36 O równaniach wykładniczych

36.1 Pewne, dwupiętrowe równania wykładnicze

W kilku następnych lematach będziemy zajmować się dwoma słowami ustalonymi S i C takimi, że

$$S \text{ jest proste i } CS \neq SC. \tag{28}$$

Zauważmy, że słowa S i C spełniające powyższy warunek są niepuste.

Lemat 36.1 *Przypuśćmy, że (28) i mamy słowa A i B, oraz liczbę σ taką, że $|AS^\sigma| \geqslant |BS| \geqslant |AS|$. Jeżeli $AS^\sigma CS^\sigma U = BS^\sigma CV$ dla pewnych słów U i V, to $A = B$.*

Dowód. Weźmy maksymalne i takie, że $AS^i \leqslant B$. To i jest $< \sigma$. Odejmując od obu stron równości prefiks AS^i otrzymujemy $S^{\sigma-i}CS^\sigma U = B'S^\sigma CV$ dla pewnego słowa B' krótszego niż S. Ponieważ $BS \leqslant AS^\sigma$, więc $B'S \leqslant S^{\sigma-i}$. Stąd i z założenia o tym, że S jest proste wynika, że $B' = \varepsilon$. Wobec tego, równość $S^{\sigma-i}CS^\sigma U = B'S^\sigma CV$ implikuje, że $CS^i = S^iC$. Tak więc S^i oraz C są potęgami pewnego słowa T. Przyjmijmy, że $S^i = T^j$.

Ponieważ $B' = \varepsilon$, więc gdy $i = 0$, to mamy $A = B$. W pozostałych przypadkach pokażemy, że słowa S i C komutują, a to jest sprzeczne z założeniem. Wobec tego pozostałe przypadki nie mogą zajść. Jeżeli $i = 1$, to S i C komutują jako potęgi tego samego słowa. Jeżeli $i \geqslant 2$ i $j = 1$, to C jest potęgą S i komutuje z S. Jeżeli $i, j \geqslant 2$, to S i T, a więc także S i C są potęgami tego słowa i komutują. □

Lemat 36.2 *Przypuśćmy, że (28) i mamy słowa A i B, oraz liczbę σ taką, że $|AS^\sigma| \geqslant |BS|$ i $|BS^\sigma| \geqslant |AS|$. Jeżeli $AS^\sigma CS^\sigma U = BS^\sigma CS^\sigma V$ dla pewnych słów U i V, to $A = B$.*

Dowód. Przypuśćmy, że $|B| \geqslant |A|$. Wtedy $|AS^\sigma| \geqslant |BS| \geqslant |AS|$ i – na podstawie poprzedniego lematu – mamy $A = B$. W drugim, możliwym przypadku lemat dowodzimy tak samo. □

Lemat 36.3 *Przypuśćmy, że (28) i mamy słowa A i B, oraz liczbę σ taką, że $|S^\sigma| \geqslant |ABS|$. Jeżeli $AS^\sigma CS^\sigma U = BS^\sigma CS^\sigma V$ dla pewnych słów U i V, to $A = B$.*

Dowód. Jeżeli $|S^\sigma| \geqslant |ABS|$, to także $|AS^\sigma| \geqslant |A^2BS| \geqslant |BS|$ oraz $|BS^\sigma| \geqslant |AB^2S| \geqslant |AS|$. Teza wynika z poprzedniego lematu. □

Lemat 36.4 *Przypuśćmy, że (28) i mamy liczbę σ taką, że $|S^\sigma| \geqslant |A_1CS|$. Jeżeli*

$$[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=1}^m = [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=1}^n,$$

$\lambda_2 > 0$ i $\lambda_1 < \mu_1 - 1$, to $m \geqslant 2$ i $A_1 = C$.

