15 Zwartość

Lemat 15.1 *Zbiór*

$$\mathcal{A} = \{\begin{pmatrix} 2^n & m \\ 0 & 1 \end{pmatrix} : n, m \in N \wedge 0 \leqslant m < 2^n\}$$

jest półgrupą wolną generowaną przez macierze

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ oraz } \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}. \ \square$$

Zauważmy też, że

$$\begin{pmatrix} y_1 & z_1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} y_n & z_n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y_1 \ldots y_n & z_1 + y_1 z_2 + y_1 y_2 z_3 + \ldots + y_1 \ldots y_{n-1} z_n \\ 0 & 1 \end{pmatrix}. \qquad (1)$$

Lemat 15.2 *Niech $Y = \{y_1, \ldots, y_n, z_1, \ldots, z_n\}$ będzie zbiorem zmiennych. Półgrupa M macierzy o wyrazach będących wielomianami ze zbioru $Z[Y] = Z[y_1, \ldots, y_n, z_1, \ldots, z_n]$, generowaną przez macierze postaci*

$$\begin{pmatrix} y_i & z_i \\ 0 & 1 \end{pmatrix},$$

gdzie $i = 1, \ldots, n$, jest półgrupą wolną.

Dowód. Wzór (1) implikuje, że jest to półgrupa wolna i podane macierze są jej wolnymi generatorami (tworzą zbiór niezależnych generatorów). Zachodzi bowiem twierdzenie o jednoznaczności rozkładu 7.1. Znając prawą stronę równości (1) potrafimy odtworzyć pierwszą macierz A z lewej strony równości (1). W lewym górnym rogu A znajduje się zmienna, która jest składnikiem stopnia 1 w lewym górnym rogu macierzy B z prawej strony równości (1), natomiast w prawym górnym rogu A jest ta zmienna, która ma prawo wystąpić w prawym górnym rogu generatora i występuje w składniku stopnia 2 w lewym górnym rogu B. □

Twierdzenie 15.3 *Każdy układ równań w słowach bez stałych i ze skończoną liczbą zmiennych zawiera równoważny podukład skończony.*

Dowód. Przypuśćmy, że rozważamy równania ze zmiennymi ze zbioru $V = \{x_1, \ldots, x_n\}$. Weźmy zbiór zmiennych $Y = \{y_1, \ldots, y_n, z_1, \ldots, z_n\}$ i półgrupę M z lematu 15.2. Z lematu 15.2 wynika, że półgrupy X^* i M są izomorficzne. Niech φ oznacza izomorfizm tych półgrup taki, że

$$\varphi(x_i) = \begin{pmatrix} y_i & z_i \\ 0 & 1 \end{pmatrix}.$$

Przyjmijmy też, że

$$\varphi(w) = \begin{pmatrix} p_1(w) & p_2(w) \\ 0 & 1 \end{pmatrix}.$$

Równanie w słowach $u = v$ wyznacza równanie diofantyczne $e(u, v)$ równe

$$(p_1(u) - p_1(v))^2 + (p_2(u) - p_2(v))^2 = 0.$$

W ten sposób dowolny układ równań w słowach U wyznacza układ równań diofantycznych $e(U)$.

Przypuśćmy, że rozważamy układ U. Na mocy wniosku 14.5, układ $e(U)$ jest równoważny skończonemu podukładowi. Ten podukład jest postaci $e(U')$ dla pewnego skończonego zbioru $U' \subseteq U$. Pokażemy, że układy U i U' są równoważne. Aby to zrobić, wystarczy pokazać, że rozwiązanie dowolne rozwiązanie układu U' spełnia wszystkie równania z układu U.

Przypuśćmy, że rozważamy rozwiązania równań ze zmiennymi z V przyjmujące wartości w zbiorze A^*. Ponieważ półgrupa $\mathcal{A}$ z lematu 15.1 jest wolna, więc zawiera podpółgrupę izomorficzną z A^*. Dzięki temu ograniczyć się do rozważania rozwiązań, które przyjmują wartości w $\mathcal{A}$.

