .

Na przykład graf przepływu automatu, opisanego wyżej, wygląda następująco:



Wierzchołki grafu przepływu, do których nie wchodzi żadna strzałka i z których wychodzi przynajmniej jedna strzałka nazywamy źródłami. Wierzchołki, do których wchodzi przynajmniej jedna strzałka, ale nie wychodzi żadna, nazywamy wypływami. Łatwo zauważyć, że w grafie przepływu dowolnego automatu skończonego wszystkie wierzchołki odpowiadające elementom alfabetu wyjściowego Y są wypływami, natomiast wierzchołki odpowiadające elementom Q mogą być źródłami, ale nigdy nie są wypływami, ponieważ dla każdego $q \in Q$ i dla każdego $x \in X$ istnieją takie $p \in Q$ i $y \in Y$, że $p = \delta(q,x)$ i $y = \lambda(q,x)$.

Automat interpretuje się zwykle jako urządzenie /mniej lub bardziej abstrakcyjne/ z jakimś wejściem i wyjściem, dla którego zostało określone pojęcie stanu wejścia i wyjścia oraz stanu wewnętrznego, a także zbiory tych stanów, X, Y i Q. Konstrukcja wewnętrzna tego urządzenia nie jest dla nas interesująca i nie musimy jej znać. Interesuje nas tylko jego zachowanie, które jest opisane przy pomocy dwóch funkcji δ i λ : jeśli stan automatu jest równy q i stan jego wejścia jest równy x, to stan wyjścia jest równy $\lambda(q;x)$ i stan wewnętrzny automatu staje się równy $\delta(q,x)$.

Jak z tego wynika, stan wyjścia automatu zależy nie tylko od stanu wejścia, ale także od stanu wewnętrznego. Ten z kolei zależy od poprzedniego stanu wejścia i poprzedniego stanu wewnętrznego itd. Inaczej mówiąc, stan wyjścia zależy nie tylko od aktualnego stanu wejścia, ale także od wszystkich poprzedzających stanów wejść, licząc od pewnego momentu wybranego jako początek badania oraz od stanu automatu w tym momencie. Jeżeli mamy do czynienia z automatem ze stanem początkowym, to zwykle zakłada się, że na początku badań automat jest zawsze w tym stanie - wtedy stan wyjścia w każdym momencie zależy tylko od sekwencji stanów wejść, aktualnego i wszystkich poprzedzających. Na razie jednak, ponieważ nasze rozważania mają charakter ogólny, istnienia takiego stanu początkowego nie będziemy zakładać. W każdym razie automat można rozpatrywać jako urządzenie, przekształcające słowa w alfabecie X

/będziemy je nazywać słowami wejściowymi/ na słowa w alfabecie Y /słowa wyjściowe/, mające taką samą długość, przy czym przekształcenie to zależy od stanu automatu w momencie podawania na jego wejście pierwszej litery słowa wejściowego.

Przykład:

Weźmy automat o alfabecie wejściowym $X = \{a, b\}$, alfabecie wyjściowym $Y = \{u, v\}$ i alfabecie stanów $Q = \{1,2,3\}$, mający tablicę

δ,λ	a	b
1	2,u	2,v
2	3,v	1,u
3	3,v	2,u

Zbadajmy jego zachowanie, jeśli na jego wejściu pojawi się sekwencja abaa, a na początku doświadczenia on jest w stanie 1. W tym celu wypiszemy w trzech kolejnych wierszach stany wejścia, stany wewnętrzne i stany wyjścia według ogólnego schematu

$$\begin{array}{lllll} x_1 & x_2 & x_3 & \dots & x_m \\ q & q_1 = \delta(q,x_1) & q_2 = \delta(q_1,x_2) \dots & q_{m-1} & q_m \\ y_1 = \lambda(q,x_1) & y_2 = \lambda(q_1,x_2) & y_3 = \lambda(q_2,x_3) \dots & y_m = \lambda(q_{m-1},x_m) & \end{array}$$

gdzie q jest stanem automatu na początku, zaś $x_1x_2x_3 \dots$ zadaną sekwencją stanów wejścia. W naszym przypadku będziemy mieli

a	b	a	a	
1	2	1	2	3
u	u	u	v	

Jak widać, określona sekwencja stanów wejścia /np. abaa/ powoduje przy danym stanie /np. 1/ określoną zmianę stanów automatu /12123/ oraz pojawienie się określonej sekwencji stanów wyjścia /uuuv/ przy czym i sekwencja stanów i sekwen-

cja wyjściowa zależą zarówno od stanu na początku, jak i od sekwencji wejściowej. Skutki zmiany jednej z tych danych pokazują następujące przykłady:

a	b	a	a	
2	3	2	3	3
v	u	v	v	

lub

a	a	a	a	
i	2	3	3	3
u	v	v	v	

Z ostatniego przebiegu widać, że zmiana ciągu wejściowego tylko na jednym miejscu może zmienić całe dalsze zachowanie automatu. Inaczej mówiąc, zależy ono na ogół od całej poprzedzającej "historii" automatu.

Koniec przykładu.

Dowolne słowo wejściowe jest elementem półgrupy z jednością X^*, generowanej przez zbiór X. Podobnie każde słowo wyjściowe jest elementem wolnej półgrupy z jednością Y^*, generowanej przez zbiór Y. W tej sytuacji możemy dla dowolnego automatu $\{Q, X, Y, \delta, \lambda\}$ rozszerzyć jego funkcje przejść i wyjść do

$$\delta : Q \times X^* \to Q ,$$
$$\lambda : Q \times X^* \to Y^* ,$$

tak, żeby dla dowolnych $q \in Q$, $s \in X^*$, $t \in X^*$ było

$$\delta(q, st) = \delta(\delta(q,s), t) , \qquad 5.4$$
$$\lambda(q, st) = \lambda(q,s)\lambda(\delta(q,s), t) . \qquad 5.5$$

Jeżeli na wejście automatu w stanie $q \in Q$ podamy najpierw sekwencję $s \in X^*$, a potem $t \in X^*$, to po podaniu s znajdzie się on w stanie $p = \delta(q,s)$ a na wyjściu będzie słowo $\lambda(q,s)$. Podanie teraz sekwencji t na wejście powoduje przejście automatu do stanu $\delta(p,t) = \delta(\delta(q,s), t)$, a na wyjściu będzie słowo $\lambda(p,t) = \lambda(\delta(q,s), t)$.

W ciągu całego doświadczenia na wyjściu będzie złożenie $\lambda(q,s)$ i $\lambda(p,t)$, czyli $\lambda(q,s)\lambda(\delta(q,s), t)$ - stąd 5.4 i 5.5. Dla słowa pustego e /jedności półgrupy X^*/ przyjmujemy dla dowolnego $q \in Q$

$$\delta(q,e) = q \quad , \qquad 5.6$$

$$\lambda(q,e) = e \quad . \qquad 5.7$$

Otrzymaliśmy w ten sposób nowy automat $\{Q,X^*,Y^*, \delta, \lambda\}$ będący w pewnym sensie rozszerzeniem automatu $\{Q,X,Y,\delta,\lambda\}$. Jest on zawsze nieskończony.

Jeżeli nas nie interesują całe sekwencje wyjściowe, a tylko ostatnie stany wyjścia, otrzymywane na końcu doświadczenia, możemy zamiast funkcji $\lambda(q,s)$ wziąć funkcję $\mu(q,s)$, której wartością jest zawsze ostatnia litera słowa $\lambda(q,s)$, o ile $s \neq e$ oraz $\mu(q,e) = e$ dla dowolnego q. Wtedy otrzymamy parę odwzorowań

$$\delta : Q \times X^* \to Q \quad ,$$
$$\mu : Q \times X^* \to Y \cup e \quad ,$$

gdzie δ jest taka sama, jak w 5.4 i 5.6, zaś dla dowolnych $q \in Q$, $s \in X^*$, $t \in X^*$ jest

$$\mu(q,st) = \mu(\delta(q,s), t) \quad . \qquad 5.8$$

Jeżeli $q \in Q$ i $x \in X$ /tzn. x jest słowem jednoliterowym/ to

$$\mu(q,x) = \lambda(q,x) \quad , \qquad 5.9$$

Piątka uporządkowana $\{Q, X^*, Y \cup e, \delta, \mu\}$ jest także automatem. Jest on zawsze nieskończony.

Każde z tych dwu rozszerzeń automatu $A = \{Q,X,Y,\delta,\lambda\}$ można uważać za inną formę jego opisu. Dla każdego z nich, można z łatwością odtworzyć A.

Mając dany taki automat A możemy określić zbiory słów w alfabecie X

$$T_{pq} = \{s \in X^* : \delta(p,s) = q\} \quad , \qquad 5.10$$

$$R_{py} = \{s \in X^* : \mu(p,s) = y\} \qquad 5.11$$

Nie trudno zauważyć, że zadanie zbiorów Q, X, Y oraz rodzin $\{T_{pq}\}_{p \in Q, q \in Q}$ i $\{R_{py}\}_{p \in Q, y \in Y}$ całkowicie wyznacza funkcje δ i μ, a zatem także automat A.

Na ogół nie musimy zresztą w tym celu podawać wszystkich zbiorów T_{pq}, R_{py}, gdyż niektóre z nich da się wyznaczyć przy pomocy innych. Przypuśćmy, że $s \in T_{pq}$, czyli $\delta(p,s) = q$. Jeżeli $s = e$, to zgodnie z 5.6 musi być $p = q$; stąd $e \in T_{pq}$ wtedy i tylko wtedy, gdy $p = q$. Jeżeli $s \neq e$, to jest słowem zawierającym przynajmniej jedną literę - oznaczmy pierwszą z nich /od lewej/ przez x, zaś pozostałą część słowa przez t; $s = xt$. Wtedy $\delta(p,s) = \delta(p,xt) = \delta(\delta(p,x),t) = q$. Stąd $t \in T_{\delta(p,x)q}$, a zatem każde słowo z T_{pq} zaczynające się od litery x należy do $xT_{\delta(p,x)q}$. Odwrotnie, dla każdego $t \in T_{\delta(p,x)q}$ jest $\delta(\delta(p,x),t) = q$. Stąd dla dowolnych $p \in Q$, $q \in Q$ jest

$$T_{pq} = \varepsilon(T_{pq}) \cup \bigcup_{x \in X} xT_{\delta(p,x)q}. \qquad 5.12$$

Zupełnie analogicznie można wyprowadzić zależność

$$R_{py} = \bigcup_{x \in X} xR_{\delta(p,x)y} \cup (X \cap R_{py}), \qquad 5.13$$

gdzie $y \in Y$.

Różnica w wyprowadzeniu polega tylko na tym, że wobec $\mu(q,e) = e$ oraz 5.11 $\varepsilon(R_{py}) = 0$ dla wszystkich $p \in Q$ i $y \in Y$ i wobec tego składnik ten można opuścić. Za to dochodzi składnik $X \cap R_{py}$ zawierający wszystkie słowa jednoliterowe $x \in X$ takie, że $\mu(p,x) = y$.

Ponieważ $x \in X \cap R_{py}$ wtedy i tylko wtedy, gdy $x \in X$ i $\varepsilon(R_{py} /\!/ x) = e$, wzór 5.13 można także zapisać w formie

$$R_{py} = \bigcup_{x \in X} xR_{\delta(p,x)y} \cup \bigcup_{x \in X} x\,\varepsilon(R_{py} /\!/ x). \qquad 5.14$$

Z 5.12 i 5.14 wynika, że dla dowolnej litery $a \in X$ i dla dowolnych $p \in Q$, $q \in Q$, $y \in Y$

$$T_{pq} /\!/ a = T_{\delta(p,a)q} \quad , \qquad 5.15$$

$$R_{py} /\!/ a = R_{\delta(p,a)y} \cup \varepsilon\left(R_{py} /\!/ a\right). \qquad 5.16$$

Z wzorów 5.4 - 5.15 wynikają następujące własności T_{pq} i R_{py} :

dla każdego $p \in Q$ zbiór wszystkich niepustych

$$T_{pq},\ q \in Q \text{ jest podziałem } X^*, \qquad 5.17$$

dla każdego $p \in Q$ zbiór wszystkich niepustych

$$R_{py},\ y \in Y \text{ jest podziałem } XX^*, \qquad 5.18$$

$$T_{pq} = \bigcup_{r \in Q} T_{pr} T_{rq} \quad , \qquad 5.19$$

$$R_{py} = \bigcup_{r \in Q} T_{pr} R_{ry} \quad , \qquad 5.20$$

gdzie $p \in Q$, $q \in Q$, $y \in Y$.

Jeżeli automat jest skończony, to możemy ponumerować elementy Q i Y i wtedy rodziny zbiorów T_{pq} i R_{py} można przedstawić jako macierze, których elementami są zdarzenia w alfabecie X ; oznaczymy je odpowiednio $\mathbb{T}$ i $\mathbb{R}$. Macierze tego typu będziemy nazywać macierzami zdarzeń.

Określmy działania na macierzach zdarzeń; jeżeli $\mathbb{A}$, $\mathbb{B}$, $\mathbb{C}$ są dowolnymi macierzami odpowiednio o elementach $\mathbb{A}_{ij}$, $\mathbb{B}_{ij}$, $\mathbb{C}_{jk}$, gdzie $1 \leqslant i \leqslant n_1$, $1 \leqslant j \leqslant n_2$, $1 \leqslant k \leqslant n_3$ oraz n_1 , n_2, n_3 są dowolnymi liczbami naturalnymi /różnymi od 0/ to

$$(\mathbb{A} \cup \mathbb{B})_{ij} = \mathbb{A}_{ij} \cup \mathbb{B}_{ij} \quad , \qquad 5.21$$

$$(\mathbb{A} \cap \mathbb{B})_{ij} = \mathbb{A}_{ij} \cap \mathbb{B}_{ij} \quad , \qquad 5.22$$

$$(-\mathbb{A})_{ij} = -\mathbb{A}_{ij} \quad , \qquad 5.23$$

$$(\mathbb{A}\,\mathbb{C})_{ik} = \bigcup_{j=1}^{n_2} \mathbb{A}_{ij}\,\mathbb{C}_{jk} \quad , \qquad 5.24$$

$$(\varepsilon(\mathbb{A}))_{ij} = \varepsilon(\mathbb{A}_{ij}) \quad . \qquad 5.25$$

Jeżeli S jest dowolnym zdarzeniem w tym samym alfabecie, to

$$(S\,\mathbb{A})_{ij} = S\,\mathbb{A}_{ij} \quad , \qquad 5.26$$

$$(\mathbb{A}\,S)_{ij} = \mathbb{A}_{ij}\,S \quad , \qquad 5.27$$

$$(\mathbb{A}\,/\!/S)_{ij} = \mathbb{A}_{ij}\,/\!/\,S \quad , \qquad 5.28$$

$$(\mathbb{A}\,\backslash\!\backslash\,S)_{ij} = \mathbb{A}_{ij}\,\backslash\!\backslash\,S \quad . \qquad 5.29$$

Zbiór macierzy o tych samych wymiarach z operacjami $\cup$, $\cap$, $-$ jest algebrą Boole'a. Złożenie macierzy, o ile jest wykonalne, jest łączne i rozdzielne względem dodawania.

Jeżeli $\mathbb{P}$ jest macierzą kwadratową, $\mathbb{e}$ jest macierzą jednostkową o tych samych wymiarach /mającą słowa puste e na głównej przekątnej i 0 poza nią/ a $\mathbb{O}$ jest macierzą o tych samych wymiarach, której wszystkie elementy są zbiorami pustymi 0, to

$$\mathbb{P}\,\mathbb{e} = \mathbb{e}\,\mathbb{P} = \mathbb{P} \quad , \qquad 5.30$$

$$\mathbb{P}\,\mathbb{O} = \mathbb{O}\,\mathbb{P} = \mathbb{O} \quad . \qquad 5.31$$

Dla macierzy kwadratowych można określić operację

$$\mathbb{P}^* = \bigcup_{i=0}^{\infty} \mathbb{P}^i \quad , \qquad 5.32$$

gdzie $\mathbb{P}^0$ jest macierzą jednostkową oraz $\mathbb{P}^{i+1} = \mathbb{P}\,\mathbb{P}^i$.