Dowód. Oczywiście,

$$A_1[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=2}^m = C(S^\sigma C)^{\mu_1-\lambda_1-1} S^\sigma B_1[(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=2}^n.$$

Równość $m = 1$ implikuje, że $|A_1| \geqslant |S^\sigma|$, a to przeczy założeniu. Dalej wystarczy skorzystać z poprzedniego lematu. □

Lemat 36.5 *Przypuśćmy, że* (28) *i mamy liczbę σ taką, że $\mid S^\sigma \mid \geqslant \mid A_1CS \mid, \mid B_1CS \mid$. Jeżeli dla pewnych $\lambda_i, \mu_i \geqslant 2$ zachodzi równość*

$$[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=1}^m = [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=1}^n,$$

to zachodzi jeden z następujących warunków:

1) $\lambda_1 = \mu_1$ *i* $A_1 = B_1$,

2) $\lambda_1 = \mu_1 + 1$ *i* $B_1 S^k C = C S^k A_1$ *dla dowolnego* $k \geqslant 0$,

3) $\lambda_1 + 1 = \mu_1$ *i* $A_1 S^k C = C S^k B_1$ *dla dowolnego* $k \geqslant 0$,

4) $\lambda_1 + 1 < \mu_1$ *i* $A_1 = C$,

5) $\lambda_1 > \mu_1 + 1$ *i* $B_1 = C$.

Dowód. Jeżeli $\lambda_1 + 1 < \mu_1$, to z poprzedniego lematu otrzymujemy, że $A_1 = C$. Tak samo dowodzimy, że $B_1 = C$ w przypadku, gdy $\lambda_1 > \mu_1 + 1$. Jest oczywiste, że $A_1 = B_1$, jeżeli $\lambda_1 = \mu_1$ i $n = m = 1$. Zauważmy, że $n + m > 3$. W przeciwnym razie jedno ze słów A_1 lub B_1 byłoby dłuższe niż S^σ, a to przeczy założeniu. Jeżeli $\lambda_1 = \mu_1$ i $n, m \geqslant 2$, to równość $A_1 = B_1$ wynika z jednego z poprzednich lematów.

Załózmy teraz, że $\lambda_1 + 1 = \mu_1$. Wtedy

$$A_1[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=2}^m = CS^\sigma B_1[(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=2}^n,$$

Co więcej, $m \geqslant 2$, gdyż w przeciwnym razie A_1 byłoby dłuższe niż S^σ. Jeżeli $m \geqslant 2$, to z tego samego powodu zachodzi nierównosć $n \geqslant 2$. Wobec tego,

$$A_1(S^\sigma C)^{\lambda_2} S^\sigma A_2[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=3}^m = CS^\sigma B_1(S^\sigma C)^{\mu_2} S^\sigma B_2[(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=3}^n.$$

Będziemy porównywać A_1 i C. Jeżeli A_1 jest krótsze, to $C = A_1 S^i$ dla pewnego $i < \sigma$ oraz (podstawiamy za C, skracamy i ponownie dopisujemy A_1)

$$A_1C(S^\sigma C)^{\lambda_2 - 1} S^\sigma A_2[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=3}^m = CB_1(S^\sigma C)^{\mu_2} S^\sigma B_2[(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=3}^n.$$

Stąd, korzystając z założenia $\lambda_2 \geqslant 2$ otrzymujemy, że $A_1C = CB_1$. Ponieważ $C = A_1S^i$, więc także $C = S^iB_1$. Z tych dwóch równości bez trudu wyprowadzamy wzór $CS^kB_1 = A_1S^kC$. Jeżeli A_1 jest przynajmniej tak długie, jak C, to wzór ten dowodzimy analogicznie.

