Równania na słowach

Wojciech PLANDOWSKI[*]

Aby mówić o równaniach na słowach, trzeba zacząć od definicji słowa. W języku potocznym słowem jest ciąg liter, któremu przypisane jest pewne znaczenie. Słowem jest więc „pociąg", „wieża", „samochód". W matematyce słowem określa się *dowolny* ciąg liter, np. „abaab". Równaniem na słowach nazywamy równanie, w którym po obu stronach występują słowa składające się z liter. Litery dzielą się na *stałe* i *niewiadome*. My będziemy oznaczać niewiadome wielkimi literami, stałe zaś małymi literami. Równaniem na słowach jest, na przykład, $XabY = YbaX$, w którym niewiadomymi są X i Y, stałymi zaś a i b. *Rozwiązaniem* równania jest takie podstawienie słów za niewiadome, aby po wstawieniu ich do równania po obu stronach otrzymać to samo słowo. Rozwiązaniem równania $XabY = YbaX$ jest, na przykład, $X = bab$, $Y = babab$, bo wtedy $XabY = bababbabab = YbaX$.

W tym artykule powiemy, jak rozwiązywać najprostsze nietrywialne równania na słowach. Okazuje się, że nie jest to zadanie proste i wymaga udowodnienia kilku lematów dotyczących własności słów. Równania najprostsze to, jak można się spodziewać, równania z jedną niewiadomą. Do tej pory jednak nie wszystko wiadomo o takich równaniach. Na przykład nie wiadomo, ile rozwiązań może mieć takie równanie. Są przykłady równań mających 0, 1, 2 lub nieskończenie wiele rozwiązań. Nie wiadomo, czy równanie takie może mieć dokładnie trzy rozwiązania. Musimy więc jeszcze bardziej uprościć zadanie: ograniczymy liczbę wystąpień niewiadomej w równaniu.

Jeśli niewiadoma występuje dokładnie raz, to sprawa jest prosta. Wtedy równanie jest postaci $uXv = w$, przy czym u, v, w to słowa niezawierające niewiadomej. Równanie takie może mieć zero rozwiązań lub jedno rozwiązanie. Równanie $aXa = a$ ma zero rozwiązań, ponieważ bez względu na to, co podstawimy pod X, po lewej stronie będzie słowo dłuższe niż po prawej. Równanie $X = a$ ma jedno rozwiązanie. Równanie $uXv = w$ nie może mieć więcej niż jedno rozwiązanie, bo jeśli ma jakiekolwiek, to w musi się zaczynać od u i kończyć na v, a zatem $w = uxv$ dla pewnego x. Wtedy $X = x$ jest jedynym rozwiązaniem.

Przyjrzyjmy się teraz równaniom z dwoma wystąpieniami niewiadomej X. Są one albo postaci $uXvXw = z$, albo $uXv = u'Xv'$, gdzie u, v, w, z, u', v' są słowami niezawierającymi niewiadomej. Rozważmy najpierw pierwsze z równań. Aby miało ono rozwiązanie, z musi się zaczynać od u i kończyć na w. Wtedy $z = uz'w$, a więc $XvX = z'$. Przypuśćmy, że $X = x$ jest rozwiązaniem tego równania. Wtedy $xvx = z'$. Długość słowa po lewej stronie musi być taka sama jak długość słowa po prawej stronie. Jeśli długość słowa u oznaczymy przez $|u|$, to $2 \cdot |x| + |v| = |xvx| = |z'|$. Stąd $|x| = (|z'| - |v|)/2$. Długość rozwiązania x jest więc jednoznacznie wyznaczona przez długości z' i v. Ale z' musi się zaczynać od x. Jest tylko jedno słowo określonej długości, które zaczyna ustalone słowo, np. słowem długości 2 zaczynającym słowo *abaab* jest *ab*. Stąd jest tylko jeden kandydat na rozwiązanie. Albo ten kandydat jest rozwiązaniem, albo nie. Stąd równanie $uXvXw = z$ ma albo zero rozwiązań, albo jedno rozwiązanie.