Weźmy automat skończony $\{Q, X, Y, \delta, \lambda\}$ i ponumerujemy jego stany i stany wyjścia

$$Q = \{q_1, q_2, \ldots, q_n\} \quad ,$$

$$Y = \{y_1, y_2, \ldots, y_m\} \quad .$$

Wtedy $\mathbb{T}$ będzie macierzą $n \times n$, zaś $\mathbb{R}$ macierzą $n \times m$ elementów i zależności 5.19, 5.20 możemy krócej zapisać

$$\mathbb{T} = \mathbb{T}\,\mathbb{T} \quad , \qquad 5.33$$

$$\mathbb{R} = \mathbb{T}\,\mathbb{R} \quad . \qquad 5.34$$

Warto przy tym zauważyć, że

$$\varepsilon(\mathbb{T}) = \mathbb{e} \quad . \qquad 5.35$$

Nazwijmy macierzą przejść $\mathbb{A}$ /nie mylić z tablicą przejść/ macierz o wymiarach n x n taką, że

$$\mathbb{A}_{ij} = \{x \in X: \ \delta(q_i, x) = q_j\} \quad , \qquad 5.36$$

czyli

$$\mathbb{A}_{ij} = X \cap \mathbb{T}_{ij} \quad . \qquad 5.37$$

Analogicznie możemy określić macierz wyjść $\mathbb{B}$ o wymiarach n x m

$$\mathbb{B}_{il} = \{x \in X: \ \lambda(q_i, x) = y_l\} \quad , \qquad 5.38$$

czyli

$$\mathbb{B}_{il} = X \cap \mathbb{R}_{il} \quad . \qquad 5.39$$

Wtedy, opierając się na 5.12, 5.35 i 5.13 możemy napisać

$$\mathbb{T} = \mathbb{e} \cup \mathbb{A}\mathbb{T} \quad , \qquad 5.40$$

$$\mathbb{R} = \mathbb{A}\mathbb{R} \cup \mathbb{B} \quad . \qquad 5.41$$

Macierze $\mathbb{A}$ i $\mathbb{B}$ wyznacza się bezpośrednio z tablicy automatu i można je również uważać za pewien sposób jego przedstawienia.

Macierz $\mathbb{A}$ daje nam wszystkie przejścia w automacie /od stanu do stanu/ po podaniu na wejście słów jednoliterowych. $\mathbb{A}^2 = \mathbb{A}\mathbb{A}$ daje nam wszystkie przejścia od stanu do stanu pod wpływem słów dwuliterowych, zaś $\mathbb{e} \cup \mathbb{A} \cup \mathbb{A}^2$ przejścia pod wpływem słów o co najwyżej dwu literach /być może pustych/. Ponieważ $\mathbb{T}$ opisuje nam wszystkie przejścia od stanu do stanu pod wpływem słów wejściowych o dowolnej długości,

$$\mathbb{T} = \mathbb{A}^* \quad . \qquad 5.42$$

Jeżeli narysujemy graf przepływu rozważanego automatu, to zobaczymy, że macierz $\mathbb{B}$ podaje wszystkie przejścia od stanów wewnętrznych do stanów wyjścia, spowodowane przez słowa jednoliterowe. Macierz $\mathbb{A}\mathbb{B}$ daje nam wszystkie

e przejścia pod wpływem słów dwuliterowych. Ogólnie, $\mathbb{A}\ \mathbb{B}$ daje wszystkie przejścia na grafie przepływu od stanów wewnętrznych automatu do stanów jego wyjścia, spowodowane przez i-literowe słowa wejściowe. Ponieważ $\mathbb{R}$ opisuje wszystkie takie przejścia, spowodowane przez słowa o dowolnej długości dodatniej,

$$\mathbb{R} = \mathbb{A}^* \mathbb{B} \ . \qquad 5.43$$

Przykład:

Weźmy następujący automat

$Q = \{1, 2, 3\}$,

$X = \{a, b\}$,

$Y = \{u, v\}$.

Tablica przejść:

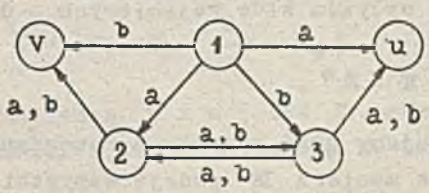
	a	b
1	2	3
2	3	3
3	2	2

tablica wyjść:

	a	b
1	u	v
2	v	v
3	u	u

Przyjmujemy, że każdy element Q jest jednocześnie swoim numerem oraz $y_1 = u$, $y_2 = v$.

Graf przepływu tego automatu:



W układzie równań 5.12 współczynniki przy niewiadomych nie zależą od q. Wobec tego możemy zebrać razem wszystkie równania o tych samych współczynnikach, zostawiając q jako zmienną. Wskaźniki przy niewiadomych po prawej stronie przepisujemy z tablicy przejść

$$T_{1q} = \varepsilon(T_{1q}) \cup aT_{2q} \cup bT_{3q} ,$$
$$T_{2q} = \varepsilon(T_{2q}) \cup aT_{3q} \cup bT_{3q} ,$$
$$T_{3q} = \varepsilon(T_{3q}) \cup aT_{2q} \cup bT_{2q} .$$

Stąd

$$T_{3q} = \varepsilon(T_{3q}) \cup XT_{2q} ,$$
$$T_{2q} = \varepsilon(T_{2q}) \cup XT_{3q} = \varepsilon(T_{2q}) \cup X\,\varepsilon(T_{3q}) \cup X^2T_{2q} =$$
$$= X^{2*}\varepsilon(T_{2q}) \cup X^{2*}X\,\varepsilon(T_{3q}) ,$$
$$T_{3q} = \varepsilon(T_{3q}) \cup XX^{2*}\varepsilon(T_{2q}) \cup XX^{2*}X\,\varepsilon(T_{3q}) =$$
$$= XX^{2*}\varepsilon(T_{2q}) \cup (e \cup X^2X^{2*})\varepsilon(T_{3q}) =$$
$$= XX^{2*}\varepsilon(T_{2q}) \cup X^{2*}\varepsilon(T_{3q}) ,$$
$$T_{1q} = \varepsilon(T_{1q}) \cup aX^{2*}\varepsilon(T_{2q}) \cup aX^{2*}X\,\varepsilon(T_{3q})$$
$$\cup\, bXX^{2*}\varepsilon(T_{2q}) \cup bX^{2*}\varepsilon(T_{3q}) .$$

Korzystając z 5.35 obliczamy wartości funkcji ε i w rezultacie

$$\mathbb{T} = \begin{pmatrix} e & aX^{2*} \cup bXX^{2*} & aX^{2*}X \cup bX^{2*} \\ 0 & X^{2*} & X^{2*}X \\ 0 & XX^{2*} & X^{2*} \end{pmatrix} .$$

W równaniach 5.13 wyrazy wolne zależą istotnie od y, chociaż współczynniki przy niewiadomych są przy ustalonym q dla wszystkich wartości y takie same. Aby nie rozwiązywać wielokrotnie równań o tych samych współczynnikach przy niewiadomych, utwórzmy dla skrócenia zapisu nowe równania, w których jako niewiadome wystąpią wiersze macierzy $\mathbb{R}$

$$\overline{R}_p = \bigcup_{x \in X} x\overline{R}_{\delta(p,x)} \cup \overline{B}_p \quad , \qquad 5.44$$

gdzie

$$\overline{R}_p = (R_{p1}, R_{p2}, \ldots , R_{pm}) ,$$

$$\overline{B}_p = (B_{p1}, B_{p2}, \ldots , B_{pm}) .$$

Dla naszego automatu jest

$$\overline{R}_1 = a\overline{R}_2 \cup b\overline{R}_3 \cup (a,b) \quad ,$$

$$\overline{R}_2 = a\overline{R}_3 \cup b\overline{R}_3 \cup (0, a \cup b) ,$$

$$\overline{R}_3 = a\overline{R}_2 \cup b\overline{R}_2 \cup (a \cup b, 0) .$$

Wskaźniki przy niewiadomych po prawej stronie przepisujemy bezpośrednio z tablicy przejść, macierze wierszowe wyrazów wolnych wyznaczamy z tablicy wyjść automatu.

$$\overline{R}_3 = X\overline{R}_2 \cup (X,0) \quad ,$$

$$\overline{R}_2 = X\overline{R}_3 \cup (0,X) = X^2\overline{R}_2 \cup X(X,0) \cup (0,X) =$$
$$= X^2\overline{R}_2 \cup (X^2,X) = X^{2*}(X^2,X) \quad ,$$

$$\overline{R}_3 = XX^{2*}(X^2,X) \cup (X,0) = (X^{2*}X^2X \cup X, X^{2*}X^2) =$$
$$= X^{2*}(X,X^2) \quad ,$$

$$\overline{R}_1 = aX^{2*}(X^2,X) \cup bX^{2*}(X,X^2) \cup (a,b) =$$
$$= a(X^{2*}X^2 \cup e, X^{2*}X) \cup b(X^{2*}X, X^{2*}X^2 \cup e) =$$
$$= a\,X^{2*}(e,X) \cup bX^{2*}(X,e) \quad ,$$

Stąd

$$\mathbb{R} = \begin{pmatrix} aX^{2*} \cup bX^{2*}X & aX^{2*}X \cup bX^{2*} \\ X^{2*}X^2 & X^{2*}X \\ X^{2*}X & X^{2*}X^2 \end{pmatrix} .$$

Korzystając z tego, że mnożenie dowolnej potęgi X przez X^2 jest przemienne, oraz z wzoru 5.27, możemy napisać

$$\mathbb{R} = \begin{pmatrix} a \cup bX & aX \cup b \\ X^2 & X \\ X & X^2 \end{pmatrix} X^{2*}$$

Macierz przejść automatu:

$$\mathbb{A} = \begin{pmatrix} 0 & a & b \\ 0 & 0 & a \cup b \\ 0 & a \cup b & 0 \end{pmatrix}$$

Macierz wyjść:

$$\mathbb{B} = \begin{pmatrix} a & b \\ 0 & a \cup b \\ a \cup b & 0 \end{pmatrix}$$

Mając obliczone $\mathbb{T}$ można było również obliczyć $\mathbb{R}$ jako iloczyn macierzy

$$\mathbb{R} = \mathbb{T}\,\mathbb{B} = \begin{pmatrix} e & aX^{2*} \cup bXX^{2*} & aX^{2*}X \cup bX^{2*} \\ 0 & X^{2*} & X^{2*}X \\ 0 & XX^{2*} & X^{2*} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & X \\ X & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} a \cup aX^{2*}X^2 \cup bX^{2*}X & b \cup aX^{2*}X \cup bXX^{2*}X \\ X^{2*}X^2 & X^{2*}X \\ X^{2*}X & XX^{2*}X \end{pmatrix} =$$

$$= \begin{pmatrix} aX^{2*} \cup bXX^{2*} & bX^{2*} \cup aXX^{2*} \\ X^2X^{2*} & XX^{2*} \\ XX^{2*} & X^2X^{2*} \end{pmatrix}$$

Z kolei $\mathbb{T}$ można było również obliczyć jako sumę wszystkich potęg $\mathbb{A}$.

$$\mathbb{A}^2 = \begin{pmatrix} 0 & a & b \\ 0 & 0 & X \\ 0 & X & 0 \end{pmatrix} \begin{pmatrix} 0 & a & b \\ 0 & 0 & X \\ 0 & X & 0 \end{pmatrix} = \begin{pmatrix} 0 & bX & aX \\ 0 & X^2 & 0 \\ 0 & 0 & X^2 \end{pmatrix},$$

$$\mathbb{A}^3 = \begin{pmatrix} 0 & a & b \\ 0 & 0 & X \\ 0 & X & 0 \end{pmatrix} \begin{pmatrix} 0 & bX & aX \\ 0 & X^2 & 0 \\ 0 & 0 & X^2 \end{pmatrix} = \begin{pmatrix} 0 & aX^2 & bX^2 \\ 0 & 0 & X^3 \\ 0 & X^3 & 0 \end{pmatrix} = \mathbb{A}\, X^2 ,$$

$$\mathbb{A}^4 = \mathbb{A}^2 X^2 ,$$

$$\mathbb{A}^5 = \mathbb{A}^3 X^2 = \mathbb{A}\, X^4 ,$$

$$\mathbb{A}^6 = \mathbb{A}^2 X^4$$

i ogólnie

$$\mathbb{A}^{2i+1} = \mathbb{A}\, X^{2i} ,$$

$$\mathbb{A}^{2i+2} = \mathbb{A}^2 X^{2i} \qquad \text{dla } i = 0, 1, 2, \ldots$$

Wobec tego

$$\mathbb{T} = \mathbb{e} \cup \bigcup_{i=0}^{\infty} \left(\mathbb{A}\, X^{2i} \cup \mathbb{A}^2 X^{2i} \right) = \mathbb{e} \cup \left(\mathbb{A} \cup \mathbb{A}^2 \right) X^{2*} =$$

$$= \mathbb{e} \cup \begin{pmatrix} 0 & a \cup bX & aX \cup b \\ 0 & X^2 & X \\ 0 & X & X^2 \end{pmatrix} X^{2*}$$

Identyczność pewnych kolumn macierzy, występujących przy obliczaniu $\mathbb{T}$ i $\mathbb{R}$ wynika ze sposobu określenia funkcji przejść i wyjść rozważanego automatu i w tym sensie jest całkowicie przypadkowa.

Koniec przykładu.

Wszystkie sposoby opisywania automatu skończonego $\{Q, X, Y, \delta, \lambda\}$, które rozważaliśmy dotychczas: tablica przejść i wyjść, tablica automatu, wykres Mealy'ego, graf przepływu, automat $\{Q, X^*, Y^*, \delta, \lambda\}$, automat $\{Q, X^*, Y_{uc}, \delta, \mu\}$, para macierzy $\mathbb{T}$, $\mathbb{R}$, para macierzy $\mathbb{A}$, $\mathbb{B}$ podawały lub pozwalały zawsze odtworzyć wszystkie jego elementy /co najwyżej mogło przy tym dojść do zmian oznaczeń elementów zbioru Q lub Y /.

Czasami rozważa się tylko zewnętrzne zachowanie automatu, to znaczy wyobrażamy sobie automat jako pewne urządzenie, w którym uwzględniamy tylko to, co da się stwierdzić przez obserwowanie ciągów sygnałów wejściowych i wyjściowych, bez zaglądania do środka urządzenia, bez badania stanów wewnętrznych i przejść między nimi. Robi się to wtedy, gdy takie "zajrzenie do środka" automatu jest niemożliwe, bądź jego wyniki nie byłyby dla nas interesujące. Takie sytuacje występują często nie tylko w badaniach teoretycznych, ale także w zastosowaniach. Typowym tego przykładem jest projektowanie urządzeń, które można traktować jako automaty /np. elektronicznych urządzeń liczących/. Założenia konstrukcyjne precyzują zazwyczaj tylko zewnętrzne zachowanie projektowanego urządzenia, a opracowanie jego budowy i szczegółów działania należy do projektanta.

Zachowanie automatu można opisywać przez podanie funkcji przyporządkowujących słowom wejściowym słowa wyjściowe /np. funkcję λ lub podobne/, albo przez podanie określonego przez automat przyporządkowania słowom wejściowym końcowych liter ich obrazów, albo przez podanie zbiorów niepustych słów wejściowych, których końcowe litery obrazów są jednakowe. Inaczej mówiąc, można traktować automat jako urządzenie przekształcające słowa wejściowe lub jako urządzenie, które je klasyfikuje. Przejście od jednego z wymienionych sposobów opisu zachowania do innego jest łatwe - wybiera się taki, który jest wygodniejszy w danej sytuacji.