W przypadku $\lambda_1 > \mu_1 + 1$ przeprowadzamy symetryczny dowód. □

Lemat 36.6 *Przypuśćmy, że* (28)*. Liczba σ taką, że $|S^\sigma| \geqslant |A_1CS|, |B_1CS|$ i liczby $\lambda_i, \mu_i \geqslant 2$ spełniają równanie*

$$[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=1}^m = [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=1}^n$$

wtedy i tylko wtedy, gdy spełniają jeden z następujących układów:

1) $\lambda_1 = \mu_1$, $A_1 = B_1$ *i* $[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=2}^m = [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=2}^n$,

2) $\lambda_1 = \mu_1 + 1$, $B_1 S^k C = C S^k A_1$ *dla dowolnego* $k \geqslant 0$ *i*
$(S^\sigma C)^{\lambda_2+1} S^\sigma A_2 [(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=3}^m = [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=2}^n$,

3) $\lambda_1 + 1 = \mu_1$, $A_1 S^k C = C S^k B_1$ *dla dowolnego* $k \geqslant 0$ *i*
$[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=2}^m = (S^\sigma C)^{\mu_2+1} S^\sigma B_2 [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=3}^n$,

4) $A_1 = C$ *i* $(S^\sigma C)^{\lambda_1+\lambda_2+1} S^\sigma A_2 [(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=3}^m = [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=1}^n$,

5) $B_1 = C$ *i* $[(S^\sigma C)^{\lambda_i} S^\sigma A_i]_{i=1}^m = (S^\sigma C)^{\mu_1+\mu_2+1} S^\sigma B_2 [(S^\sigma C)^{\mu_i} S^\sigma B_i]_{i=3}^n$,

Dowód. Nietrudno zauważyć, że jeżeli spełnione są wymienione układy równań, to także jest spełnione podane równanie. Implikacja odwrotna wynika z poprzedniego lematu. □

36.2 Uproszczone słowa parametryczne

Zbiór jednopiętrowych słów parametrycznych to najmniejszy spośród zbiorów X takich, że

1) dowolne słowa należą do X,

2) jeżeli w jest słowem i x jest zmienną, to $w^x \in X$,

3) jeżeli $w_1 \in X$ i $w_2 \in X$, to $w_1 w_2 \in X$.

Zmiennym w słowach parametrycznych przyporządkowujemy liczby naturalne. Dla danego wartościowania zmiennych definiujemy w naturalny i oczywisty sposób wartość parametrycznego słowa przy danym wartościowaniu.

Umawiamy się, że $w^x w^y = w^{x+y}$, $w^x w^2 = w^{x+2}$, $w^x w^x = w^{2\cdot y}$ i przyjmujemy inne umowy podobne do podanych. Zgodnie z tymi umowami każde jednopiętrowe słowo parametryczne ma postać

$$P_0 [S_i^{L_i} P_i]_{i=1}^n \tag{29}$$

gdzie $P_0, \ldots, P_n$ oraz $S_1, \ldots, S_n$ są słowami, a L_i są liniowymi wielomianami o współczynnikach i wyrazach wolnych będących liczbami naturalnymi.

Słowo (29) nazywamy **uproszczonym**, jeżeli

1) słowa S_i mają tę samą długość,

2) dla $i = 1, \ldots, n$, jeżeli $P_{i-1} \neq \varepsilon$, to ostatnie litery słów P_{i-1} i S_i są różne,

3) dla $i = 2, \ldots, n$, słowo S_{i-1} nie jest odcinkiem początkowym słowa $P_{i-1} S_i$,

4) słowo S_n nie jest odcinkiem początkowym słowa P_n.

Parametryczne słowa $\varphi(t_1, \ldots, t_n)$ i $\psi(t_1, \ldots, t_n)$ są **równoważne w dziedzinie** $\mathcal{P}(t_1, \ldots, t_n)$, jeżeli

$$\mathcal{P}(t_1, \ldots, t_n) \Rightarrow \varphi(t_1, \ldots, t_n) = \psi(t_1, \ldots, t_n).$$

Lemat 36.7 *Załóżmy, że słowa A_i mają tę samą długość. Parametryczne słowo*

$$P_0[A_i^{L_i} P_i]_{i=1}^n \tag{30}$$

jest równoważne w dziedzinie $L_1, \ldots, L_n > 0$ pewnemu uproszczonemu słowu.

Dowód. Dowód będzie polegać na powodowaniu, że dla kolejnych wartości $i = 0, \ldots, n$ spełnione są warunki 2), 3) i 4) z definicji słowa uproszczonego.