Niech α będzie dowolnym homomorfizmem przekształcającym V^* w $\mathcal{A}$. Przyjmijmy, że homomorfizm α przyporządkowuje zmiennej x_i macierz

$$\begin{pmatrix} y(i) & z(i) \\ 0 & 1 \end{pmatrix}.$$

Homomorfizm α wyznacza więc pewien układ liczb $x(1), \ldots, x(n), y(1), \ldots, y(n)$. Układ ten będziemy oznaczać symbolem $\tilde{\alpha}$.

Dla dowolnego słowa $u \in V^*$ macierz $\alpha(u)$ możemy liczyć na dwa, równoważne sposoby. Albo zmienne postaci x_i w słowie u zastępujemy macierzami $\varphi(x_i)$, obliczamy macierz $\varphi(u)$ wykonując obliczenia symboliczne i w końcu w otrzymanej macierzy podstawiamy liczby z układu $\tilde{\alpha}$, albo też zmienną x_i w słowie u zastępujemy macierzą $\alpha(x_i)$, a następnie mnożymy odpowiednie macierze liczbowe. Ponieważ oba sposoby liczenia dają ten sam wynik, więc

$$\alpha(u) = \begin{pmatrix} p_1(u)(\tilde{\alpha}) & p_2(u)(\tilde{\alpha}) \\ 0 & 1 \end{pmatrix}. \tag{2}$$

Jeżeli α jest rozwiązaniem równania $u = v$, to stosując wzór (2) do obu stron równania pokazujemy, że $\tilde{\alpha}$ jest rozwiązaniem równania $e(u, v)$.

Przypuśćmy teraz, że α jest rozwiązaniem układu U' oraz $u = v$ jest jednym z równań układu U. Jeżeli α jest rozwiązaniem U', to $\tilde{\alpha}$ jest rozwiązaniem układu $e(U')$. W tej sytuacji $\tilde{\alpha}$ jest także rozwiązaniem układu $e(U)$, a więc w szczególności jest rozwiązaniem równania $e(u, v)$. Mamy więc

$$(p_1(u)(\tilde{\alpha}) - p_1(v)(\tilde{\alpha}))^2 + (p_2(u)(\tilde{\alpha}) - p_2(v)(\tilde{\alpha}))^2 = 0.$$

Wobec tego,

$$p_1(u)(\tilde{\alpha}) = p_1(v)(\tilde{\alpha}) \ \text{ oraz } \ p_2(u)(\tilde{\alpha}) = p_2(v)(\tilde{\alpha}).$$

Stąd i z wzoru (2) wynika, że α jest rozwiązaniem równania $u = v$. $\square$

Wniosek 15.4 *Każdy układ równań w słowach ze skończoną liczbą zmiennych i stałych zawiera równoważny podukład skończony.* $\square$

Układ równań nazywamy niezależnym wtedy i tylko wtedy, gdy nie jest równoważny ze swoim właściwym podukładem.

Wniosek 15.5 *Każdy niezależny układ równań w słowach ze skończoną liczbą zmiennych jest skończony.* $\square$

16 Zbiory regularne

Zbiór X zawarty w półgrupie M jest regularny wtedy i tylko wtedy, gdy należy do najmniejszej rodziny podzbiorów M zamkniętej ze względu na sumę mnogościową, iloczyn (kompleksowy) i domknięcie Kleenego, oraz zawierającej wszystkie skończone podzbiory M.