W przeciwieństwie do wymienionych poprzednio form opisu automatu, które zawierają pełną informację o nim i pozwalają go jednoznacznie wyznaczyć, sam opis zachowania automatu bez dodatkowych informacji nie określa go jednoznacznie. Może istnieć wiele różnych automatów, których zewnętrzne zachowanie jest jednakowe. Bliższe zbadanie tego zagadnienia wymaga wprowadzenia pojęć homomorfizmu, izomorfizmu i nieodróżnialności automatów, co będzie tematem następnego rozdziału.

Wracając jeszcze do pełnych opisów automatów, sformułujemy wyraźnie własności T_{pq} i R_{pq} dla automatów skończonych. Otóż, jeśli Q, X, Y są skończone, to układy równań 5.12 i 5.13 są również skończone i spełniają warunki twierdzenia 4.2. Stąd:

Twierdzenie 5.1. Jeżeli automat jest skończony, to wszystkie jego zbiory T_{pq} i R_{py} są regularne.

6. NIEODRÓŻNIALNOŚĆ AUTOMATÓW I ICH UPRASZCZANIE

Weźmy dwa automaty /nie koniecznie różne/

$$\{Q_1, X, Y, \delta_1, \lambda_1\},$$

$$\{Q_2, X, Y, \delta_2, \lambda_2\}$$

mające wspólny alfabet wejściowy i wyjściowy. Możemy utworzyć rozszerzenie każdego z nich

$$\{Q_1, X^*, Y^*, \delta_1, \lambda_1\},$$

$$\{Q_2, X^*, Y^*, \delta_2, \lambda_2\}.$$

Stany $q_1 \in Q_1$ i $q_2 \in Q_2$ będziemy nazywać nieodróżnialnymi wtedy i tylko wtedy, gdy dla każdego słowa $s \in X^*$

$$\lambda_1(q_1, s) = \lambda_2(q_2, s).$$

Jeżeli będziemy uważać, że te automaty są pewnymi urządzeniami i będziemy przeprowadzać z nimi doświadczenia, polegające na podawaniu dowolnych słów wejściowych i odczytywaniu słów wyjściowych /bez możliwości odczytywania wartości stanów automatu/ tak, że na początku każdego z doświadczeń automaty te będą odpowiednio w stanie q_1 i q_2 i stany te będą nieodróżnialne w sensie podanej definicji, to sekwencje wyjściowe obu automatów będą w każdym doświadczeniu jednakowe. Nie mając żadnych innych informacji poza tymi sekwencjami nie będziemy mogli odróżnić jednego automatu od drugiego.

Relacja nieodróżnialności stanów jest równoważnością; jest zwrotna /każdy stan jest nieodróżnialny od samego siebie/, przechodnia /jeśli q_1 jest nieodróżnialny od q_2 i q_2 jest nieodróżnialny od q_3, to q_1 jest nieodróżnialny od q_3/ i symetryczna /jeśli q_1 jest nieodróżnialny od q_2, to q_2 jest nieodróżnialny od q_1 /.

<u>Twierdzenie 6.1.</u> Dla każdego automatu $\{Q, X, Y, \delta, \lambda\}$ i dla dowolnych $p \in Q$, $q \in Q$ następujące warunki są równoważne

1. p i q są nieodróżnialne ,
2. dla każdego $s \in X^*$ $\lambda(p,s) = \lambda(q,s)$,
3. dla każdego $s \in X^*$ $\mu(p,s) = \mu(q,s)$,
4. dla każdego $y \in Y$ $R_{py} = R_{qy}$,
5. dla każdego $x \in X$ $\lambda(p,x) = \lambda(q,x)$ i $\delta(p,x)$, $\delta(q,x)$ są nieodróżnialne.

Dowód:

1 i 2 są równoważne z definicji. Równoważność 2 i 3 wynika z wzoru, który jest bezpośrednią konsekwencją definicji funkcji μ oraz 5.5 i 5.8 /$\mu(p,s)$ oznacza, tak jak poprzednio, ostatnią literę słowa $\lambda(p,s)$, lub e, jeśli $s = e$/:

$\lambda(p,x_1x_2 \ldots x_m) = \mu(p,x_1)\mu(\delta(p,x_1),x_2) \ldots$
$\ldots\mu(\delta(p,x_1x_2 \ldots x_{m-1}),x_m)$, a dla dowolnych stanów p, q jest zawsze

$$\lambda(p,e) = \lambda(q,e) = \mu(p,e) = \mu(q,e) = e \quad .$$

Z tej ostatniej tożsamości korzystamy stale w dalszych krokach dowodu. Równoważność 3 i 4 opiera się na 5.11. Dalej, dowolne słowo niepuste $s \in XX^*$ można przedstawić jako $s = xt$, gdzie $x \in X$, $t \in X^*$ i wtedy

$$\lambda(p,s) = \lambda(p,xt) = \lambda(p,x)\lambda(\delta(p,x), t) \quad ,$$
$$\lambda(q,s) = \lambda(q,xt) = \lambda(q,x)\lambda(\delta(q,x), t) \quad .$$

Stąd równoważność 5.1 2.

Koniec dowodu.

Dwa automaty o wspólnym alfabecie wejściowym i wyjściowym nazywamy nieodróżnialnymi, o ile dla każdego stanu pierwszego automatu istnieje nieodróżnialny od niego stan drugiego automatu i odwrotnie.

W automatach ze stanem początkowym musi być oprócz tego spełniony warunek nieodróżnialności stanów początkowych. Nieodróżnialność stanów automatów ze stanem początkowym rozumie się tak samo, jak w przypadku automatów bez stanu początkowego.

Homomorfizmem automatu

$$\{Q_1, X, Y, \delta_1, \lambda_1\}$$

w /na/ automat

$$\{Q_2, X, Y, \delta_2, \lambda_2\}$$

nazywamy takie odwzorowanie h zbioru Q_1 w /na/ Q_2, że dla dowolnych $x \in X$, $q \in Q_1$

$$h(\delta_1(q,x)) = \delta_2(h(q), x), \qquad 6.1$$

$$\lambda_1(q,x) = \lambda_2(h(q), x). \qquad 6.2$$

Dla automatów ze stanem początkowym pojęcie homomorfizmu określa się podobnie, ale dodatkowo wymaga się, by obraz stanu początkowego był stanem początkowym.

Jeżeli A_1, A_2 są dowolnymi automatami /lub automatami ze stanem początkowym/, to mówimy, że A_2 jest obrazem homomorficznym A_1, wtedy i tylko wtedy, gdy istnieje homomorfizm A_1 na A_2.

Homomorfizm automatu $\{Q_1, X, Y, \delta_1, \lambda_1\}$ w /na/ automat $\{Q_2, X, Y, \delta_2, \lambda_2\}$ jest jednocześnie homomorfizmem automatu rozszerzonego $\{Q_1, X^*, Y^*, \delta_1, \lambda_1\}$ w /na/ automat $\{Q_2, X^*, Y^*, \delta_2, \lambda_2\}$ i homomorfizmem automatu $\{Q_1, X^*, Y \cup e, \delta_1, \mu_1\}$ w /na/ automat $\{Q_2, X^*, Y \cup e, \delta_2, \mu_2\}$. Odwrotnie, każde odwzorowanie, które jest homomorfizmem dla rozszerzeń automatów /jednego lub drugiego rodzaju, z funkcjami λ lub μ / jest jednocześnie homomorfizmem dla automatów, z których te rozszerzenia otrzymano. Można to uzasadnić, stosując indukcję względem długości słowa. Jeżeli dla słów jednoliterowych mamy 6.1 i 6.2, dla słów pustych jest zawsze /na mocy 5.6 i 5.7/

$$h(\delta_1(q,e)) = h(q) = \delta_2(h(q), e),$$
$$\lambda_1(q,e) = e = \lambda_2(h(q), e),$$
$$\mu_1(q,e) = e = \mu_2(h(q), e),$$

zaś dla dowolnych $t \in X^*$, $x \in X$ jest /na mocy 5.4, 5.5, 5.8, 5.9, 6.1, 6.2 i przesłanki indukcyjnej/

$$h(\delta_1(q,tx)) = h(\delta_1(\delta_1(q,t),x)) = \delta_2(h(\delta_1(q,t)),x) =$$
$$= \delta_2(\delta_2(h(q),t),x) = \delta_2(h(q),tx),$$

$$\lambda_1(q,tx) = \lambda_1(q,t)\lambda_1(\delta_1(q,t),x) =$$
$$= \lambda_2(h(q),t)\lambda_2(h(\delta_1(q,t)),x) =$$
$$= \lambda_2(h(q),t)\lambda_2(\delta_2(h(q),t),x) = \lambda_2(h(q),tx),$$

$$\mu_1(q,tx) = \mu_1(\delta_1(q,t),x) = \lambda_1(\delta_1(q,t),x) =$$
$$= \lambda_2(h(\delta_1(q,t)),x) = \lambda_2(\delta_2(h(q),t),x) =$$
$$= \mu_2(\delta_2(h(q),t),x) = \mu_2(h(q),tx).$$

Stąd, jeżeli 6.1 i 6.2, to dla dowolnych $s \in X^*$, $q \in Q_1$ jest

$$(h_1(q,s)) = \delta_2(h(q,s)), \qquad 6.3$$
$$\lambda_1(q,s) = \lambda_2(h(q),s), \qquad 6.4$$
$$\mu_1(q,s) = \mu_2(h(q),s) \qquad 6.5$$

i odwrotnie: 6.1 i 6.2 można otrzymać, podstawiając do tych wzorów słowa jednoliterowe.

Z wzoru 6.4 widać, że jeśli h jest homomorfizmem, to stany q i $h(q)$ są nieodróżnialne. Wobec tego, jeżeli homomorfizm odwzorowuje jeden automat na drugi, to te automaty są nieodróżnialne.

Wzajemnie jednoznaczny homomorfizm nazywamy izomorfizmem.

Dwa automaty nazywamy izomorficznymi, jeżeli istnieje izomorfizm, odwzorowujący jeden automat na drugi /tzn. odwzorowujący zbiór stanów jednego automatu na zbiór stanów drugiego/. Taki izomorfizm jednego automatu na drugi jest po prostu przemianowaniem stanów i tej nazwy też będziemy w przyszłości używać.

Twierdzenie 6.2. Dla każdego automatu $A = \{Q, X, Y, \delta, \lambda\}$ istnieje jeden i tylko jeden /z dokładnością do przemianowania stanów/ automat $A' = \{Q', X, Y, \delta', \lambda'\}$ taki, że wszystkie jego stany są parami odróżnialne /tzn. nie ma dwu różnych stanów nieodróżnialnych/ i dla każdego automatu B nieodróżnialnego od A istnieje homorfizm, odwzorowujący B na A'.

Dowód:

Nieodróżnialność stanów jest równoważnością, a więc wyznacza podział zbioru Q na klasy abstrakcji, które będziemy nazywać klasami nieodróżnialności automatu A.

Niech Q' będzie zbiorem wszystkich takich klas. Dla każdego $x \in X$ i dla każdej klasy nieodróżnialności $K \in Q'$ istnieje jedna i tylko jedna klasa $L \in Q'$ taka, że dla każdego $k \in K$ $\delta(k,x) \in L$. Przyjmujemy

$$\delta'(K,x) = L ,$$
$$\lambda'(K,x) = \lambda(k,x) ,$$

gdzie k jest dowolnym elementem klasy K - wobec nieodróżnialności wszystkich elementów K wartość $\lambda'(K,x)$ nie zależy od wyboru tego elementu.

Jeżeli weźmiemy rozszerzenia λ i λ' na zbiór wszystkich słów, to jak wynika z określenia λ', dla każdego $s \in X^*$ i dla dowolnych $K \in Q'$, $k \in K$ $\lambda'(K,s) = \lambda(k,s)$. Jeśli $K \in Q'$, $L \in Q'$, $K \neq L$ i $k \in K$, $l \in L$, to k i l są odróżnialne, czyli istnieje takie słowo $s \in X^*$, że

$$\lambda'(K,s) = \lambda(k,s) \neq \lambda(l,s) = \lambda'(L,s)$$

a więc stany automatu A' są parami odróżnialne.

Funkcja h, odwzorowująca każdy stan automatu A na jego klasę nieodróżnialności, jest homomorfizmem A na A'. Niech teraz B będzie dowolnym automatem, nieodróżnialnym od A. Oznaczmy zbiór jego stanów przez Q_B, a jego funkcje przejść

i wyjść odpowiednio przez δ_B, λ_B. Dla każdego stanu $b \in Q_B$ istnieje nieodróżnialny od niego stan $K \in Q'$. Stan taki jest tylko jeden i możemy przyjąć $h(b) = K$, określając w ten sposób odwzorowanie zbioru stanów automatu B na zbiór Q'. Z nieodróżnialności b i $h(b)$ wynika, że dla każdego $x \in X$ $\delta_B(b,x)$ i $\delta'(h(b), x)$ są też nieodróżnialne, czyli

$$h(\delta_B(b,x)) = \delta'(h(b), x),$$

a bezpośrednio z nieodróżnialności b od $h(b)$ wynika

$$\lambda_B(b,x) = \lambda'(h(b), x).$$

Zatem h jest homomorfizmem B na A'.

Koniec dowodu.

Wniosek 6.3. Warunkiem koniecznym i dostatecznym nieodróżnialności dwu automatów jest istnienie automatu, który jest obrazem homomorficznym każdego z nich.

Wniosek 6.4. W klasie wszystkich automatów, nieodróżnialnych od dowolnego automatu A istnieje jeden i tylko jeden /z dokładnością do przemianowania stanów/ automat taki, że moc zbioru jego stanów jest mniejsza od mocy zbioru stanów dowolnego automatu, który należy do tej samej klasy i nie jest z nim izomorficzny.

Korzystając z pojęcia homomorfizmu, możemy dla każdego automatu $A = \{Q, X, Y, \delta, \lambda\}$ zbudować nieodróżnialny od niego automat o mocy zbioru stanów równej $\overline{\overline{Q}} \cdot \overline{\overline{X^*}}$ /gdzie $\overline{\overline{S}}$ oznacza moc zbioru S /; w szczególności dla każdego automatu skończonego można zbudować nieodróżnialny od niego automat nieskończony. Jest to $\hat{A} = \{QX^*, X, Y, \hat{\delta}, \hat{\lambda}\}$. Stanami tego automatu są słowa postaci qs, gdzie $q \in Q$, $s \in X^*$, zaś funkcje $\hat{\delta}$ i $\hat{\lambda}$ są określone w następujący sposób: dla dowolnych $q \in Q$, $s \in X^*$, $x \in X$

$$\hat{\delta}(qs,x) = qsx, \qquad 6.6$$

$$\hat{\lambda}(qs,x) = \mu(q,sx). \qquad 6.7$$

Jeżeli przyjmiemy, że

$$h(qs) = \delta(q,s) \qquad 6.8$$

dla dowolnych $q \in Q$, $s \in X^*$, to h będzie homomorfizmem, odwzorowującym QX^* na Q, a zatem A i $\hat{A}$ są nieodróżnialne. Można przy okazji zauważyć, że $\hat{\hat{A}} = \hat{A}$, bo $QX^*X^* = QX^*$.

Opisana tu konstrukcja automatu przy pomocy operacji $\hat{}$ jest interesująca dlatego, że pozwala w każdym przypadku sprowadzić funkcję δ do złożenia, dzięki czemu badanie przynajmniej niektórych własności automatów można sprowadzić do odpowiednich rozważań teorii półgrup. Sama możliwość powiększenia mocy zbioru stanów jest oczywiście mniej istotna: mając dowolny automat $A = \{Q, X, Y, \delta, \lambda\}$ i dowolny zbiór M o mocy większej od mocy Q, możemy wziąć jakiekolwiek odwzorowanie h zbioru M na Q i utworzyć automat $\{M, X, Y, \delta_M, \lambda_M\}$, w którym δ_M i λ_M będą tak dobrane, żeby h było homomorfizmem, zgodnie z wzorami 6.1 i 6.2.