Pokażemy, jak można zagwarantować spełnianie warunku 2) dla pewnego i. Niech P będzie najdłuższym słowem takim, że $P_{i-1} = P'P$ i $A_i = A'P$. Wtedy

$$P_{i-1}A_i^{L_i} = P'P(A'P)^{L_i} = P'(PA')^{L_i}P.$$

Wobec tego słowo P_{i-1} zastępujemy przez P', a $A_i = A'P$ przez PA'. Oczywiście, warunek 1) nadal pozostaje prawdziwy.

Teraz zajmiemy się warunkiem 3. Załóżmy, że $i \geqslant 2$. Jeżeli A_{i-1} jest odcinkiem początkowym słowa P_{i-1}, to przedstawiamy słowo P_{i-1} w postaci $A_{i-1}^a P$ i odpowiednio zmieniamy wzór (30) zwiększając wykładnik L_{i-1} o a. Na tym przykształcenia kończymy w przypadku, gdy A_{i-1} nie jest odcinkiem początkowym PA_i.

Przypuśćmy, że A_{i-1} jest odcinkiem początkowym PA_i, ale nie jest odcinkiem początkowym słowa P. Wtedy $A_{i-1} = PQ$ dla pewnego Q. Niech b będzie największą liczbą taką, że A_{i-1}^b jest odcinkiem początkowym PA_i^2. Mamy $PA_i^2 = (PQ)^b V = P(QP)^{b-1}QV$ dla pewnego V. Stąd $A_i^2 = (QP)^{b-1}QV$. Jest też oczywiste, że $1 \leqslant b \leqslant 2$.

Przypadek 1: $b = 2$. Ze wzoru $A_i^2 = (QP)^{b-1}QV$ i równości $|\, A_i \,| = |\, A_{i-1} \,| = |\, PQ \,|$ wynika, że $A_i = QP$. W tym przypadku fragment

$$A_{i-1}^{L_{i-1}} P_{i-1} A_i^{L_i}$$

słowa (30) możemy zastąpić przez równoważne mu słowo

$$A_{i-1}^{L_{i-1}+a+L_i} P.$$

Przypadek 2: $b = 1$. W tym przypadku $A_i^2 = QV$ dla pewnego V takiego, że A_{i-1} nie jest odcinkiem początkowym V. Oczywiście $V = RA_i$ dla pewnego R, oraz $A_i = QR$.

Zauważmy, że $L_i \geqslant 1$. Nierówność ta (potrzebna w dowodzie pierwszej równości) implikuje, że

$$\begin{aligned} &A_{i-1}^{L_{i-1}} P_{i-1} A_i^{L_i} = A_{i-1}^{L_{i-1}+a} PA_i A_i^{L_i-1} = A_{i-1}^{L_{i-1}+a} PQRA_i^{L_i-1} \\ &= A_{i-1}^{L_i+a+1} R(QR)^{L_i-1} = A_{i-1}^{L_i+a+1} (RQ)^{L_i-1} R. \end{aligned}$$

Pierwsze z wymienionych słów może więc zostać zastąpione przez ostatnie. Warunek 2) jest oczywiście spełniony. Słowo A_{i-1} nie jest odcinkiem początkowym RQ, ponieważ długości tych słów są równe i A_{i-1} nie jest odcinkiem początkowym $V = RS_i = RQR$. Tak więc jest spełniony warunek 3).

Spełnienie warunku 4) jest łatwe do uzyskania. □

Będziemy rozważać jednopiętrowe równania wykładnicze

$$P_0[A^{L_i}P_i]_{i=1}^n = Q_0[A^{M_i}Q_i]_{i=1}^m, \tag{31}$$

w których obie strony są jednopiętrowymi słowami parametrycznymi.

Lemat 36.8 *Jednopiętrowe równanie wykładnicze* (31) *jest równoważne w dziedzinie*

$$L_1, \ldots, L_n, M_1, \ldots, M_m > 0$$

pewnemu równaniu o uproszczonych stronach.