Rozważmy teraz drugie równanie, tj. $uXv = u'Xv'$. Załóżmy najpierw, że $u = u'$. Wtedy albo $v = v'$ i każde słowo jest rozwiązaniem równania, albo $v \neq v'$ i wtedy równanie nie ma rozwiązań. Załóżmy teraz, że $u \neq u'$. Wtedy, jeśli równanie ma rozwiązanie, to albo u' jest początkiem u, albo u jest początkiem u'. Podobnie albo v' jest końcem v, albo v jest końcem v'. Usuwając wspólny początek i koniec obu stron równania, otrzymamy albo równanie $zXy = X$, albo równanie $zX = Xy$. Analizując długości lewej i prawej strony pierwszego równania, dojdziemy do wniosku, że nie może mieć ono rozwiązań.

[*]Instytut Informatyki,
Uniwersytet Warszawski

Pozostaje do rozwiązania równanie $zX = Xy$. I tu się zaczyna prawdziwa matematyka: definicje, lematy, twierdzenia. Najpierw zdefiniujemy *słowa pierwotne*. Są to słowa, które nie są postaci $uu\dots u$, przy czym u powtarza się co najmniej dwa razy. Słowem pierwotnym jest więc *ababa*, ale nie *abab*.

Przez u^k, dla $k \geqslant 1$, będziemy rozumieli słowo $uu\dots u$, przy czym u powtarza się dokładnie k razy. Przez u^0 rozumiemy specjalne słowo – słowo puste (będziemy oznaczać je 1), które składa się z zerowej liczby liter. Zauważmy, że $(u^k)^l = u^{kl}$ oraz $u^k u^l = u^{k+l}$, dla $k, l \geqslant 0$.

Lemat 1. *Zbiorem rozwiązań równania $XY = YX$ jest $\{X = u^k, Y = u^l$ dla $k, l \geqslant 0\}$.*

Dowód. Niech $X = x$, $Y = y$ będzie rozwiązaniem równania. Jeśli $|x| = 0$, to $x = 1$, a więc $X = y^0$ i $Y = y^1$. Podobnie rozważamy przypadek $|y| = 0$.

Załóżmy teraz, że x i y są niepustymi słowami. Stosujemy indukcję względem $|x| + |y|$. Jeśli $|x| + |y| = 2$, to $|x| = |y| = 1$. Mamy $xy = yx$, a zatem x jest początkiem y lub odwrotnie. Skoro x i y są tej samej długości, więc $x = y$. Stąd $X = x^1$, $Y = x^1$.

Załóżmy wreszcie, że $|x| + |y| > 2$. Wtedy albo $x = y$, albo x jest początkiem y, albo y jest początkiem x. W pierwszym przypadku nie ma czego dowodzić. Trzeci przypadek dowodzi się symetrycznie do drugiego. Pozostaje drugi. Mamy $y = xy'$. Stąd $xxy' = xy = yx = xy'x$. Skracając początkowe x po obu stronach równania, mamy $xy' = y'x$. Ponieważ x i y' są niepustymi słowami, więc $|x| + |y'| < |x| + |y|$. Można więc zastosować hipotezę indukcyjną do równania $xy' = y'x$. Mamy $y' = u^k$ i $x = u^l$. Wtedy $y = xy' = u^l u^k = u^{l+k}$. To kończy dowód. △

Lemat 2. *Każde niepuste słowo w można jednoznacznie przedstawić jako u^k dla pewnego pierwotnego słowa u i $k \geqslant 1$.*

Dowód. Najpierw udowodnimy, że w można przedstawić w postaci u^k, gdzie u jest słowem pierwotnym i $k \geqslant 1$. Jeśli w jest pierwotne, to $u = w$ i $k = 1$. Jeśli nie jest pierwotne, to dowód jest indukcyjny względem $|w|$. Wtedy w jest postaci v^k, przy czym $k \geqslant 2$, a więc $|v| < |w|$. Zgodnie z hipotezą indukcyjną v da się przedstawić w postaci u^l dla pewnego słowa pierwotnego u i $l \geqslant 1$. A zatem $w = (u^l)^k = u^{kl}$, gdzie u jest słowem pierwotnym i $kl \geqslant 2$.