Lemat 16.1 $X^+ = X^*X$ *oraz* $X^* = X^+ \cup \{\varepsilon\}$. □

17 Automaty (transducers, przetworniki (?))

Niech M będzie dowolną półgrupą (z jednością lunb nie). Rozważamy grafy skierowane (zwykle skończone), których krawędzie są etykietowane elementami M, i w których jest wyróżniony wierzchołek początkowy oraz jeden lub kilka wierzchołków końcowych. Krawędź może zaczynać się i kończyć w tym samym wierzchołku, krawędzie są jednoznacznie wyznaczone przez początek, koniec i etykietę. Krawędź prowadzącą od wierzchołka w_1 do w_2 z etykietą g będziemy oznaczać oznaczać symbolem

$$w_1 \xrightarrow[g]{} w_2.$$

Scieżką w grafie nazywamy ciąg wierzchołków i etykiet $w_0, g_1, w_1, g_2, w_2, \ldots, g_n, w_n$ taki, że w_i są wierzchołkami, a g_i są etykietami oraz dla dowolnego $i < n$ z wierzchołka w_i wychodzi krawędź etykietowana elementem g_{i+1} i kończąca się w wierzchołku w_{i+1}, a więc taki, że

$$w_0 \xrightarrow[g_1]{} w_1 \xrightarrow[g_2]{} w_2 \xrightarrow[g_3]{} \ldots \xrightarrow[g_{n-1}]{} w_{n-1} \xrightarrow[g_n]{} w_n. \tag{3}$$

Liczba n jest nazywana długością ścieżki (3), ścieżka może mieć długość 0 (taka ścieżka to właściwie wierzchołek rozpoczynający ścieżkę, będziemy ją nazywać pustą). Ścieżka (3) wyznacza element $g_1 g_2 \ldots g_n \in M$, ścieżka pusta wyznacza jedność półgrupy. Fakt, że istnieje ścieżka zaczynająca się w wierzchołku w_1, kończąca się w wierzchłku w_2 i wyznaczająca element $g \in M$ wyrażamy pisząc

$$w_1 \xrightarrow[g]{*} w_2.$$

Graf akceptuje $g \in M$ wtedy i tylko wtedy, gdy istnieje w nim ścieżka (także pusta) wierzchołka początkowego do końcowego wyznaczająca g. Zbiór wszystkich elementów akceptowanych przez graf G nazywamy zbiorem akceptowanym przez G. Rozważane grafy można uważać za uogólnienie automatu niedeterministycznego.

Lemat 17.1 *Podzbiory regularne są akceptowalne.* □

Twierdzenie 17.2 *Podzbiory akceptowalne są regularne.*

Dowód. Dowód przez indukcję ze względu na sumę liczby wierzchołków i liczby krawędzi grafu. Bierzemy graf G akceptujący zbiór L.

Przypadek 1: w G jest wierzchołek w różny od początkowego i końcowego taki, że żadna ścieżka akceptująca nie przechodzi przez w.

Wtedy wyrzucamy z grafu G ten wierzchołek i otrzymujemy graf G^w akceptujący język L^w. Oczywiście $L = L^w$ i teza wynika z założenia indukcyjnego.

Przypadek 2: w G jest wierzchołek w różny od początkowego i końcowego, do którego dociera pewna krawędź, i z którego wychodzi pewna krawędź.

Niech G^w będzie grafem G bez wierzchołka w (wyrzucamy wszystkie krawędzie zaczynające się i kończące się w w), Przyjmujemy, że G^w akceptuje język L^w. Niech $G^{out(w)}$ będzie grafem G bez krawędzi wychodzących z w, z wierzchołkiem w uznanym za jedyny wierzchołek końcowy. Podobnie, $G^{in(w)}$ otrzymujemy z G wyrzucając krawędzie wchodzące do w i uznając w za wierzchołek początkowy. Przyjmijmy, że grafy te akceptują zbiory $L^{out(w)}$ i $L^{in(w)}$.

Dla każdej krawędzi zaczynającej się w wierzchołku x, kończącej się wierzchołkiem w i etykietowanej słowem $s(x)$ definiujemy graf $G_x^{in(w)}$ wyrzucając z G krawędzie wchodzące do w, uznając w za wierzchołek początkowy i x za (jedyny) wierzchołek końcowy. Przyjmijmy, że graf ten akceptuje język $L_x^{in(w)}$.

