32 Algorytm Chmielewskiego

Algorytm Chmielewskiego bada niesprzeczność danego równania ze stałymi i trzema zmiennymi. Algorytm ten zostanie przedstawiony jednak przy założeniu, że otrzymuje równanie z dwoma zmiennymi (i stałymi). Działanie algorytmu polega na konstruowaniu pewnego drzewa z wierzchołkami etykietowanymi równaniami. Przypomina to algorytm Plotkina: budowane jest drzewo podobne do drzewa wszystkich ścieżek w grafie $\mathcal{G}_V$ zaczynających się w wierzchołku wyznaczonym przez dane równanie.

Będziemy dbać o to, by drzewo w algorytmie Chmielewskiego miało następującą własność: jeżeli $R_1, \ldots, R_n$ są etykietami (wszystkich) wierzchołków będących następnikami (synami) wierzchołka wyznaczonego przez równanie R, to

1. jeżeli równania R ma rozwiązanie, to dla pewnego indeksu $i \leqslant n$ równanie R_i ma rozwiązanie,

2. dla dowolnego $i \leqslant n$, dowolne rozwiązanie α równania R_i wyznacza rozwiązanie α' równanie R.

Jeżeli mamy równanie R i skończony zbiór równań $R_1, \ldots, R_n$ spełniający podane warunki, to będziemy mówić, że równania (zbiór równań) $R_1, \ldots, R_n$ zastępuje równanie R, albo że równanie R możemy zastąpić lub zastępujemy równaniami $R_1, \ldots, R_n$. Podobnie jest w drzewie związanym z algorytmem Plotkina. Wierzchołek wyznaczony przez równanie $xu = yv$ ma synów wyznaczonych przez równania $\varphi_{xy}(u) = y\varphi_{xy}(v)$, $x\varphi_{yx}(u) = \varphi_{yx}(v)$ i $\varepsilon_{xy}(u) = \varepsilon_{xy}(v)$. Nietrudno zauważyć, że równanie $xu = yv$ można zastąpić wyżej podanymi trzema równaniami. W tym przypadku mamy wzajemnie jednoznaczną odpowiedniość między zbiorem rozwiązań równania $xu = yv$ i zbiorem rozwiązań trzech podanych równań. W algorytmie Chmielewskiego nie wymagamy takiej odpowiedniości zbiorów rozwiązań.

Liście drzewa budowanego w algorytmie Chmielewskiego powinny być etykietowane równaniami o znanym rozwiązaniu. Będziemy to drzewo budować tak długo, aż w liściach znajdą się pewne równania, które potrafimy rozwiązać, np. równania z jedną zmienną.

Symbolem $s(x/t)$ oznaczamy słowo powstające ze słowa s przez zastąpienie symbolu x słowem t.

32.1 Równania jednostronne

Jeżeli mamy równanie, w który lewa i prawa strona zaczynają się różnymi zmiennymi, to możemy je uważać za równanie jednostronne. Równanie jednostronne zapisujemy w postaci $xu \to yv$. Rozwiązanie tego równania jest zwykłym rozwiązaniem równania $xu = yv$, np. jest to homomorfizm α taki, że $\alpha(xu) = \alpha(yv)$, ale dodatkowo rozwiązanie α równania jednostronnego spełnia warunek $\alpha(x) > \alpha(y)$. Nietrudno zauważyć, że dowolne równanie postaci $xu = yv$ można zastąpić rówaniami $xu \to yv$, $yv \to xv$ i równaniem z jedną zmienną $u(y/x) = v(y/x)$.

W algorytmie Chmielewskiego wierzchołki budowanego drzewa będą etykietowane także równaniami jednostronnymi.

32.2 Typ równania

Przyjmijmy, że u' oznacza słowo u, z ktorego usunęliśmy wszystkie stałe. O równaniu $u = v$ mówimy, że jest typu $u' = v'$. Pojęcie typu stosujemy też do równań jednostronnych. Mówiąc o typie będziemy często pomijać nieistotne fragmenty słów u' i v'. Będziemy np. zajmować się równaniami typu $x \ldots = y \ldots$, a więc równaniami, w których pierwszą zmienną po lewej stronie równania jest zmienna x, a po prawej stronie – zmienna y.