Jak widać z przytoczonego poprzednio wywodu automat A można otrzymać z $\hat{A}$, stosując homomorfizm h związany z rozszerzoną funkcją przejść automatu A. Interesujący wynik może również dać wprowadzenie odwzorowania automatu $\hat{A}$ na inny automat przy pomocy innego homomorfizmu związanego z rozszerzoną funkcją wyjść automatu A.

Funkcja λ określa w automacie A odwzorowanie zbioru X^* w Y^*, zależne od dodatkowego parametru, jakim jest stan automatu. Dla każdego $q \in Q$ można wprowadzić funkcję $\varphi_q: X^* \to Y^*$, rozumiejąc to oznaczenie w następujący sposób: dla każdego $q \in Q$ i każdego $t \in X^*$

$$\varphi_q(t) = \lambda(q, t) \quad . \qquad 6.9$$

Uogólniając ten zapis, możemy przyjąć, że dla dowolnych $q \in Q$, $s \in X^*$, $t \in X^*$

$$\varphi_{qs}(t) = \lambda(\delta(q, s), t) \quad . \qquad 6.10$$

Ponieważ dla każdego $r \in QX^*$ jest $h(r) \in Q$, przyjęcie 6.10 jest równoważne z przyjęciem tożsamości $\varphi_r(t) = \varphi_{h(r)}(t)$ dla każdego $t \in X^*$, czyli krócej

$$\varphi_r = \varphi_{h(r)} \qquad 6.11$$

dla każdego $r \in QX^*$.

Weźmy teraz funkcję g, określoną na zbiorze QX^*

$$g(r) = \varphi_r \qquad 6.12$$

i utwórzmy automat $\hat{A}' = \{\hat{Q}', X, Y, \hat{\delta}', \hat{\lambda}'\}$ tak, żeby on był homomorficznym obrazem automatu $\hat{A}$, otrzymanym za pomocą odwzorowania g. Powinno więc być

$$\hat{Q}' = \{\varphi_r\} \; r \in QX^*$$

oraz dla dowolnych $r \in QX^*$, $x \in X$

$$\hat{\delta}'(\varphi_r, x) = \varphi_{\hat{\delta}(r,x)} ,$$

$$\hat{\lambda}'(\varphi_r, x) = \hat{\lambda}(r,x) .$$

Ale, na mocy 6.7, 5.8, 5.9, 6.10 dla dowolnych $q \in Q$, $s \in X^*$, $x \in X$ $\hat{\lambda}(qs, x) = \mu(q, sx) = \mu(\delta(q,s), x) = \lambda(\delta(q,s), x) = \varphi_{qs}(x)$. Wobec tego

$$\hat{\delta}'(\varphi_r, x) = \varphi_{rx} , \qquad 6.13$$

$$\hat{\lambda}'(\varphi_r, x) = \varphi_r(x) . \qquad 6.14$$

Aby automat $\hat{A}'$ był dobrze określony potrzeba /i wystarcza/ aby tak wprowadzone $\hat{\delta}'$, $\hat{\lambda}'$ były funkcjami. Że tak jest, Czytelnik może się o tym przekonać, korzystając z 6.11 i 6.8, 6.9.

Z 6.11 widać, że dla każdego $r \in QX^*$ istnieje taki $q \in Q$, że $\varphi_r = \varphi_q$. Z 6.9 wynika, że dla dowolnych $p \in Q$ oraz $q \in Q$ $\varphi_p = \varphi_q$ wtedy i tylko wtedy, gdy $\lambda(p,t) = \lambda(q,t)$

dla każdego $t \in X^*$, czyli, inaczej mówiąc, wtedy i tylko wtedy, gdy stany p i q są nieodróżnialne. Zatem zbiór $\hat{Q}'$ jest równoliczny ze zbiorem wszystkich klas nieodróżnialności automatu A. Ze sposobu wyprowadzenia automatów A', $\hat{A}$, $\hat{A}'$ przez homomorfizmy wynika, że wszystkie one, razem z A, należą do tej samej klasy automatów nieodróżnialnych. Z równoliczności $\hat{Q}'$ i Q' oraz z twierdzenia 6.2 wynika, że automaty $\hat{A}'$ i A' są izomorficzne. Różnią się one tylko tym, że stany A' są klasami równoważności, zaś stany $\hat{A}'$ są odwzorowaniami zbioru X^* w Y^*.

Korzystając z 6.11, możemy zapisać 6.13 i 6.14 w inny sposób: dla dowolnych $x \in X$, $q \in Q'$

$$\hat{\delta}'(\varphi_q, x) = \varphi_{\delta(q,x)}, \qquad 6.15$$

$$\hat{\lambda}'(\varphi_q, x) = \varphi_q(x). \qquad 6.16$$

Tą drogą otrzymaliśmy także homomorfizm automatu A na $\hat{A}'$. Funkcję $\varphi_{\delta(q,x)}$ można wyznaczyć z funkcji φ_q, korzystając z tego, że dla dowolnych $s \in X^*$, $q \in Q$, $x \in X$

$$\varphi_{\delta(q,x)}(s) = \varphi_q(xs) /\!/ \varphi_q(x) \qquad 6.17$$

- zależność ta wynika z 6.9, 6.10 i 5.5.

Obraz nie zmieni się zasadniczo, jeżeli zamiast funkcji $\varphi_q: X^* \to Y^*$ wprowadzimy funkcje $\psi_q: X^* \to Y \cup e$, określone w następujący sposób: dla każdego $t \in X^*$

$$\psi_q(t) = \mu(q, t) \qquad 6.18$$

i dla dowolnego $r \in QX^*$ przyjmiemy

$$\psi_r = \psi_{h(r)}. \qquad 6.19$$

Ponieważ w każdym automacie funkcja φ określa jednoznacznie funkcję ψ i odwrotnie, istnieje wzajemnie jednoznaczne przyporządkowanie elementów zbioru $\{\psi_r\}_{r \in QX^*}$ elementom $\{\varphi_r\}_{r \in QX^*}$.

Powtarzając całe wyprowadzenie automatu $\hat{A}$, ale z jednoczesnym zastąpieniem φ przez ψ, otrzymamy nowy automat, którego zbiorem stanów będzie $\{\psi_r\}_{r \in QX^*} = \{\psi_q\}_{q \in Q}$, izomorficzny z $\hat{A}'$ i A'. Poważniejsza różnica będzie tylko we wzorze na obliczanie $\psi_{\delta(q,x)}$: zamiast zależności, analogicznej do 6.17 mamy

$$\psi_{\delta(q,x)}(s) = \psi_q(xs) \qquad 6.20$$

dla dowolnych $q \in Q$, $x \in X$, $s \in XX^*$. Wynika to z 6.18 i 5.8.

Mając dany automat A i jego funkcję μ, możemy sobie wyznaczyć zbiory R_{qy}, zgodnie z 5.11. Wprowadźmy funkcje ρ_q, $q \in Q$ odwzorowujące Y w rodzinę wszystkich zdarzeń w alfabecie X

$$\rho_q(y) = R_{qy} . \qquad 6.21$$

Zmieniając w 5.11 oznaczenia, otrzymujemy

$$\rho_q(y) = \{s \in X^* : \psi_q(s) = y\} .$$

Ogólniej, przyjmiemy, że dla każdego $r \in QX^*$

$$\rho_r(y) = \{s \in X^* : \psi_r(s) = y\} ,$$

czyli

$$\rho_r = \rho_{h(r)} . \qquad 6.22$$

I znowu, jak poprzednio, możemy skonstruować automat, którego stanami będą wszystkie funkcje ρ_r i który jest obrazem homomorficznym $\hat{A}$. Aby tak było, funkcja przejść δ_ρ i funkcja wyjść tego automatu λ_ρ muszą spełniać warunki

$$\delta_\rho(\rho_r, x) = \rho_{\hat{\delta}(r,x)} = \rho_{rx} , \qquad 6.23$$
$$\lambda_\rho(\rho_r, x) = \hat{\lambda}(r, x) = \psi_r(x) . \qquad 6.24$$

Wobec 6.22 jest $\{\rho_r\}_{r \in QX^*} = \{\rho_q\}_{q \in Q}$; jeżeli zechcemy ograniczyć się tylko do zależności dla ρ_q, $q \in Q$, to otrzymamy

$$\delta_\varrho(\varrho_q, x) = \varrho_{\delta(q,x)}, \qquad 6.25$$

$$\lambda_\varrho(\varrho_q, x) = \mu(q, x). \qquad 6.26$$

Jak wynika z 5.16 i 5.18, znając ϱ_q można obliczyć $\varrho_{\delta(q,x)}$; dla dowolnych $q \in Q$, $x \in X$, $y \in Y$

$$\varrho_{\delta(q,x)}(y) = \varrho_q(y)/\!/x - \varepsilon(\varrho_q(y)/\!/x). \qquad 6.26$$

Jeżeli zbiór Y jest skończony lub przeliczalny, to zakładając, że jego elementy są w jakiś sposób ponumerowane, możemy dla każdego $q \in Q$ utworzyć ciąg /skończony lub nie/

$$\overline{R}_q = R_{qy1}, R_{qy2}, \ldots$$

Taki ciąg jest też swego rodzaju zapisem funkcji ϱ_q, a więc w tym przypadku możemy napisać

$$\delta_\varrho(\overline{R}_q, x) = \overline{R}_{\delta(q,x)}, \qquad 6.27$$

$$\lambda_\varrho(\overline{R}_q, x) = \mu(q, x). \qquad 6.28$$

Znając ϱ_q lub $\overline{R}_q$, można wyznaczyć wartość $\mu(q,x)$: jest to taki $y \in Y$, że $x \in \varrho_q(y) = R_{qy}$, czyli $\varepsilon(R_{qy}/\!/x) = e$.

Jak widać z tych rozważań, automat o alfabecie wejściowym X i alfabecie wyjściowym Y, który spośród wszystkich nieodróżnialnych od niego automatów ma najmniej stanów, może być przedstawiany rozmaicie: jego stanami mogą być klasy nieodróżnialności, odwzorowania X^* w Y^*, odwzorowania X^* w $Y \cup e$, albo odwzorowania Y w rodzinę wszystkich podzbiorów X^*. Stosownie do tego wyznacza się jego funkcje przejść i wyjść. W praktycznych obliczeniach można, zależnie od potrzeby, posługiwać się tym lub innym przedstawieniem. Chociaż z teoretycznego punktu widzenia nie jest istotne, który z izomorficznych automatów sobie wybierzemy, bo zawsze dochodzi

się do tej samej - z dokładnością do oznaczeń stanów - tablicy automatu, praktycznie nie jest obojętne, jaką metodą go obliczymy.

Przykład:

Dwa stany automatu są oznaczone odpowiednio 1 i 2 . Jego alfabetem wejściowym i wyjściowym jest zbiór $\{a, b\}$. Zaczynając działanie w stanie 1, automat przepuszcza słowa bez zmian, to znaczy słowo wyjściowe jest wtedy zawsze równe słowu wejściowemu. Jeżeli jego działanie zaczyna się od stanu 2 i na początku słowa wejściowego występuje sekwencja liter a , to wszystkie one zostają zamienione na b . Pierwsza litera b w słowie wejściowym /o ile wogóle jest/, zostaje zamieniona na literę a i wtedy dalsza część tego słowa przechodzi przez automat bez zmian. Inaczej mówiąc

$$\lambda(1, s) = s \quad ,$$
$$\lambda(2, a^i) = b^i \quad ,$$
$$\lambda(2, a^i bs) = b^i as$$

dla dowolnego $s \in X^*$ i dowolnej liczby naturalnej $i \geqslant 0$. Należy obliczyć funkcję przejść.

Mając zadane w ten sposób funkcje φ_1 , φ_2 , możemy wyznaczyć φ_{1a}, φ_{1b}, φ_{2a}, φ_{2b} i tak dalej, w myśl 6.13. Skorzystajmy z 6.17.

$$\varphi_{1a}(s) = \varphi_1(as) /\!/ \varphi_1(a) = as /\!/ a = s \quad ,$$
$$\varphi_{1b}(s) = \varphi_1(bs) /\!/ \varphi_1(b) = bs /\!/ b = s \quad ,$$

czyli

$$\varphi_{1a} = \varphi_{1b} = \varphi_1 \quad ,$$
$$\varphi_{2a}(s) = \varphi_2(as) /\!/ \varphi_2(a) \quad .$$

Aby móc to dokładniej obliczyć, trzeba rozważyć dwa przypadki: gdy s nie zawiera żadnej litery b i gdy zawiera przynajmniej jedną.

$$\varphi_{2a}(a^i) = \varphi_2(a^{i+1}) /\!/ \varphi_2(a) = b^{i+1} /\!/ b = b^i ,$$

$$\varphi_{2a}(a^i bs) = \varphi_2(a^{i+1} bs) /\!/ \varphi_2(a) = b^{i+1} as /\!/ b = b^i as ,$$

czyli

$$\varphi_{2a} = \varphi_2 .$$

$$\varphi_{2b}(a^i) = \varphi_2(ba^i) /\!/ \varphi_2(b) = aa^i /\!/ a = a^i ,$$

$$\varphi_{2b}(a^i bs) = \varphi_2(ba^i bs) /\!/ \varphi_2(b) = aa^i bs /\!/ a = a^i bs ,$$

czyli

$$\varphi_{2b} = \varphi_1 .$$

Tablica przejść, utworzona zgodnie z 6.13:

	a	b
φ_1	φ_1	φ_1
φ_2	φ_2	φ_1

Można ją zapisać nieco prościej

	a	b
1	1	1
2	2	1

Tablica wyjść:

	a	b
1	a	b
2	b	a

Koniec przykładu.

Przykład:

Zbiorem stanów automatu i jego alfabetem wejściowym jest zbiór wszystkich liczb naturalnych /z zerem włącznie/.

Alfabetem wyjściowym jest zbiór $\{0, 1\}$. Dla dowolnego słowa wejściowego s i dowolnego stanu q $\mu(q,s) = 1$ wtedy i tylko wtedy, gdy suma q i wszystkich liczb, występujących w słowie s, jest podzielna przez 2 lub przez 3. W przeciwnym razie $\mu(q,s) = 0$. Trzeba znaleźć dowolny automat, który byłby nieodróżnialny od tego automatu.

Obliczymy rozwiązanie o najmniejszej możliwej ilości stanów. Jak wynika z warunków zadania dla dowolnej liczby naturalnej q

$$\varphi_q = \varphi_{q+6} = \varphi_{q+12} = \ldots$$

i wartość $\varphi_q(s)$ nie zmieni się, jeżeli zastąpimy dowolną liczbę w słowie s liczbą naturalną, różniącą się od niej o wielokrotność 6. Można więc rozważać tylko słowa wejściowe, zbudowane z liczb 0, 1, 2, 3, 4, 5, gdyż wszystkie pozostałe dadzą się do nich sprowadzić bez zmiany wartości funkcji . Można także ograniczyć się tylko do badania funkcji φ_q dla $0 \leqslant q \leqslant 5$. Funkcje te są parami różne, ponieważ zawsze da się tak dobrać liczbę x z przedziału $[0, 5]$, że dla dwu różnych liczb p, q z tego samego przedziału jest $\varphi_p(x) \neq \varphi_q(x)$. Stąd i z warunków zadania otrzymujemy tablicę szukanego automatu /dla prostoty zapisu zamiast symboli funkcji piszemy tylko ich wskaźniki/.