Przypuśćmy teraz, że w da się przedstawić na dwa sposoby w postaci u^k i v^l, gdzie u i v są pierwotne. Gdyby było $k = 1$ lub $l = 1$, to w byłoby słowem pierwotnym, a więc musiałoby być $k = l = 1$ i w konsekwencji $u = v$. A zatem $k, l \geqslant 2$. Mamy $w = u^k = v^l$ i $k, l \geqslant 2$. Stąd $|w| = |u^k| = |v^l| \geqslant \max\{2 \cdot |v|, 2 \cdot |u|\} \geqslant |u| + |v|$. A zatem $|u| \leqslant (l-1) \cdot |v|$ oraz $|v| \leqslant (k-1) \cdot |u|$. Skoro u jest początkiem v^l, więc u jest na tyle krótkie, że jest początkiem v^{l-1}. Podobnie v jest początkiem u^{k-1}. Stąd uv jest początkiem $uu^{k-1} = w$ i vu jest początkiem $vv^{l-1} = w$. Ponieważ uv i vu są tej samej długości, więc $uv = vu$. Z Lematu 1 mamy $u = p^i$ i $v = p^j$. Ponieważ u i v są pierwotne, więc $i = j = 1$ i w konsekwencji $u = v$ i $k = l$. △

Niech x będzie niepustym słowem. Przez $c(x)$ oznaczamy słowo powstałe z x przez przestawienie pierwszej litery x na koniec. Na przykład, $c(aba) = baa$, $c(baa) = aab$. Zauważmy, że jeśli $i < |x|$, to i-krotne zastosowanie funkcji c do słowa x polega na przestawieniu pierwszych i liter x na jego koniec. Słowo y nazwiemy *obrotem cyklicznym* słowa x, jeśli y można otrzymać z x poprzez zero-, jedno- lub więcej-krotne zastosowanie funkcji c do x. Jeśli y jest obrotem cyklicznym x, to y powstaje z x przez przestawienie jakiegoś początku słowa x na jego koniec, a zatem istnieją takie słowa p i q, że $y = pq$ i $x = qp$ (przestawiamy q). Z drugiej strony, jeśli istnieją takie słowa p i q, że $y = pq$ i $x = qp$, to y jest obrotem cyklicznym słowa x, bo powstało przez przestawienie q z początku x na jego koniec. Zachodzi zatem następujący fakt.

Obserwacja. *Słowo y jest obrotem cyklicznym słowa x wtedy i tylko wtedy, gdy istnieją takie słowa p i q, że $y = pq$ i $x = qp$.*

Rozwiązanie zadania M 1291.
Dla każdego i zaznaczmy wspólny bok tych dwóch pól, na których znajdują się liczby i oraz $i+1$. Teza zadania będzie spełniona, jeśli wykażemy, że istnieje wierzchołek (punkt kratowy szachownicy), z którego wychodzą trzy odcinki.

Przyjmijmy wbrew tezie, że taki wierzchołek nie istnieje. Wówczas w każdym wierzchołku wewnątrz szachownicy spotykają się co najwyżej dwa zaznaczone odcinki. Ponadto do każdego wierzchołka na brzegu szachownicy może dochodzić tylko jeden odcinek, przy czym żaden odcinek nie dochodzi do rogów szachownicy. Stąd wynika, że liczba zaznaczonych odcinków nie może przekraczać

$$\frac{1}{2}(2(m-1)(n-1) + 2(n-1) + 2(m-1)) = mn - 1.$$

Tymczasem wszystkich zaznaczonych odcinków jest dokładnie $mn - 1$. Stąd w szczególności wynika, że każdy wierzchołek znajdujący się na brzegu szachownicy, z wyjątkiem jej rogów, musi być końcem jednego z zaznaczonych odcinków. Wobec tego, jeśli w któreś pole brzegowe szachownicy wpisano liczbę i, to liczby $i+1$ oraz $i-1$ też musiały zostać wpisane w brzegowe pola szachownicy. Wynika z tego, że wszystkie liczby są na brzegu – to jednak nie jest możliwe.