32.3 Przenoszenie fragmentu równania

Przypuśćmy, że mamy równanie $uw_1 = vw_2$, gdzie u i v są słowami, w których dla dowolnej zmiennej liczby jej wystąpień w obu słowach są równe, a w_1 i w_2 są dowolnymi słowami. Przyjmijmy, że liczba stałych występująch w słowie u pomnijeszona o liczbę stałych ze słowa v jest równa $m \geqslant 0$. Wtedy dla dowolnego rozwiązania α równania $uw_1 = vw_2$ istnieje słowo s długości m takie, że $\alpha(u) = \alpha(v)s$ Równanie $uw_1 = vw_2$ możemy zastąpić równaniami $sw_1u = w_2sv$ dla wszystkich stałych słów s długości m.

Postępujemy analogicznie, jeżeli w v jest więcej stalych niż w u. Zauważmy, że odpowiednio dobierając słowa u i v możemy spowodować, że pierwsze zmienne po lewej i prawej stronie równania $sw_1u = w_2sv$ są różne.

Opisane tu prezkształcenie pozwala zastąpić dowolne równanie, które nie jest typu $u = u$, zastąpić równaniem typu $xu = yv$.

32.4 Równania wykładnicze

Równaniem wykładniczym (słowowym) nazywamy równość postaci $u = v$, gdzie u i v są słowami parametrycznymi. Rozwiązaniem takiego równania nazywamy przyporządkowanie, które zmiennym słowowym przyporządkowuje słowa, a zmiennym liczbowym – liczby naturalne takie, że po zastąpieniu zmiennych w słowach u i v tym, co zostało im przyporządkowane, otrzymujemy słowa identyczne. Równanie wykładnicze nazywamy jednopiętrowym, jeżeli obie strony równania są konkatenacjami zwykłych słów i słów parametrycznych postaci s^n, gdzie s jest zwykłym słowem, a n – zmienną naturalną. O równaniu wykładniczym mówimy, że jest równaniem z jedną zmienną (z dwoma zmiennymi), jeżeli obie strony tego równania są konkatenacjami słów stałych i słów postaci s^n (lub odpowiednio s_1^n lub s_2^m), gdzie s, s_1 i s_2 są słowami stałymi, a n i m są (konkretnymi) zmiennymi naturalnymi.

Nietrudno zauważyć, że równanie (słowowe) z jedną zmienną może zostać zastąpione zbiorem równań wykładniczych z jedną zmienną.

32.5 Równania typu $u = u$

Równania (słowowe z dwoma zmiennymi) typu $u = u$ są albo równaniami z jedną zmienną, albo dają sią zastąpić równaniami wykładniczymi z dwoma zmiennymi.

32.6 Odwracanie równań

Równanie $x_1 \dots x_n = y_1 \dots y_m$ można zastąpić równaniem odwróconym $x_n \dots x_1 = y_m \dots y_1$. Zależność między rozwiązaniami równania i równania odwróconego jest oczywista.

32.7 Usuwanie stałych z początku równania

Przypuśćmy, że mamy równanie postaci $xu = syv$, gdzie x i y są różnymi zmiennymi, s – niepustym słowem bez zmiennych, a u i v – dowolnymi słowami. Równanie $xu = syv$ możemy zastąpić równaniami $u(x/s') = s''yv(x/s')$, gdzie s' jest dowolnym niepustym prefiksem s oraz $s = s's''$ i równaniem $xu(x/sx) = yv(x/sx)$.

Dzięki usuwaniu stałych dowolne równanie typu $x \dots = y \dots$ można zastąpić równaniem postaci $x \dots = y \dots$ To ostanie równanie można zastąpić (z dokładnością do nazw zmiennych) równaniami jednostronnymi postaci $x \dots \to y \dots$ (i równaniami z jedną zmienną).

Nietrudno zauważyć, że mnożąc w razie potrzeby równanie z prawej strony przez zmienną, równania z dwoma zmiennymi potrafimy sprowadzić do równań typu $x^a y \dots \to y^c x \dots$ dla $a, c \geqslant 1$.

32.8 Równania z jednym wystąpieniem zmiennej po jednej stronie

Jeżeli z równania, w którym po lewej stronie jest tylko jedno wystąpienie zmiennej, usuniemy wszystkie stałe rozpoczynające i kończące lewą stronę, to otrzymamy równanie postaci $x = u$. Takie równanie bardzo łatwo rozwiązać. Albo jest to równanie z jedną zmienną, albo jest już właściwie rozwiązane.