	0	1	2	3	4	5		
0	0:1	1:0	2:1	3:1	4:1	5:0	...	
1	1:0	2:1	3:1	4:1	5:0	0:1	...	i tak dalej
2	2:1	3:1	4:1	5:0	0:1	1:0	...	okresowo
3	3:1	4:1	5:0	0:1	1:0	2:1	...	po 6 kolumn
4	4:1	5:0	0:1	1:0	2:1	3:1	...	
5	5:0	0:1	1:0	2:1	3:1	4:1	...	

Przy tych oznaczeniach funkcja przejść jest po prostu dodawaniem modulo 6. Nietrudno zauważyć, że rozszerzając ten

automat przy pomocy operacji $\hat{}$ opisanej wyżej, otrzymalibyśmy /przy odpowiednich oznaczeniach stanów/ automat, w którym funkcja przejść byłaby zwykłym dodawaniem liczb.

Koniec przykładu.

Przykład:

Alfabetem wejściowym automatu jest zbiór $X = \{a, b\}$, alfabetem wyjściowym $Y = \{y_1, y_2\}$. Na wyjściu automatu ukazuje się y_1 wtedy, gdy na jego wejście było podane słowo zaczynające się i kończące literą a i automat był przedtem w stanie 1 lub gdy na wejście było podane słowo zawierające przynajmniej jedną literę a i automat był przedtem w stanie 2. We wszystkich pozostałych przypadkach na wyjściu jest y_2 /lub praca automatu zaczyna się od innego stanu/.

$$R_{1y_1} = a \cup aX^*a ,$$

$$R_{1y_2} = -\left(R_{1y_1} \cup e\right) ,$$

$$R_{2y_1} = X^*aX^* ,$$

$$R_{2y_2} = -\left(R_{2y_1} \cup e\right) ,$$

czyli

$$\overline{R}_1 = \left(a \cup aX^*a , -\left(a \cup aX^*a \cup e\right)\right) ,$$

$$\overline{R}_2 = \left(X^*aX^* , -\left(X^*aX^* \cup e\right)\right) .$$

Aby wyznaczyć funkcję przejść automatu, musimy, zgodnie z 6.26, obliczać ilorazy $\overline{R}_q // x$ dla różnych liter x. W naszym przypadku, ponieważ drugi element $\overline{R}_q$ jest zawsze uzupełnieniem pierwszego do zbioru wszystkich słów niepustych, wystarczy obliczać tylko ilorazy pierwszych elementów i brać później ich uzupełnienia. Obliczmy wobec tego wszystkie ilorazy charakterystyczne zdarzeń $S = a \cup aX^*a$ i $T = X^*aX^*$ oraz wartości ε dla tych ilorazów.

$$S /\!/ a = e \cup X^* a \;, \qquad \varepsilon(S /\!/ a) = e \;,$$
$$S /\!/ b = 0 \;, \qquad \varepsilon(S /\!/ b) = 0 \;,$$
$$S /\!/ aa = X^* a \cup e = S /\!/ a \;, \qquad \varepsilon(S /\!/ aa) = e \;,$$
$$S /\!/ ab = X^* a = S /\!/ a - e \;, \qquad \varepsilon(S /\!/ ab) = 0 \;,$$
$$S /\!/ ba = S /\!/ bb = 0 = S /\!/ b, \quad \varepsilon(S /\!/ ba) = \varepsilon(S /\!/ bb) = 0 \;.$$

$$T /\!/ a = X^* a X^* \cup X^* = X^* \;, \qquad \varepsilon(T /\!/ a) = e \;,$$
$$T /\!/ b = X^* a X^* = T \;, \qquad \varepsilon(T /\!/ b) = 0 \;,$$
$$T /\!/ aa = X^* = T /\!/ a \;, \qquad \varepsilon(T /\!/ aa) = e \;,$$
$$T /\!/ ab = X^* = T /\!/ b \;, \qquad \varepsilon(T /\!/ ab) = e \;,$$

Tablica przejść:

	a	b
$(S, -(S \cup e))$	$(S /\!/ a - e, -S /\!/ a)$	$(0, -e)$
$(T, -(T \cup e))$	$(XX^*, 0)$	$(T, -(T \cup e))$
$(S /\!/ a - e, -S /\!/ a)$	$(S /\!/ a - e, -S /\!/ a)$	$(S /\!/ a - e, -S /\!/ a)$
$(0, -e)$	$(0, -e)$	$(0, -e)$
$(XX^*, 0)$	$(XX^*, 0)$	$(XX^*, 0)$

Oczywiście można by zastosować bardziej jednolity zapis, zauważywszy np, że $XX^* = -e$, jednakże nie jest to w tym przypadku istotne. Tablicę wyjść obliczamy, korzystając z poprzednio obliczonych wartości funkcji ε dla ilorazów S i T /por. uwagę po wzorze 6.28/:

	a	b
$(S, -(S \cup e))$	y_1	y_2
$(T, -(T \cup e))$	y_1	y_2
$(S /\!/ a - e, -S /\!/ a)$	y_1	y_2
$(0, -e)$	y_2	y_2
$(XX^*, 0)$	y_1	y_1

Przemianowując stany i łącząc obie tablice w jedną otrzymamy:

	a	b
1	3: y_1	4: y_2
2	5: y_1	2: y_2
3	3: y_1	3: y_2
4	4: y_2	4: y_2
5	5: y_1	5: y_1

Koniec przykładu.

Wróćmy jeszcze raz do twierdzenia 6.2. Mówi ono o upraszczaniu automatu - w szczególności automatu skończonego - zajmijmy się teraz czysto techniczną stroną upraszczania właśnie dla tego przypadku.

Przyjmijmy, że automat jest zadany swoją tablicą i że stany jego są oznaczone kolejnymi liczbami naturalnymi $1,2,\ldots,n$. Opisywany algorytm składa się z następujących kroków.

Narysować kwadratową tablicę o wymiarach $n \times n$ i odrzucić wszystkie pola na głównej przekątnej i ponad nią.

Wpisać X na przecięciu każdego wiersza i oraz kolumny j, dla których istnieje taki stan wejścia x, że $\lambda(i,x) \neq \lambda(j,x)$, gdzie λ jest funkcją wyjść tego automatu.

W polach, w których nie ma X, wpisać na przecięciu i-wiersza i j-kolumny wszystkie pary $\delta(i,x)$, $\delta(j,x)$, gdzie x jest elementem alfabetu wejściowego, z tym że nie warto powtarzać par jednakowych lub różniących się tylko kolejnością elementów, a także nie warto wpisywać par i,j oraz j,i oraz takich, których oba elementy są jednakowe.

Jeżeli po wykonaniu tych czynności pozostaną jeszcze w tablicy wolne miejsca, wpisać w nich znak V. Następnie w polach, w których nie ma X ani V wpisywać znak X wszędzie

tam, gdzie jest wpisana para i,j taka, że na przecięciu i-wiersza i j-kolumny jest X . Czynność tę powtarzać dopóty, dopóki nie będzie można już wpisać żadnego nowego X .

W rezultacie otrzymamy tablicę nieodróżnialności stanów upraszczanego automatu, w której X oznacza 0 , zaś brak X oznacza 1 . Mając tę tablicę, możemy utworzyć zbiór stanów automatu uproszczonego /stany te odpowiadają klasom nieodróżnialności/, a następnie wyznaczyć jego funkcję przejść i wyjść tak, jak to jest opisane w dowodzie twierdzenia 6.2.

Przykład:

Uprościć automat:

	a	b
1	1,0	3,1
2	4,0	3,1
3	5,0	6,0
4	2,0	6,1
5	7,0	8,0
6	7,0	3,0
7	5,0	8,0
8	2,0	1,0

Tablica:

1								
2	14							
3	X	X						
4	12 36	36	X					
5	X	X	57 68	X				
6	X	X	57	X	38			
7	X	X	68	X	V	57 38		
8	X	X	25 16	X	27 18	27 13	25 18	
	1	2	3	4	5	6	7	8

Dopisanie X :

1								
2	14							
3	X	X						
4	12 36	36	X					
5	X	X	57 68	X				
6	X	X	57	X	38			
7	X	X	68	X	V	57 38		
8	X	X	25X 16	X	27X 18	27X 13	25X 18	
	1	2	3	4	5	6	7	8

Dopisanie X jeszcze raz:

1								
2	14							
3	X	X						
4	12 36	36	X					
5	X	X	57 68X	X				
6	X	X	57	X	38X			
7	X	X	68X	X	V	57 38X		
8	X	X	X	X	X	X	X	
	1	2	3	4	5	6	7	8

Dalej już X nie można dopisać. Automat uproszczony:

	a	b
124	124,0	36,1
36	57,0	36,0
57	57,0	8,0
8	124,0	124,0

Możemy w nim przemianować stany

	a	b
1	1,0	2,1
2	3,0	2,0
3	3,0	4,0
4	1,0	1,0

Koniec przykładu.

7. OBLICZANIE AUTOMATÓW NA PODSTAWIE ICH ZACHOWANIA

Zachowanie automatu może być opisane przez podanie odpowiedniości pomiędzy słowami wejściowymi i wyjściowymi lub pomiędzy słowami wejściowymi i końcowymi literami słów wyjściowych, albo przez podanie wszystkich zbiorów słów wejściowych, które ten automat jednakowo klasyfikuje, przyporządkowując im słowa wyjściowe o jednakowych literach końcowych. Zależnie od formy opisu mamy do czynienia z funkcjami φ, ψ lub ϱ takimi, jakie były opisane w poprzednim rozdziale. Omawiane w nim zadanie wyznaczania automatu, nieodróżnialnego od danego automatu o znanym zachowaniu, miało zawsze rozwiązanie, ponieważ mieliśmy do czynienia z opisem zachowania automatu już istniejącego. Jak przekonamy się niżej, istnieją odwzorowania φ zbioru wszystkich słów w alfabecie X w zbiór wszystkich słów w alfabecie Y takie, że nie istnieje automat, dla którego X byłby alfabetem wejściowym, Y alfabetem wyjściowym, zaś φ odpowiedniością między słowami wejściowymi i wyjściowymi. Powstaje więc pytanie, jakie warunki muszą spełniać funkcje φ, ψ, ϱ, ażeby istniał automat, dla którego takie funkcje byłyby opisem jego zachowania.

Nazwijmy funkcją sekwencyjną dowolną funkcję φ odwzorowującą zbiór wszystkich słów w alfabecie X w zbiór słów w alfabecie Y, która spełnia następujące warunki: dla dowolnych $s \in X^*$, $t \in X^*$

$$l(\varphi(s) = l(s)), \qquad 7.1.$$

$$\text{istnieje} \quad u \in Y^* \text{ taki, że } \varphi(st) = \varphi(s)\,u\,. \qquad 7.2.$$

przy czym $l(s)$ oznacza tu długość słowa s.

<u>Lemat 7.1.</u> Jeżeli X, Y są zbiorami niepustymi, to $\varphi : X^* \to Y^*$ jest funkcją sekwencyjną wtedy i tylko wtedy, gdy spełnia jednocześnie warunki

$$\varphi(e) = e\,, \qquad 7.3.$$

dla każdego $s \in X^*$ i każdego $x \in X$ istnieje $y \in Y$ taki, że

$$\varphi(sx) = \varphi(s)\, y \quad . \qquad 7.4$$

Dowód:

Z 7.1 wynika $l(\varphi(e)) = l(e) = 0$ i 7.3, a także $l(\varphi(sx)) = l(sx) = l(s) + l(x) = l(\varphi(s)) + 1$. Wobec 7.2 dla dowolnych $s \in X^*$, $x \in X$ istnieje $u \in Y^*$ taki, że $\varphi(sx) = \varphi(s)u$, ale $l(\varphi(sx)) = l(\varphi(s)) + l(u)$ i stąd $l(u) = 1$, czyli $u \in Y$ i 7.4.

Odwrotnie, z 7.4 wynika 7.2, a 7.1 można wyprowadzić z 7.3 i 7.4 przez indukcję względem długości słowa.

Koniec dowodu.

Warto zauważyć, że w tym lemacie nie można osłabić 7.4, zastępując go przez 7.2. Jako przykład może służyć funkcja $\varphi(s) = a^{2l(s)}$, gdzie a jest ustalonym elementem Y . Mamy $\varphi(e) = a^0 = e$ oraz $\varphi(st) = a^{2l(st)} = a^{2l(s) + 2l(t)} = \varphi(s)a^{2l(t)}$, ale $l(\varphi(s)) = 2l(s) \neq l(s)$ dla $s \neq e$.

Zauważmy też, że warunek 7.2 jest równoważny warunkowi: dla dowolnych $s \in X^*$, $t \in X^*$

$$\varphi(st) \,/\!/\, \varphi(s) \neq 0 \quad ,$$

czyli

$$\varphi(st) \,/\!/\, \varphi(s) \in Y^* \qquad 7.5$$

i analogicznie dla dowolnych $s \in X^*$, $x \in X$ zachodzi

$$\varphi(sx) \,/\!/\, \varphi(s) \in Y \quad , \qquad 7.6$$

wtedy i tylko wtedy, gdy 7.4.

Weźmy dowolny automat $\{Q, X, Y, \delta, \lambda\}$ i funkcje φ_q, określone zgodnie z wzorem 6.9. Wtedy, jak to wynika z 5.5 i 5.7, dla każdego $q \in Q$ funkcja φ_q jest sekwencyjna. Odwrotnie, mamy także

<u>Twierdzenie 7.2.</u> Jeżeli X, Y są dowolnymi zbiorami niepustymi oraz $\{\varphi_i\}_{i \in I}$ jest dowolną niepustą rodziną funkcji sekwencyjnych

$$\varphi_i : X^* \to Y^*$$

to istnieje automat $\{Q, X, Y, \delta, \lambda\}$ o tej własności, że dla każdego $i \in I$ istnieje taki $q \in Q$, że dla każdego $s \in X^*$

$$\varphi_i(s) = \lambda(q,s) .$$

Automat ten można utworzyć w następujący sposób:

1. Q jest zbiorem wszystkich funkcji $\varphi_{i,t}: X^* \to Y^*$, $i \in I$, $t \in X^*$ takich, że dla każdego $s \in X^*$

$$\varphi_{i,t}(s) = \varphi_i(ts) /\!/ \varphi_i(t) .$$

2. Dla dowolnych $x \in X$, $i \in I$, $t \in X^*$

$$\delta(\varphi_{i,t}, x) = \varphi_{i,tx} ,$$

$$\lambda(\varphi_{i,t}, x) = \varphi_{i,t}(x) .$$

Wtedy:

3. Dla każdego $i \in I$ i dla każdego $t \in X^*$

$$\lambda(\varphi_{i,e}, t) = \varphi_i(t) .$$

4. Wszystkie stany tego automatu są parami odróżnialne.

Dowód:

To, że $\varphi_{i,t}$ są funkcjami, wynika z sekwencyjności φ_i, a dokładniej, z 7.2: dla dowolnych $i \in I$, $t \in X^*$, $s \in X^*$ istnieje takie słowo $u \in Y^*$, że $\varphi_i(ts) = \varphi_i(t)\, u$. Stąd $\varphi_{i,t}(s) = \varphi_i(ts) /\!/ \varphi_i(t) = u$, a ponieważ dla każdego i,t,s takie u istnieje tylko jedno, $\varphi_{i,t}(s)$ faktycznie jest funkcją tych argumentów.

Jeżeli $\varphi_{i,t} \in Q$ i $x \in X$, to oczywiście $\delta(\varphi_{i,t}, x) = \varphi_{i,tx} \in Q$, a także $\lambda(\varphi_{i,t}, x) = \varphi_{i,t}(x) = \varphi_i(tx) /\!/ \varphi_i(t)$; ponieważ φ_i jest sekwencyjna i spełnia 7.6, iloraz ten jest elementem Y. Wykazaliśmy w ten sposób, że tak określona piątka $\{Q, X, Y, \delta, \lambda\}$ jest rzeczywiście automatem.