Niech $L_w = L_{x_1}^{in(w)} s(x_1) \cup \ldots \cup L_{x_n}^{in(w)} s(x_n)$, gdzie $x_1, \ldots, x_n$ są wszystkimi wierzchołkami, z których wychodzi krawędź kończąca się w w (L_w jest właściwie sumą po wszystkich krawędziach, a nie po wszystkich wierzchołkach początkowych, utożsamiając krawędź z jej początkiem upraszczamy zapis).

Nietrudno zauważyć, że $L = L^w \cup L^{out(w)} L_w^* L^{in(w)}$. $\square$

18 Równania mające rozwiązanie α

Rozważamy równania bez stałych nad alfebetem Ξ i rozwiązania takich równań w półgrupie A^*. Równania można uważać za elementy zbioru $\Xi^* \times \Xi^*$. Jest to półgrupa. Dla homomorfizmu α definiujemy zbiór równań $E(\alpha)$ mających rozwiązanie α. Nietrudno zauważyć, że $E(\alpha)$ jest podpółgrupą $\Xi^* \times \Xi^*$.

Twierdzenie 18.1 *Zbiór $E(\alpha)$ jest regularny.*

Dowód. Przyjmijmy, że $\Xi = \{x_1, \ldots, x_n\}$. Możemy założyć, że $\alpha(x_i) \neq \varepsilon$.

Zdefiniujemy graf, którego wierzchołami będą pary postaci $[a, \varepsilon]$ oraz $[\varepsilon, a]$ takie, że a jest właściwym ($\neq \alpha(x_i)$) sufiksem jednego ze słów $\alpha(x_i)$. Graf ten składa się z krawędzi wymienionych w tabelce 1. Za wierzchołek początkowy i końcowy uznajemy $[\varepsilon, \varepsilon]$.

Zauważmy, że jeżeli $[a, a'] \xrightarrow[(x,y)]{} [b, b']$ jest krawędzią, to $a'\alpha(x)b = a\alpha(y)b'$. Łatwo sprawdzić, że jeżeli $[a, a'] \xrightarrow[(u,v)]{*} [b, b']$, to także $a'\alpha(u)b = a\alpha(v)b'$. Tak więc zbiór akceptowany przez G jest zawarty w $E(\alpha)$.

Jeżeli $[a, a']$ i $[b, b']$ są wierzchołkami grafu G i $a'\alpha(u)b = a\alpha(v)b'$, to $[a, a'] \xrightarrow[(u,v)]{*} [b, b']$. Dowodzimy to przez indukcję ze względu na sumę długości u i v. Z przytoczonej własności wynika, że równania spełnione przez α są akceptowane przez G. $\square$

Krawędź	Warunek
$[\varepsilon, \varepsilon] \xrightarrow[(x,y)]{} [\varepsilon, b]$	$\alpha(x) = \alpha(y)b$
$[\varepsilon, \varepsilon] \xrightarrow[(x,y)]{} [b, \varepsilon]$	$\alpha(x)b = \alpha(y)$
$[a, \varepsilon] \xrightarrow[(x,\varepsilon)]{} [b, \varepsilon]$	$a \neq \varepsilon \wedge a = \alpha(x)b$
$[a, \varepsilon] \xrightarrow[(x,\varepsilon)]{} [\varepsilon, b]$	$a \neq \varepsilon \wedge ab = \alpha(x)$
$[\varepsilon, a] \xrightarrow[(\varepsilon,y)]{} [\varepsilon, b]$	$a \neq \varepsilon \wedge a = \alpha(y)b$
$[\varepsilon, a] \xrightarrow[(\varepsilon,y)]{} [b, \varepsilon]$	$a \neq \varepsilon \wedge ab = \alpha(y)$

Rysunek 1: Krawędzie i warunki, pod którymi krawędzie te są dołączane do grafu