32.9 Przykład przekształcania

Rozważamy równanie jednostronne $xu \to yxv$ z dwoma zmiennymi x i y. Będziemy przekształcać to równanie zgodnie z algorytmem Plotkina. Ponieważ jest to równanie jednostronne, możemy zastosować jedynie przekształcenie φ_{yx}. Przypuśćmy, że to przekształcenie stosujemy stosujemy pewną liczbę razy. Zauważmy, że

$$\varphi_{yx}^t(x) = y^t x \quad \text{oraz} \quad \varphi_{yx}^t(y) = y.$$

Po t-krotnym wykonaniu tego przekształcenia otrzymujemy równanie

$$y^t xu(x/y^t x) = yy^t xv(x/y^t x),$$

czyli

$$xu(x/y^t x) = yxv(x/y^t x).$$

Po wykonaniu tych przekształceń możemy uznać, że dalej zastosujemy φ_{xy} (a więc dalej rozwiązujemy równanie $yxv(x/y^t x) \to xu(x/y^t x)$), albo stosujemy ε_{xy} (w ten sposób otrzymujemy równanie $xv(x/x^t x) = u(x/x^t x)$ z jedną zmienną, albo też kontunuujemy stosowanie φ_{yx}.

Tak więc w grafie $\mathcal{G}_V$ każda ścieżka wychodzące z wierzchołka wyznaczonego przez równanie $xu \to yxv$ przechodzi przez wierzchołek wyznaczony przez jedno z równań $xv(x/x^t x) =$

$u(x/x^t x)$ (z jedną zmienną) lub $xu(x/y^t x) = yxv(x/y^t x)$ dla pewnego $t \in N$. Niestety, zbiór tych równań (i – w konsekwencji – zbiory wierzchołków i ścieżek) jest nieskończony. Zastąpimy go zbiorem skończonym.

32.10 Opis badanego przekształcenia

Przypuśćmy, że mamy równanie typu $x^a y \ldots \to y^c x \ldots$ ze zmiennymi x i y. Przyjmijmy, że jest to równanie postaci $x \ldots \to yBz \ldots$, gdzie B jest słowem stałym, a z jest zmienną ($z = x$ lub $z = y$). Równanie to będziemy też uważać za formułę (równość) i oznaczać symbolem $r(x, y)$ (czyli $r(x, y) \Leftrightarrow x \ldots = yBz \ldots$). Równanie jednostronne $x \ldots \to yBz \ldots$ możemy uważać za formułę $R(x, y) = r(x, y) \wedge x > y$. Niech X i Y będą rozwiązaniem równania $R(x, y)$ (a więc zachodzi $R(X, Y)$). Weźmy największą liczbę t taką, że $(YB)^t$ jest prefiksem X. Są możliwe dwa przypadki: albo $X = (YB)^t Y'$ dla pewnego niepustego prefiksu $Y' < Y$, albo $X = (YB)^t YB'$ dla pewnego prefiksu $B' \leqslant B$. Niech $R_1(x, y, t)$ oznacza formułę

$$r((yB)^t x, y) \wedge x < y.$$

Podobnie, niech $R_2(y, t, b)$ oznacza formułę

$$r((yB)^t yb, y).$$

Zauważmy, że wyżej został dowiedziony następujący fakt:

$$\exists x, y\ R(x, y) \iff \exists x, y \left(\exists t > 0\ R_1(x, y, t) \vee \exists t > 0\ R_2(y, t, \varepsilon) \vee \bigvee_{\varepsilon < b \leqslant B} \exists t\ R_2(y, t, b) \right).$$

Formuła R_2 jest jednopiętrowym równaniem wykładniczym, jest to właściwie równanie wykładnicze z jedną zmienną, podobnie jest z formułą R_1.

32.11 Eliminowanie parametrów

Mówimy, że parametr t eliminujemy z formuły $\Phi(x, y, t)$, jeżeli

$$\exists n\ \forall x, y\ ((\exists t \geqslant n \Phi(x, y, t)) \Rightarrow (\forall t \geqslant n \Phi(x, y, t))). \tag{17}$$

Jeżeli tak jest, to liczbę n, której istnienie stwierdza podana formuła nazywamy granicą eliminacji. Zauważmy, że jeżeli n jest granicą eliminacji, to każda liczba większa od też jest granicą eliminacji. Jeżeli jest to potrzebne, ten rodzaj eliminacji nazywa się eliminacją w silnym sensie.