Przy tych oznaczeniach stanów $\varphi_{i,e}(s) = \varphi_i(s) /\!/ \varphi_i(e)$ i wobec 7.3 $\varphi_{i,e}(s) = \varphi_i(s)$, czyli $\varphi_{i,e} = \varphi_i$.

Stosując indukcję względem długości słowa możemy wykazać, że dla dowolnych $i \in I$, $t \in X^*$, $s \in X^*$

$$\delta(\varphi_{i,t}, s) = \varphi_{i,ts}, \qquad 7.7$$

$$\lambda(\varphi_{i,t}, s) = \varphi_{i,t}(s). \qquad 7.8$$

Rzeczywiście, jeżeli $s = e$, to wobec 5.6 i 5.7 $\delta(\varphi_{i,t}, e) = \varphi_{i,t} = \varphi_{i,te}$ oraz $\lambda(\varphi_{i,t}, e) = e = \varphi_i(t) /\!/ \varphi_i(t) = \varphi_i(te) /\!/ \varphi_i(t) = \varphi_{i,t}(e)$. Dla słów jednoliterowych równości te są prawdziwe z założenia. Przypuśćmy dalej, że dla wszystkich słów s o długości $\leqslant n$ te dwie równości są spełnione i że $x \in X$. Wtedy sx jest słowem o długości $n + 1$ oraz dla dowolnych $t \in X^*$, $i \in I$

$$\delta(\varphi_{i,t}, sx) = \delta(\delta(\varphi_{i,t}, s), x) = \delta(\varphi_{i,ts}, x) = \varphi_{i,tsx},$$

$$\lambda(\varphi_{i,t}, sx) = \lambda(\varphi_{i,t}, s)\lambda(\delta(\varphi_{i,t}, s), x) = \varphi_{i,t}(s)\lambda(\varphi_{i,ts}, x) =$$

$$= \varphi_{i,t}(s)\,\varphi_{i,ts}(x) = (\varphi_i(ts) /\!/ \varphi_i(t))(\varphi_i(tsx) /\!/ \varphi_i(ts)) =$$

$$= \varphi_i(tsx) /\!/ \varphi_i(t) = \varphi_{i,t}(sx).$$

To kończy dowód 7.7 i 7.8.

Z 7.8 wynika, jako szczególny przypadek, równość w p. 3 oraz odróżnialność stanów: dwa stany $\varphi_{i,t}$, $\varphi_{j,u}$ są nieodróżnialne wtedy i tylko wtedy, gdy dla każdego $s \in X^*$ $\lambda(\varphi_{i,t}, s) = \lambda(\varphi_{j,u}, s)$, czyli $\varphi_{i,t}(s) = \varphi_{j,u}(s)$, to znaczy $\varphi_{i,t} = \varphi_{j,u}$.

Koniec dowodu.

Przyglądając się temu dowodowi możemy zauważyć, że możliwe jest sformułowanie analogicznego twierdzenia z nieco osłabionymi wymaganiami na funkcje φ_i gdy nie będzie się wymagać spełnienia 7.1 , a tylko 7.2. Wtedy będzie można wyznaczyć automat, w którym te funkcje będą co prawda określały odpowiedniości pomiędzy słowami wejściowymi i wyjściowymi, ale jego alfabet wyjściowy będzie zbiorem słów w alfabecie Y . Można sobie wyobrazić, że ten automat, reagując na pojawienie się pojedynczych elementów alfabetu X na jego wejściu, wyrzuca na wyjście sekwencje elementów alfabetu Y zamiast pojedynczych liter. Oczywiście to nie wyklucza tego, że w określonych przypadkach jednej literze alfabetu X na wejściu będzie odpowiadała jedna litera alfabetu Y na wyjściu, ale na to, żeby tak było w każdym przypadku, potrzeba i wystarcza, żeby wszystkie funkcje φ_i były sekwencyjne.

<u>Twierdzenie 7.3.</u> Jeżeli X, Y są zbiorami niepustymi oraz $\{\varphi_i\}_{i \in I}$ jest dowolną niepustą rodziną funkcji

$$\varphi_i : X^* \to Y^* ,$$

spełniających warunek 7.2, to istnieje automat $\{Q, X, Y^*, \delta, \lambda\}$ tego rodzaju, że dla każdego $i \in I$ istnieje $q \in Q$ taki, że dla każdego $s \in X^*$

$$\lambda(q, s) = \varphi_i(s) /\!/ \varphi_i(e) .$$

Automat ten można utworzyć w sposób opisany w p. 1 i 2 twierdzenia 7.2; wtedy

3. Dla każdego $i \in I$ i każdego $t \in X^*$

$$\lambda(\varphi_{i,e}, t) = \varphi_{i,e}(t) = \varphi_i(t) /\!/ \varphi_i(e)$$

4. Wszystkie stany tego automatu są parami odróżnialne.

Dowód:

Ponieważ funkcje φ_i spełniają warunek 7.2, a 7.5 jest

mu równoważny, $\varphi_{i,t}$ są rzeczywiście funkcjami odwzorowującymi /dla każdego $i \in I$, $t \in X^*$/ X^* w Y^*. W związku z tym tak określone funkcje δ i λ odwzorowują $Q \times X$ odpowiednio w Q i Y^*. Funkcje te spełniają warunki 7.7 i 7.8 - dowód tego jest dokładnie taki sam, jak w twierdzeniu 7.2. Dowód p. 3. i 4. jest analogiczny. Nie korzystamy z równości $\varphi_{i,e} = \varphi_i$, gdyż teraz jest tylko $\varphi_{i,e}(s) = \varphi_i(s) // \varphi_i(e)$, co znalazło swoje odbicie w sformułowaniu p. 3.

Koniec dowodu.

Dalsze osłabianie założeń jest już trudniejsze. Jeżeli mamy daną rodzinę funkcji, odwzorowujących X^* w Y^*, z których przynajmniej jedna nie spełnia 7.2, to oczywiście nie można otrzymać automatu, który odwzorowuje słowa wejściowe w wyjściowe tak samo, jak to robiłyby automaty w przypadkach, objętych twierdzeniami 7.2 i 7.3. Ale można próbować obliczyć automat, którego działanie będzie w pewnym sensie opisane przez te funkcje w sposób przybliżony. Od tego, jak będziemy rozumieć to przybliżenie, będzie zależeć całe dalsze postępowanie. Rozważmy tu jedną z możliwości: tzw. metodę wyrównywania długości słów. Aby nie komplikować rozważań, załóżmy, że rodzina funkcji składa się tylko z jednego elementu.

Niech więc będą dane zbiory niepuste X i Y oraz dowolna funkcja niesekwencyjna $\varphi : X^* \to Y^*$. Metoda wyrównywania długości słów polega na tym, że do zbiorów X i Y dodajemy po jednym elemencie /oznaczmy je odpowiednio x_0 i y_0/ nie należącym do nich przedtem, a następnie tworzymy nową funkcję $\gamma : (X \cup x_0)^* \to (Y \cup y_0)^*$, która jest sekwencyjna i ma następującą własność: jeżeli oznaczymy przez k operację opuszczania x_0 w słowach w alfabecie $X \cup x_0$ i y_0 w słowach w alfabecie $Y \cup y_0$, to dla każdego $s \in (X \cup x_0)^*$

$$\varphi(k(s)) = k(\gamma(s)). \qquad 7.9$$

Tę funkcję γ wyznacza się w następujący sposób: dla każdego $t \in X^*$ przyjmujemy

$$\gamma\left(tx_0^{l(\varphi(t))}\right) = y_0^{l(t)}\,\varphi(t) \quad .$$

Wartości funkcji γ dla lewych podsłów słów postaci $tx_0^{l(\varphi(t))}$ określamy tak, żeby były spełnione warunki sekwencyjności. Te same warunki wymagają także, by było $\gamma(e) = e$. W każdym słowie t, dla którego nie można było wyznaczyć wartości γ w wyżej opisany sposób, znajdujemy najdłuższe lewe podsłowo u, dla którego wartość $\gamma(u)$ jest już określona. Wtedy $t = uv$, gdzie $v = t /\!/ u$ i przyjmujemy

$$\gamma(t) = \gamma(u)\, y_0^{l(t)-l(u)} \quad .$$

Czytelnik może się sam przekonać, że tak skonstruowana γ jest funkcją, a ponadto jest określona na całym $(X \cup x_0)^*$, jest sekwencyjna i spełnia warunek 7.9.

Wymagania stawiane innym opisom zachowania automatu przez funkcje ψ lub ρ są o wiele słabsze. Na przykład od funkcji ψ wymaga się tylko, aby odwzorowywała słowo puste w słowo puste oraz żeby obraz każdego słowa niepustego należał do alfabetu wyjściowego.

<u>Twierdzenie 7.4.</u> Niech X, Y będą dowolnymi zbiorami niepustymi i niech $\{\varphi_i\}_{i \in I}$ będzie dowolną rodziną funkcji

$$\varphi_i : XX^* \to Y \quad .$$

Wtedy automat $\{Q, X, Y, \delta, \lambda\}$, w którym dla każdego $i \in I$ istnieje $q \in Q$ taki, że dla każdego $s \in XX^*$ $\varphi_i(s)$ jest ostatnią literą słowa $\lambda(q,s)$, zawsze istnieje i można go wyznaczyć w następujący sposób:

1. Q jest zbiorem wszystkich funkcji

$$\varphi_{i,t} : XX^* \to Y \quad , \quad i \in I,\ t \in X^*$$

takich, że dla każdego $s \in XX^*$

$$\varphi_{i,t}(s) = \varphi_i(ts) .$$

2. Dla dowolnych $x \in X$, $i \in I$, $t \in X^*$

$$\delta(\varphi_{i,t}, x) = \varphi_{i,tx} ,$$

$$\lambda(\varphi_{i,t}, x) = \varphi_{i,t}(x) .$$

Wtedy

3. Dla każdego $i \in I$ i każdego $t \in XX^*$

$$\mu(\varphi_{i,e}, t) = \varphi_i(t) ,$$

gdzie $\mu(q,t)$ jest ostatnią literą słowa $\lambda(q,t)$.

4. Wszystkie stany tego automatu są parami odróżnialne.

Dowód:

Przy tak określonym Q funkcje δ i λ odwzorowują $Q \times X$ odpowiednio w Q i Y, a więc jest to rzeczywiście automat. Wykażemy, że dla każdego $s \in XX^*$ oraz dla dowolnych $i \in I$, $t \in X^*$ jest

$$\delta(\varphi_{i,t}, s) = \varphi_{i,ts} , \qquad 7.10$$

$$\mu(\varphi_{i,t}, s) = \varphi_{i,t}(s) . \qquad 7.11$$

Dla słów jednoliterowych s równości te są spełnione z założenia, gdyż wtedy funkcje μ i λ mają jednakowe wartości. Załóżmy więc, że są one spełnione dla wszystkich słów s o długości $n \geq 1$ i niech $x \in X$; wtedy sx ma długość $n+1$ oraz

$$\delta(\varphi_{i,t}, sx) = \delta(\delta(\varphi_{i,t}, s), x) = \delta(\varphi_{i,ts}, x) = \varphi_{i,tsx} ,$$

$$\mu(\varphi_{i,t}, sx) = \mu(\delta(\varphi_{i,t}, s), x) = \mu(\varphi_{i,ts}, x) = \varphi_{i,ts}(x) =$$
$$= \varphi_i(tsx) = \varphi_{i,t}(sx) ,$$

a więc obie równości są spełnione dla wszystkich słów s o długości dodatniej.

Równość w p. 3. jest szczególnym przypadkiem 7.11, gdyż, jak to wynika bezpośrednio z definicji w p. 1, $\varphi_{i,e} = \varphi_i$. Zgodnie z twierdzeniem 6.1 dwa stany, $\varphi_{i,t}$ i $\varphi_{j,u}$, są nieodróżnialne wtedy i tylko wtedy, gdy dla każdego $s \in X^*$ $\mu(\varphi_{i,t}, s) = \mu(\varphi_{j,u}, s)$, a więc $\varphi_{i,t}(s) = \varphi_{j,u}(s)$ dla każdego s niepustego, czyli $\varphi_{i,t} = \varphi_{j,u}$.

Koniec dowodu.

W tym twierdzeniu przyjmuje się, że funkcje φ_i są określone tylko na zbiorze XX^*. Gdybyśmy chcieli, żeby były określone na X^*, to zgodnie z definicją funkcji μ powinno być $\varphi_i(e) = e$ - inaczej warunek 3 nie byłby spełniony.

Jeżeli mamy rodzinę funkcji, odwzorowujących X^* w $Y \cup e$ i chcemy ją przyjąć jako opis zachowania automatu, ale przynajmniej jedna z nich nie odwzorowuje zbioru XX^* w Y lub słowa pustego w słowo puste, to na to, żeby rzeczywiście uzyskać taki opis, trzeba wprowadzić odpowiednie modyfikacje. Rozważmy przypadek, kiedy ta rodzina ma tylko jeden element.

Niech więc będzie dana funkcja $\varphi : X^* \to Y \cup e$. Jeżeli nie spełnia ona któregoś z wyżej wymienionych warunków, to tworzymy nową funkcję $\gamma : X^* \to Y \cup e \cup y_0$, $y_0 \notin Y$ w następujący sposób: $\gamma(e) = e$ i dla dowolnych $s \in XX^*$ $\gamma(s) = \varphi(s)$, gdy $\varphi(s) \in Y$ oraz $\gamma(s) = y_0$ w przeciwnym przypadku. Ta funkcja γ spełnia już założenia twierdzenia 7.3.

Ograniczenia na funkcje ϱ wynikają z 5.18: jeżeli istnieje automat, dla którego funkcje te są opisem zachowania, to dla każdego elementu ϱ_i rodziny takich funkcji $\{\varrho_i\}$ $i \in I$

$$e \cup \bigcup_{y \in Y} \varrho_i(y) = X^* \qquad 7.12$$

oraz dla dowolnych $i \in I$, $y \in Y$, $w \in Y$

$$e \cap \varrho_i(y) = 0 \quad , \qquad 7.13$$

$$\text{jeśli } y \neq w \text{ , to } \varrho_i(y) \cap \varrho_i(w) = 0 \qquad 7.14$$

Odwrotnie, jeżeli ϱ_i spełniają te warunki, to można obliczyć automat, w którym dla każdego i istnieje taki stan q, że $\varrho_i = \varrho_q$, gdzie ta ostatnia funkcja jest rozumiana w sensie 6.21.

Jeżeli mamy rodzinę funkcji odwzorowujących alfabet Y w zbiór zdarzeń w alfabecie X i niektóre elementy tej rodziny nie spełniają warunków 7.12 - 7.14, to nie istnieje automat, dla którego te funkcje byłyby funkcjami ϱ_q dla pewnych stanów q, w sensie 6.21. Ale wtedy można zbudować automat o alfabecie wejściowym X, dla którego jest spełnione pewne uogólnienie tej zależności.

<u>Twierdzenie 7.5.</u> Niech X, J będą zbiorami niepustymi i niech $\{\varrho_i\}_{i \in I}$ będzie niepustą rodziną funkcji, odwzorowujących zbiór J w zbiór wszystkich zdarzeń w alfabecie X. Niech $\{Q, X, Y, \delta, \lambda\}$ będzie automatem, utworzonym w następujący sposób:

1. Q jest zbiorem wszystkich odwzorowań $\varrho_{i,t}$ takich, że dla dowolnych $i \in I$, $t \in X^*$, $j \in J$

$$\varrho_{i,t}(j) = \varrho_i(j) /\!/ t \quad ,$$

z tym, że jeżeli wartości dwóch funkcji różnią się co najwyżej o e dla każdego $j \in J$, to uważamy je za jeden i ten sam element zbioru Q. Inaczej mówiąc, jeśli $p \in Q$, $q \in Q$ oraz dla każdego $j \in J$ $p(j) \cup e = q(j) \cup e$, to przyjmujemy, że $p = q$.