Teraz udowodnimy następujący lemat.

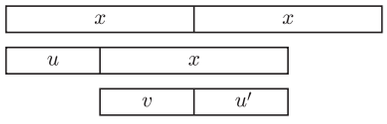
Lemat 3. *Obrót cykliczny słowa pierwotnego jest słowem pierwotnym.*

Dowód. Wystarczy dowieść, że funkcja c przekształca słowo pierwotne na słowo pierwotne. Przypuśćmy, że tak nie jest, to znaczy funkcja c przekształca słowo pierwotne x na słowo niepierwotne u^k, gdzie $k \geqslant 2$. Wtedy x powstaje z u^k przez przestawienie ostatniej litery u^k na początek. Litera ta jest ostatnią literą u. Jeśli oznaczymy $u' = c^{-1}(u)$, to $x = u'^k$ (sprawdź!), a zatem x nie jest pierwotne. Sprzeczność. $\triangle$

I jeszcze jeden lemat.

Lemat 4. *Niech y będzie obrotem cyklicznym słowa x. Jeśli x jest pierwotne, to istnieje dokładnie jedna para słów (p, q), gdzie $q \neq 1$, spełniająca $y = pq$, $x = qp$.*

Dowód. To, że taka para słów istnieje, wynika z Obserwacji. Przypuśćmy, że są dwie takie pary: (p, q) i (p', q'). Niech $0 \leqslant |p| < |p'| < |y| = |x|$. Wtedy słowo $x^2 = qpqp$ występuje w $y^3 = pqpqpq = px^2q$ od pozycji $|p| + 1$. Podobnie słowo x występuje w y^3 od pozycji $|p'| + 1$. To oznacza, że x występuje w x^2 od pozycji $1 < |p'| - |p| + 1 < |x|$, czyli x występuje w środku xx. To jest niemożliwe. Oznaczmy przez u początek xx, na prawo od którego występuje x (rysunek). Wtedy $x = uv$ i $x = vu'$, gdzie u' jest prefiksem x o długości $|x| - |v| = |uv| - |v| = |u|$. Ale u też jest prefiksem x o tej długości. A zatem $u' = u$ i mamy $x = uv = vu$ oraz u i v są niepuste. Z Lematu 1 wynika, że $u = r^k$ i $v = r^l$, a zatem $x = uv = r^{k+l}$. Ponieważ u i v są niepuste, więc $k, l \geqslant 1$, skąd $k + l \geqslant 2$. Uzyskaliśmy sprzeczność z założeniem o pierwotności x. $\triangle$



Słowo x występuje wewnątrz xx.

Teraz wróćmy do naszego równania $zX = Xy$. Niech $X = x$ będzie jego rozwiązaniem. Obliczając długości obu stron równania po podstawieniu $X = x$, otrzymamy $|z| = |y|$. Warunek $|z| = |y|$ jest więc warunkiem koniecznym do tego, aby rozwiązanie istniało. Nie jest to jednak warunek wystarczający.