Dowód. Jest to konsekwencja lematu 36.7. □

Lemat 36.9 *Niech*

$$P_0[A_i^{L_i}P_i]_{i=1}^n = Q_0[B_i^{M_i}Q_i]_{i=1}^m \tag{32}$$

będzie równaniem o uproszczonych stronach, $|\,A_1\,| = |\,B_1\,|$ *i*

$$G = \max\{|\,|\,P_i\,| - |\,Q_i\,|\,| : i = 0, 1, \ldots, \min\{n, m\}\}.$$

Jeżeli równanie (32) *ma rozwiązanie spełniające warunki*

$$L_1, \ldots, L_n, M_1, \ldots, M_m \geqslant 1 + \frac{G}{|\,A_1\,|},$$

to $n = m$, $P_0 = Q_0$, *oraz dla* $i = 1, \ldots, n$ *zachodzą równości* $P_i = Q_i$, $A_i = B_i$ *i* $L_i = M_i$.

Dowód. Dowodzimy ten lemat przez indukcję ze względu na $\max(n, m)$. Jest on oczywisty, jeżeli $\max(n, m) = 0$.

Zauważmy, że $n > 0$ wtedy i tylko wtedy, gdy $m > 0$. Gdyby bowiem $n > 0$ i $m = 0$, to $P_0A_1^{L_1} \leqslant Q_0$. Stąd $L_1|\,A_1\,| \leqslant G$ oraz $(L_1+1)|\,A_1\,| \leqslant G + |\,A_1\,| \leqslant L_1|\,A_1\,|$, a to nie jest możliwe.

Załóżmy, że $|P_0| \geqslant |Q_0|$. Ponieważ $M_1 \geqslant 1 + \frac{G}{|\,A_1\,|}$, więc słowo $Q_0B_1^{M_1}$ jest dłuższe od P_0A_1. Z równości (32) otrzymujemy, że $P_0A_1 \leqslant Q_0B_1^{M_1}$. Weźmy maksymalne k takie, że $Q_0B_1^kU = P_0$ dla $U < B_1$ oraz V takie, że $B_1 = UV$. Mamy też $Q_0B_1^{k+1} \leqslant P_0A_1 \leqslant Q_0B_1^{M_1}$. Niech więc X i Y będą takie, że $P_0A_1 = Q_0B_1^{k+1}X$ oraz $P_0A_1Y = Q_0B_1^{k+2}$. Wobec tego, $XY = B_1 = UV$ oraz $UA_1 = B_1X$. Stąd $|U| = |X|$, $U = X$ oraz $Y = V$. W końcu otrzymujemy, że $A_1 = VX = VU$. Gdyby $U \neq \varepsilon$, to słowa P_0 i A_1 kończyłyby się tą samą literą. a to nie jest możliwe. Więc $U = \varepsilon$, $A_1 = B_1$ oraz $Q_0B_1^k = P_0$. Wobec tego założenie, że $k > 0$ też prowadzi do sprzeczności w ten sam sposób. Ostatecznie, $P_0 = Q_0$ i $A_1 = B_1$.

Załóżmy teraz, że $L_1 > M_1$. Równość (32) przyjmuje teraz postać

$$A_1^{L_1-M_1}P_1[A_i^{L_i}P_i]_{i=2}^n = Q_1[B_i^{M_i}Q_i]_{i=2}^m.$$

Jeżeli $m = 1$, to równość $A_1 = B_1$ oznacza, że B_1 jest prefiksem Q_1, a to przeczy warunkowi (4) z definicji słowa uproszczonego. Jeżeli $m > 1$, to B_1 jest prefiksem Q_1B_2 i otrzymujemy sprzeczność z warunkiem (3) z definicji słowa uproszczonego.

Tak więc $M_1 = L_1$ oraz

$$P_1[A_i^{L_i}P_i]_{i=2}^n = Q_1[B_i^{M_i}Q_i]_{i=2}^m. \tag{33}$$

Do tego równania możemy zastosować założenie indukcyjne. W ten sposób otrzymamy tezę. □