2. Y jest zbiorem wszystkich złożeń $\varepsilon\varrho_{i,t}$, rozumianych w następujący sposób: $\varepsilon\varrho_{i,t}(j) = \varepsilon(\varrho_{i,t}(j))$ dla wszystkich $j \in J$.

3. Dla dowolnych $i \in I$, $t \in X^*$, $x \in X$

$$\delta(\rho_{i,t}, x) = \rho_{i,tx},$$

$$\lambda(\rho_{i,t}, x) = \varepsilon \rho_{i,tx}$$

- przy obliczaniu wartości funkcji δ stosujemy podaną w p. 1 regułę utożsamiania stanów, różniących się co najwyżej o e dla każdej wartości ich argumentu.

Wtedy:

4. Dla każdego $i \in I$ oraz dla każdego $j \in J$

$$\rho_i(j) = \{s \in XX^* : \mu(\rho_{i,e}, s)(j) = e\} \cup \varepsilon\rho_i(j),$$

gdzie $\mu(q,s)$ dla $q \in Q$, $s \in XX^*$, jest ostatnią literą $\lambda(q, s)$.

5. Wszystkie stany tego automatu są parami odróżnialne.

Dowód:

Przy tych oznaczeniach stanów $\rho_{i,e} = \rho_i$ dla każdego $i \in I$. Przez indukcję względem długości słowa możemy łatwo wyprowadzić wzór na funkcję μ: dla dowolnych $i \in I$, $t \in X^*$, $s \in XX^*$, $j \in J$ jest

$$\mu(\rho_{i,t}, s) = \varepsilon \rho_{i,ts}$$

i wobec tego $\mu(\rho_{i,e}, s)(j) = \varepsilon \rho_{i,s}(j) = \varepsilon(\rho_i(j) /\!/ s)$. Ale, zgodnie z 2.55, $\varepsilon(\rho_i(j) /\!/ s) = e$ wtedy i tylko wtedy, gdy $s \in \rho_i(j)$; stąd 4., a nawet więcej. W ten sam sposób można wykazać, że dla dowolnych $i \in I$, $t \in X^*$, $j \in J$

$$\rho_{i,t}(j) = \{s \in XX^* : \mu(\rho_{i,t}, s)(j) = e\}$$

$$\cup \varepsilon \rho_{i,t}(j),$$

Przypuśćmy teraz, że stany $\varrho_{i,t}$, $\varrho_{l,u}$ są nieodróżnialne. Wobec p. 3 twierdzenia 6.1 oznacza to, że dla każdego $s \in X^*$ $\mu(\varrho_{i,t}, s) = \mu(\varrho_{l,u}, s)$, czyli dla każdego $j \in J$ $\{s \in XX^*: \mu(\varrho_{i,t}, s)(j) = e\} = \{s \in XX^*: \mu(\varrho_{l,u}, s)(j) = e\}$. Stąd i z wyprowadzonego wyżej wzoru wynika, że wartości funkcji $\varrho_{i,t}$ oraz $\varrho_{l,u}$ różnią się dla każdego $j \in J$ co najwyżej o e. Wyżej przyjęliśmy, że takie funkcje reprezentują ten sam stan i stąd 5.

Koniec dowodu.

Jak stąd wynika, moc Y jest nie mniejsza od mocy zbioru wszystkich takich $j \in J$, dla których przynajmniej dla jednego $i \in I$ $\varrho_i(j) \neq 0$.

W praktycznych zastosowaniach teorii automatów najbardziej interesującym przypadkiem jest obliczanie automatów skończonych. Jeżeli wykluczymy powtarzanie się funkcji ϱ_i dla różnych $i \in I$ oraz odrzucimy wszystkie takie j, że $\varrho_i(j) = 0$ dla każdego $i \in I$, to warunkiem koniecznym na to, aby opisana metoda dała automat skończony, jest skończoność zbiorów X, I, J. Zajmijmy się bliżej tym przypadkiem. Zamiast funkcji ϱ_i możemy teraz wziąć ciągi $\overline{R}_i$.

<u>Twierdzenie 7.6.</u> Przyjmijmy, że X jest zbiorem skończonym i że m,n są liczbami naturalnymi dodatnimi. Niech R_{ij}, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$ będzie rodziną zdarzeń w alfabecie X. Oznaczmy:

$$\overline{R}_i = (R_{i1}, R_{i2}, \ldots, R_{in}) .$$

Niech $\{Q, X, Y, \delta, \lambda\}$ będzie automatem, utworzonym w następujący sposób:

1. Q jest zbiorem wszystkich ilorazów $\overline{R}_i /\!/ s$, gdzie $s \in X^*$. Ilorazy, różniące się co najwyżej o e na każdej pozycji /to znaczy takie $q \in Q$, $p \in Q$, że $q \cup (e, e, \ldots, e) = p \cup (e, e, \ldots, e)$ / uważamy za jeden i ten sam element zbioru Q.

2. Y jest zbiorem wszystkich wartości $\varepsilon(\overline{R}_i /\!/ s)$ dla $s \in X^*$.

3. Dla dowolnych $q \in Q$, $x \in X$

$$\delta(q, x) = q \,/\!/\, x \ ,$$

$$\lambda(q, x) = \varepsilon\,(q \,/\!/\, x)\,.$$

Przy obliczaniu wartości funkcji δ stosujemy podaną w p. 1 zasadę utożsamiania stanów.

Wtedy:

4. Dla każdego niepustego słowa s , $s \in R_{ij}$ wtedy i tylko wtedy, gdy $\overline{R}_i \,/\!/\, s$ ma na j-miejscu e , lub, co jest równoważne, dla każdego i, j

$$R_{ij} = \{s \in \overline{XX}^*: \mu(\overline{R}_i, s) \text{ ma na } j\text{-miejscu } e\} \cup \varepsilon\,(R_{ij})\,.$$

5. Wszystkie stany tego automatu są parami odróżnialne.

6. Automat jest skończony wtedy i tylko wtedy, gdy wszystkie zbiory R_{ij} są regularne .

Dowód:

4 i 5 dowodzi się analogicznie jak w poprzednim twierdzeniu. Zbiór X jest z założenia skończony. Zbiór Y składa się z ciągów n-elementowych, mających na każdej pozycji 0 lub e . Ilość takich ciągów nie przekracza 2^n , a więc Y jest skończony. Zatem nasz automat jest skończony wtedy i tylko wtedy, gdy Q jest skończony. Stąd i z twierdzenia 4.3 wynika 6.

Koniec dowodu.

Jak widać, wartość $\mu(q,s)$ dla $q \in Q$, $s \in XX^*$ zależy w tym automacie od tego, czy s należy do zbiorów wchodzących w skład ciągu q . Ciąg $\mu(q,s)$ jest w gruncie rzeczy swego rodzaju tablicą relacji "s jest elementem" ze zmiennym j . Z tego powodu możemy automat ten nazwać automatem rozpoznającym przynależność niepustych słów do zadanych zdarzeń.

Zbiory R_{qy} tego automatu /gdzie $q \in Q$, $y \in Y$/ są, zgodnie z 5.18, elementami podziału zbioru XX^* albo są puste.

W szczególności, jeżeli q jest równe z dokładnością do e na każdej pozycji ciągowi $\overline{R}_i = \overline{R}_i // e$, to dla każdego $y \in Y$ R_{qy} jest elementem podziału zbioru XX^* wyznaczonego przez rodzinę zdarzeń $\{R_{ij}\}$ $i \leq j \leq n$ albo jest zbiorem pustym.

Z uwagi tej wynika, że jeżeli zechcemy sprawdzić wyniki obliczeń wykonanych tą metodą i w tym celu obliczymy zbiory R_{qy} /np. rozwiązując układ równań 5.13/, to $R_{\overline{R}_i y}$ dla $y \in Y$ mogą nie być równe /nawet z dokładnością do e / żadnym R_{ij}, $i \leq j \leq n$, ale, jeżeli są niepuste, to są elementami podziału, wyznaczonego przez rodzinę elementów ciągu $\overline{R}_i$.

Twierdzenie 7.6 ma duże znaczenie dla zastosowań, zwłaszcza takich, jak projektowanie urządzeń cyfrowych. Traktując projektowane części urządzenia liczącego jako automaty skończone, można opisywać ich zachowanie, podając odpowiednie rodziny zdarzeń regularnych. W praktyce projektowej taki sposób opisu jest najczęściej stosowany. Twierdzenie 7.6 nie tylko pozwala obliczać na podstawie tych danych tablice automatu, ale także zapewnia to, że automat ten ma możliwie najmniejszą ilość stanów.

W praktycznych zastosowaniach bardzo często mamy do czynienia z automatami ze stanem początkowym. Na przykład, jeżeli projektujemy lub badamy urządzenia cyfrowe, to bardzo często zakłada się, że praca takiego urządzenia zawsze zaczyna się od tego samego, raz na zawsze wyróżnionego stanu. W takim przypadku wystarczy podać reakcję automatu na słowa wejściowe, gdy na początku każdego eksperymentu jest on w stanie początkowym, ponieważ dane te pozwalają już go /lub automat tak samo działający/ obliczyć.

Możemy wtedy przyjąć, że $m = 1$, czyli że rodzina zbiorów R_{ij} składa się z elementów tylko jednego ciągu $\overline{R}_i$. Wskaźnik i można w takim przypadku wogóle opuścić. Ciąg $\overline{R}$ jest wtedy stanem początkowym tego automatu /obliczanego metodą z twierdzenia 7.6/, a każdy iloraz $\overline{R} // s$, dla $s \in X^*$, jest stanem, do jakiego on dochodzi ze stanu począt-

kowego po podaniu na jego wejście słowa s .

Zauważmy jeszcze, że gdy któryś z elementów ciągu $\overline{R}$ jest zbiorem pustym lub jest uzupełnieniem sumy pozostałych elementów ciągu, to można go opuścić. W ten sposób skróci się zapis, co może ułatwić obliczenia. Konsekwencją tego jest tylko usunięcie z wszystkich ciągów /stanów i stanów wyjścia/ elementów na tej samej pozycji. W szczególności, jeżeli $\overline{R} = (R,-R)$, to można zastąpić $\overline{R}$ przez R .

Przykład:

Wyznaczyć funkcję przejść i wyjść oraz zbiór stanów zamka szyfrowego opisanego we wstępie, traktując go jako automat ze stanem początkowym.

Alfabetem wejściowym jest $X = \{1,2,3,4,5,6,7,8,9,Ø\}$.

$S_o = 256Ø92$,

$S_s = 2 \cup 25 \cup 256 \cup 256Ø \cup 256Ø9$,

$S_a = -(S_o \cup S_s)$.

Przyjmujemy

$\overline{S} = (S_o , S_s)$.

Obliczamy ilorazy i wartości funkcji ε :

$\overline{S} // 2 = (56Ø92, e \cup 5 \cup 56 \cup 56Ø \cup 56Ø9)$, $\varepsilon(\overline{S} // 2) = (0, e)$,

$\overline{S} // 25 = (6Ø92, e \cup 6 \cup 6Ø \cup 6Ø9)$, $\varepsilon(\overline{S} // 25) = (0, e)$,

$\overline{S} // 256 = (Ø92, e \cup Ø \cup Ø9)$, $\varepsilon(\overline{S} // 256) = (0, e)$,

$\overline{S} // 256Ø = (92, e \cup 9)$, $\varepsilon(\overline{S} // 256Ø) = (0, e)$,

$\overline{S} // 256Ø9 = (2, e)$, $\varepsilon(\overline{S} // 256Ø9) = (0, e)$,

$\overline{S} // 256Ø92 = (e, 0)$, $\varepsilon(\overline{S} // 256Ø92) = (e, 0)$.

Wszystkie pozostałe ilorazy są równe $(0, 0)$. Ponieważ $\overline{S} // 256Ø92$ różni się od $(0,0)$ tylko o e na pierwszej pozycji, oba te ciągi reprezentują ten sam stan.

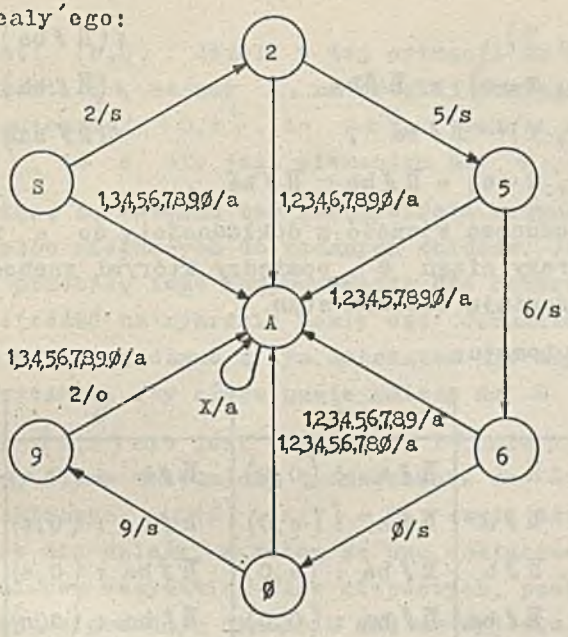
Tablica automatu:

	2	5	6	Ø	9	inna cyfra
$\bar{S}$	$\bar{S}$//2:(0,e)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)
$\bar{S}$//2	(0,0):(0,0)	$\bar{S}$//25:(0,e)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)
$\bar{S}$//25	(0,0):(0,0)	(0,0):(0,0)	$\bar{S}$//256:(0,e)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)
$\bar{S}$//256	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	$\bar{S}$//256Ø:(0,e)	(0,0):(0,0)	(0,0):(0,0)
$\bar{S}$//256Ø	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	$\bar{S}$//256Ø9:(0,e)	(0,0):(0,0)
$\bar{S}$//256Ø9	(0,0):(e,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)
(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)	(0,0):(0,0)

Pojawienie się ciągu (e,0) na wyjściu automatu oznacza, że słowo podane na jego wejście należy do zbioru S_o. Podobnie (0,e) oznacza, że słowo wejściowe należy do S_s, zaś (0,0) [illegible] czy, że to słowo nie należy ani do S_o ani do S_s, czyli należy do S_a. Wobec tego możemy wprowadzić skrócone oznaczenia elementów alfabetu wyjściowego, zastępując (e,0), (0,e), (0,0) odpowiednio przez o, s, a. Oznaczając stany automatu symbolami S, 2, 5, 6, Ø, 9, A otrzymamy tablicę zapisaną w nieco prostszy sposób:

	2	5	6	Ø	9	inna cyfra
S	2:s	A:a	A:a	A:a	A:a	A:a
2	A:a	5:s	A:a	A:a	A:a	A:a
5	A:a	A:a	6:s	A:a	A:a	A:a
6	A:a	A:a	A:a	Ø:s	A:a	A:a
Ø	A:a	A:a	A:a	A:a	9:s	A:a
9	A:o	A:a	A:a	A:a	A:a	A:a
A	A:a	A:a	A:a	A:a	A:a	A:a

Wykres Mealy'ego:



Zgodnie z twierdzeniem 7.6 jest to najprostszy /w sensie ilości stanów/ automat o takim zachowaniu.

Koniec przykładu.

Przykład:

Obliczyć automat ze stanem początkowym, rozpoznający przynależność słów w alfabecie $X = \{a, b\}$ do zbiorów

$S = a^*Xa$,

$T = X^*b$.

Przyjmujemy oznaczenie

$\overline{R} = (S , T)$.

Obliczamy ilorazy i wartości funkcji ε :

$\overline{R} /\!/ a = (a^*Xa \cup a , X^*b) = \overline{R} \cup (a, 0)$, $\varepsilon(\overline{R} /\!/ a) = (0, 0)$,

$\overline{R} /\!/ b = (a, X^*b \cup e) = (a, T \cup e)$, $\varepsilon(\overline{R} /\!/ b) = (0, e)$,

$\overline{R} /\!/ aa = \overline{R} /\!/ a \cup (e, 0) \sim \overline{R} /\!/ a$, $\varepsilon(\overline{R} /\!/ aa) = (e, 0)$,

$\overline{R} /\!/ ab = \overline{R} /\!/ b$.