Twierdzenie. *Niech $z = u^k$, $y = v^l$, gdzie u i v są pierwotne i $k, l \geqslant 1$.*

(i) *Równanie $zX = Xy$ ma rozwiązanie wtedy i tylko wtedy, gdy $k = l$ i v jest obrotem cyklicznym u.*

(ii) *Jeśli $u = qp$ i $v = pq$, gdzie $p \neq 1$, i $k = l$, to zbiorem rozwiązań równania $zX = Xy$ jest $\{(qp)^i q : i \geqslant 0\}$.*

Dowód. (i) ($\Leftarrow$) Jeśli v jest obrotem cyklicznym u, to $v = pq$ i $u = qp$, dla pewnych p, q. Wtedy, dla każdego $i \geqslant 0$, $z(qp)^i q = (qp)^{k+i} q = (qp)^i q(pq)^k = (qp)^i qy$. A zatem równanie $zX = Xy$ ma rozwiązanie. Ma ich nawet nieskończenie wiele.

($\Rightarrow$) Indukcja względem długości rozwiązania $X = x$. Jeśli $|x| < |u|$, to x jest prefiksem u, a zatem $u = xp$ dla pewnego niepustego p. Wtedy $xy = zx = (xp)^k x = x(px)^k$. Stąd $y = (px)^k$. Ponieważ xp jest pierwotne, więc px też jest pierwotne. Mamy $v^l = (px)^k$. Z Lematu 2, $k = l$ i $v = px$. Zauważmy, że ponieważ v i u są pierwotne, więc para (p, x) spełniająca $p \neq 1$, $u = xp$ i $v = px$ jest dokładnie jedna. Tak więc jedynym rozwiązaniem równania krótszym niż $|u|$ jest $X = x$.

Jeśli $|x| \geqslant |u|$, to u jest początkiem x. Stąd $x = ux'$ dla pewnego x'. Wtedy $uzx' = uu^k x' = u^k ux' = zx = xy = ux'y$. Usuwając wspólny początek obu stron równania, otrzymujemy $zx' = x'y$, a więc $X = x'$ jest rozwiązaniem równania $zX = Xy$. Skoro $|x'| < |x|$, więc można zastosować hipotezę indukcyjną, która mówi, że v jest obrotem cyklicznym u.

(ii) Załóżmy, że $u = qp$ i $v = pq$. Udowodnimy teraz, że każde rozwiązanie równania $zX = Xy$ jest postaci $(qp)^i q$, przy czym $i \geqslant 0$. W punkcie ($\Leftarrow$) udowodniliśmy, że każde słowo postaci $(qp)^i q$ jest rozwiązaniem równania. Pokażemy, że nie ma innych rozwiązań. Dowód jest indukcyjny względem długości rozwiązania. Załóżmy, że $X = x$ jest rozwiązaniem równania. W punkcie ($\Rightarrow$) udowodniliśmy, że jedynym rozwiązaniem równania krótszym niż $|u|$ jest $X = q$ oraz że każde rozwiązanie nie krótsze niż $|u|$ jest postaci ux', przy czym x' też jest rozwiązaniem równania. Z hipotezy indukcyjnej $x' = (qp)^i q$, gdzie $u = qp$ i $v = pq$. Wtedy $x = ux' = qp(qp)^i q = (qp)^{i+1} q$. To kończy dowód. $\triangle$

Rozwiązanie zadania M 1292.
Niech $p_1, p_2, \ldots, p_{100}$ będą różnymi liczbami pierwszymi.

Dla $n = 1, 2, \ldots, 100$ przyjmijmy

$$a_n = p_1 p_2 \ldots p_n p_{n+1}^2 \ldots p_{100}^2.$$

Wówczas zbiór $A = \{a_1, a_2, \ldots, a_{100}\}$ spełnia warunki zadania. Istotnie: jeśli $a_{n_1}, a_{n_2}, \ldots, a_{n_k}$ są elementami zbioru A, gdzie $n_1 < n_2 < \ldots < n_k$, to liczba $p_{n_k}^2$ dzieli każdą z liczb $a_{n_1}, a_{n_2}, \ldots, a_{n_{k-1}}$, lecz nie dzieli liczby a_{n_k}. Stąd wynika, że liczba $a_{n_1} + a_{n_2} + \ldots + a_{n_k}$ nie może być potęgą liczby naturalnej o wykładniku większym lub równym 2.