$\bar{R} /\!/ ba = (e, T)$, $\varepsilon(\bar{R} /\!/ ba) = (e, 0)$,

$\bar{R} /\!/ bb = (0, T \cup e) \sim \bar{R} /\!/ ba$, $\varepsilon(\bar{R} /\!/ bb) = (0, e)$,

$\bar{R} /\!/ baa = (0, T) \sim \bar{R} /\!/ ba$, $\varepsilon(\bar{R} /\!/ baa) = (0, 0)$,

$\bar{R} /\!/ bab = (0, T \cup e) = \bar{R} /\!/ bb \sim \bar{R} /\!/ ba$.

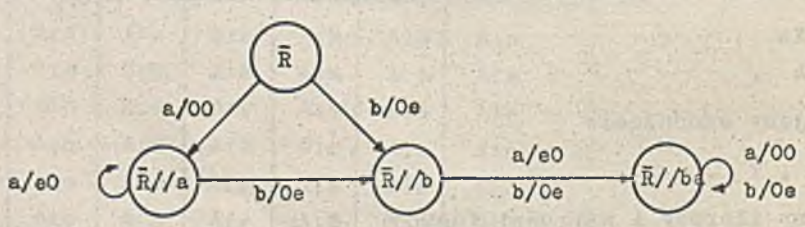
Symbol $\sim$ oznacza równość z dokładnością do e na każdej pozycji. Ilorazy ciągu $\bar{R}$, pomiędzy którymi zachodzi ta relacja, reprezentują ten sam stan.

Tablica automatu:

	a	b
$\bar{R}$	$\bar{R} /\!/ a : (0,0)$	$\bar{R} /\!/ b : (0,e)$
$\bar{R} /\!/ a$	$\bar{R} /\!/ a : (e,0)$	$\bar{R} /\!/ b : (0,e)$
$\bar{R} /\!/ b$	$\bar{R} /\!/ ba : (e,0)$	$\bar{R} /\!/ ba : (0,e)$
$\bar{R} /\!/ ba$	$\bar{R} /\!/ ba : (0,0)$	$\bar{R} /\!/ ba : (0,e)$

Stanem początkowym tego automatu jest $\bar{R}$, alfabetem wyjściowym $Y = \{(e,0), (0,e), (0,0)\}$.

Wykres Mealy'ego:



Jeżeli po podaniu dowolnego niepustego słowa s na wejście tego automatu /będącego w stanie początkowym/ ukaże się na jego wyjściu element alfabetu Y, który ma e na pierwszej pozycji, to $s \in S$. W naszym przypadku jest tylko jeden

taki element: $(e,0)$. Jeżeli w tej sytuacji na wyjściu ukaże się element Y, mający e na drugiej pozycji, czyli /dla tego automatu/ $(0,e)$, to $s \in T$. Jeżeli na wyjściu jest $(0,0)$, to s nie jest elementem ani S, ani T.

Widać więc, że automat ten rzeczywiście rozpoznaje przynależność słów niepustych do żadanych zbiorów. Jego działanie, czyli przebieg tego rozpoznawania dla konkretnych słów, można prześledzić na wykresie Mealy'ego. Jednakże takie doświadczenia przeprowadzane z tym automatem nie mogą dać odpowiedzi na pytanie, czy słowo puste należy do S lub do T.

Ponieważ (e,e) nie jest elementem Y, nie istnieje słowo niepuste, które należałoby jednocześnie do S i T. Jak łatwo obliczyć $\varepsilon(S) = \varepsilon(T) = 0$, czyli słowo puste do tych zbiorów nie należy, a zatem są one rozłączne. Suma ich nie jest zbiorem wszystkich słów niepustych, ponieważ istnieją słowa, które powodują ukazanie się na wyjściu automatu ciągu $(0,0)$.

Koniec przykładu.

Przykład:

Automat ze stanem początkowym, rozpoznający przynależność słów w zadanym alfabecie X do zbiorów A, B, C, D, obliczony metodą Brzozowskiego /twierdzenie 7.6/ ma alfabet wyjściowy

$$Y = \{(e,e,0,0), (0,e,0,0), (0,e,e,0), (0,0,e,0)\}.$$

Obliczenia były przeprowadzane dla ciągu $\overline{R} = (A, B, C, D)$, który jest stanem początkowym tego automatu. Jakie można stąd wysnuć wnioski o zbiorach A, B, C, D, jeżeli oprócz tego wiadomo, że żaden z nich nie zawiera słowa pustego?

Do alfabetu Y nie należy ciąg $(0,0,0,0)$, a więc każde słowo niepuste należy do któregoś z tych zbiorów. Nie ma elementu Y, który by miał e na czwartej pozycji, a zatem nie ma słowa niepustego należącego do D. Ponieważ słowo puste także do niego nie należy, jest to zbiór pusty. Jedynym elementem Y mającym e na pierwszym miejscu jest

$(e,e,0,0)$. Widać, że jeżeli słowo niepuste należy do A , to należy także do B . Stąd, wobec tego, że $e \notin A$, jest $A \subset B$. Dalej, jeżeli słowo niepuste należy do A , to nie należy do C , ponieważ nie ma elementu Y , który miałby e jednocześnie na pierwszym i trzecim miejscu. Stąd $A \cap C = 0$. Zbiory B i C nie są rozłączne, gdyż $(0,e,e,0) \in Y$. Istnieją elementy B nie należące do C i elementy C nie należące do B .

Jak powiedzieliśmy, każde słowo niepuste należy do któregoś z tych zbiorów, a puste nie należy do żadnego. Wobec $D = 0$ i $A \subset B$ jest $B \cup C = XX^*$.

Koniec przykładu.

Literatura

[1] BIRKHOFF G.: Lattice Theory, New York 1948.

[2] BODNARCZUK W.G.: Sistemy uravnenij v algebre sobytij. Žurnał Vycislitel'noj Matematiki i Matematičeskoj Fiziki, t. 3, Nr 6 /1963/, s. 1077-1088.

[3] BRZOZOWSKI J.A.: Derivatives of Regular Expressions. Journal of the ACM, vol. 11, N° 4 /Oct.1964/, 481-494.

[4] CHOMSKY N., MILLER G.A.: Finite State Languages. Information and Control, vol. 1, N° 2 /1958/, s. 91-112.

[5] COPI I.M., ELGOT C.C., WRIGHT J.B.: Realization of Events by Logical Nets. Journal of the ACM, vol. 5, N° 2 /Apr. 1958/, s. 181-196. Jest także w [18].

[6] DUBREIL-JACOTIN M.L., LESIEUR L., CROISOT R.: Théorie des treillis des structures algébriques ordonnées et de treillis géométriques. Paris 1953.

[7] EILENBERG S., WRIGHT J.B.: Automata in General Algebras. Information and Control vol. 11 /1967/, s. 452-470.

[8] GINSBURG S.: An Introduction to Mathematical Machine Theory. Reading 1962.

[9] GLUŠKOV V.M.: Abstraktnaja teorija avtomatov. Uspechi Matematičeskich Nauk, t. XVI, vyp. 5 /1961/, s. 3-62.

[10] JANOV Ju.I.: O tožděstvennych preobrazovanijach regularnych vyraženij. Dokłady Akademii Nauk SSSR, t. 147, Nr 2 /1962/, s. 327-330.

[11] KLEENE S.C.: Representation of Events in Nerve Nets and Finite Automata. Automata Studies, ed. by C.E.Shannon and J.McCarthy. Princeton 1956.

[12] KURATOWSKI K., MOSTOWSKI A.: Teoria mnogości, wyd. 2. Warszawa 1966.

[13] LJAPIN E.S.: Poługruppy, Moskva 1960.

[14] McNAUGHTON R., YAMADA H.: Regular Expressions and State Graphs for Automata. Trans. of the IRE on Electronic Computers, vol. EC-9 /1960/, s. 39-47. Jest także w [18].

[15] McNAUGHTON R.: The Theory of Automata, a Survey. Advances in Computers, vol. 2, New York 1961.

[16] MEALY G.H.: A Method for Synthesizing Sequential Circuits. Bell System Technical Journal, vol. 34 /1955/, s. 1045-1079.

[17] MOORE E.F.: Gedanken-Experiments on Sequential Machines. Automata Studies, ed. by C.E. Shannon and J.McCarthy, Princeton 1956.

[18] MOORE E.F.; ed.: Sequential Machines, Selected Papers. Reading 1964.

[19] PAPY G.: Groupoides. Paris 1965.

[20] PAULL M.C., UNGER S.H.: Minimizing the Number of States in Incompletely Specified Sequential Switching Functions. IRE Transactions on Electronic Computers, vol. EC-8 /1959/, s. 356-366.

[21] RABIN M.O., SCOTT D.: Finite Automata and their Decision Problems. IBM Journal of Research and Development, vol. 3, N° 2 /1959/, s. 114-125. Także w [18].

[22] RASIOWA H., SIKORSKI R.: The Mathematics of Metamathematics. Warszawa 1963.

[23] RASIOWA H.: Wstęp do matematyki współczesnej. Warszawa 1968.

[24] RED'KO V.N.: Ob opredeljajuščej sovokupnosti sootnošenij algebry regularnych sobytij. Ukrainskij Matematičeskij Žurnał, t. XVI, Nr 1 /1964/, s. 120-126.

[25] UNGER S.H.: Simplification of State Tables. A Survey of Switching Circuit Theory, ed. by E.J.McCluskey and T.C.Bartee, New York 1962.

[26] YOELI M.: Lattice-Ordered Semigroups, Graphs and Automata. Journal of the SIAM, vol. 13 /1965/, s. 411-422.

ALGEBRAIC THEORY OF AUTOMATA

Summary

The paper presents fundamentals of the automata theory, preceded by an elementary exposition of necessary information from general algebra. A notion of algebra of subsets of abstract algebra is introduced. For any abstract algebra $\{I, o_1, \ldots, o_s\}$ by the algebra of its subsets the algebra $\{E, \cup, \cap, -, *, \theta_1, \ldots, \theta_s\}$ is meant, where E is the family of all subsets of I, $\cup$, $\cap$, - are Boolean operations on the sets, * is a closure in respect to all operations $o_1, \ldots, o_s$, and $\theta_1, \ldots, \theta_s$ are operations of the algebra considered, shifted appropriately to the level of subsets of I. From the point of view of the theory of automata algebras of subsets of free monoids, i.e. so called algebras of events are most interesting. However, theorems which are valid not only in algebras of events but also in algebras of subsets of arbitrary semigroups or even groupoids, are formulated in a possibly general form. A detailed investigation of properties of left and right residuals, defined on algebras of subsets of semigroups, is made.

Following the general algebraic introduction there are presented main theorems of algebra of events dealing with the notion of regularity and characteristic properties of regular events, and methods of investigation of the regularity. Methods of solving of right and left linear equations in the algebras are described, too.

Last three paragraphs of the paper contain definitions, theorems, and calculational methods of the automata theory itself. By an automaton there is meant here a Moaly-type automaton /9/ or a sequential machine /8/. There are discussed various ways of presentation of automata and there are shown connections between them and previously introduced algebraic notions. There is shown that every automaton A /not necessarily finite, i.e. having finite both input and output alphabets and a set of states/ may be extended in various ways to an infinite automaton with the same set of states having as input symbols input words of the automaton A. On this basis there is made an investigation of equivalence of automata relation, and there are introduced methods

of simplification of automata and methods of construction of an infinite free automaton equivalent to a given one. Algebraic methods of analysis /i.e. deriving a behaviour of an automaton from its structure/ and synthesis /deriving a structure from the behaviour/ of automata are discussed in detail. Three basic kinds of the behaviour description are distinguished: by events /regular, if the calculated automaton is to be finite/, by sequential functions /9/, or by functions mapping the words of the input alphabet of the calculated automaton to the elements of its output alphabet. The synthesis method for the first case is based on calculation of left residuals of the given events and is slightly modified Brzozowski's method /3/. Methods of synthesis for the two remaining cases are partly based on results of /9/, but take advantage of the calculation of left residuals. Descriptions of all computational methods and more important theorems are supplemented by numerous examples.

АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ АВТОМАТОВ

Резюме

Работа содержит основные сведения по теории автоматов в алгебраической трактовке, представленные с помощью довольно широкого использования аппарата общей алгебры, теории группоидов и полугрупп. На основе приведенного в начале работы понятия алгебры подмножеств любой абстрактной алгебры, рассмотрены свойства алгебр подмножеств группоидов, полугрупп и свободных полугрупп. Под понятием алгебры подмножеств произвольной алгебры $\{I, o_1, \ldots, o\}$ понимается алгебра $\{E, \cup, \cap, -, {}^{*}, \theta_1, \ldots, \theta_s\}$, где E является семьёй всех подмножеств множества I, символы $\cup, \cap$ являются операциями поля множеств, * является операцией замыкания по всем операциям $o_1, \ldots, o_s$, а $\theta_1, \ldots, \theta_s$ возникают вследствие переноса этих операций на уровень подмножеств множества I. С точки зрения теории автоматов наибольшее значение имеют алгебры подмножеств свободных полугрупп с единицей, т.е. так называемые алгебры событий. Однако много теорем, истинных для алгебр событий, являются также истинными для алгебр подмножеств произвольных группоидов или, по крайней мере, произвольных полугрупп. В таких случаях эти теоремы приведены по возможности в общей

формулировке. Детально рассматриваются свойства лево и правостороннего деления: операций производимых на подмножествах группоидов, применяемых во многих вычислительных методах теории автоматов.

В части посвященной рассмотрению детальных свойств алгебр событий /п. 3, 4/ приведены теоремы решения лево - и правосторонне линейных систем уравнений, которые также играют большую роль в дальнейших рассуждениях. В той же части рассмотрены понятия регулярного события и регулярного выражения, а также указан ряд теорем о характеристических свойствах регулярных событий. Дальше вводится определение автомата(последовательной машины в смысле [8], автомата Мили в смысле [9],)и рассматриваются различные способы его представления, а также указывается их связь с ранее введенными алгебраическими понятиями.

Эти рассуждения касаются не только конечных автоматов /то есть автоматов имеющих конечные множество состояний, входный и выходный алфавит/. Пользуясь тем, что возможно расширение функции переходов и выходов произвольного автомата А на множество всех слов в его входном алфавите (см. [21], [9]), можно создавать различные расширения этого автомата, имеющие такое же множество состояний как А, но являющиеся бесконечными автоматами, так как их входным алфавитом есть множество всех слов во входном алфавите автомата А. Рассматриваются свойства отношения неразличимости автома-

тов и методы их упрощения и указывается способ построения, для данного автомата A, неразличимого от него свободного автомата с бесконечным множеством состояний. Подробно обсуждаются алгебраические методы анализа автоматов и методы синтеза, то есть вычисления автоматов на основе их поведения. При этом различаются три основные виды описаний поведения автомата: по событиям (они регулярные, если вычисляемый автомат должен быть конечным), по последовательным функциям ([9]), или по функциям отображающим слова входного алфавита на элементы выходного алфавита вычисляемого автомата. Описанный в работе метод синтеза для первого случая является незначительно модифицированным методом Брзозовского [8]. Методы синтеза для остальных двух случаев базируют на результатах [9], но в них используется левостороннее деление. Описания всех методов вычисления и более важные теоремы дополняются многочисленными примерами.

W. D. N. - Zam. 1059/0/69. Nakład 450+25 egz.

TECHNISCHE
BIBLIOTHEK
WIEN
ech

BIBLIOTEKA GŁÓWNA
Politechniki Śląskiej
P 2223/69