Przypuśćmy, że potrafimy eliminować parametr t z formuły $\Phi(x, y, t)$ i n jest granicą eliminacji. Wtedy

$$\exists x, y\ \exists t\ \Phi(x, y, t) \iff \exists x, y \bigvee_{i=1}^{n} \Phi(x, y, i). \tag{18}$$

Nietrudno zauważyć, że jeżeli mamy dwie formuły (lub skończenie wiele formuł), z których potrafimy eliminować parametr t, to ten parametr potrafimy też eliminować z alternatywy tych formuł.

32.12 Eliminowanie parametru z równania z jedną zmienną

Twierdzenie 32.1 *Przypuśćmy, że mamy słowa* $P_0, \ldots, P_n$ *i* $Q_0, \ldots, Q_m$*, oraz liczby* $k = \min\{n, m\}$ *i* $G = \max\{|\,|P_0 \ldots P_i| - |Q_0 \ldots Q_i|\,| : i \leqslant k\}$*. Jeżeli* A *jest niepustym słowem i* $l \geqslant 1 + \frac{G}{|A|}$ *taką, że*

$$P_0 A^l P_1 A^l \ldots A^l P_n = Q_0 A^l Q_1 A^l \ldots A^l Q_m,$$

to $n = m$ *i zachodzą równości*

$$P_0 A^t P_1 A^t \ldots A^t P_n = Q_0 A^t Q_1 A^t \ldots A^t Q_m$$

dla wszystkich $t \in N$*.*

Dowód. Najpierw dodatkowo załóżmy, że A jest słowem prostym. Będziemy rozważać przypadek, gdy $|P_0| \geqslant |Q_0|$. Oczywiście, $l|A| \geqslant |A| + G \geqslant |A| + |P_0| - |Q_0|$. Tak więc słowo $P_0 A$ jest prefiksem $Q_0 A^l$. Ponieważ słowo A jest prostę, więc $P_0 = Q_0 A^i$ dla pewnego i. Co więcej, zachodzi także

$$P_1 A^l \ldots A^l P_n = A^i Q_1 A^l \ldots A^l Q_m.$$

Wobec tego,

$$A^t P_1 A^l \ldots A^l P_n = A^i A^t Q_1 A^l \ldots A^l Q_m$$

oraz

$$P_0 A^t P_1 A^l \ldots A^l P_n = Q_0 A^t Q_1 A^l \ldots A^l Q_m$$

dla dowolnej liczby t. Tym bardziej,

$$P_0 P_1 A^l \ldots A^l P_n = Q_0 Q_1 A^l \ldots A^l Q_m$$

i dalszy dowód może korzystać z zasady indukcji.

Jeżeli A nie jest słowem prostym, $A = T^c$ i twierdzenie zachodzi dla T, to także zachodzi dla, gdyż jeżeli

$$l \geqslant 1 + \frac{G}{|A|},$$

to

$$cl \geqslant c + \frac{cG}{|T^c|} = c + \frac{G}{|T|} \geqslant 1 + \frac{G}{|T|}$$

i można wywnioskować dowodzone twierdzenie z jego prawdziwości dla słów prostych. □

Udowodnione twierdzenie oznacza, że potrafimy eliminować parametr z równania wykładniczego z jedną zmienną. Korzystając z tego twierdzenia można dowieść parametryzowalność równań słowowych z jedną zmienną i opracować algorytm rozwiązujący takie równania.

32.13 Eliminowanie parametru z równania $R_1(x, y, t)$

Zauważmy, że równanie $R_1(x, y, t)$ może zostać zapisane w postaci

$$P_0(y)(yB)^t xP_1(y)(yB)^t \dots (yB)^t xP_n(y) = Q_0(y)(yB)^t xQ_1(y)(yB)^t \dots (yB)^t xQ_m(y).$$

gdzie $P_i(y)$ i $Q_i(y)$ są słowa zapisanymi za pomocą stałych i litery y. Mamy dowieść własność (17) dla $\Phi = R_1$. Liczbę granicę N parametryzacji podamy później. Aby dowieść, że N jest granicą parametryzacji, bierzemy słowa X i Y i zakładamy, że dla pewnej liczby $l \geqslant N$ zachodzi równość

$$P_0(Y)(YB)^l XP_1(Y)(YB)^l \dots (YB)^l XP_n(Y) = Q_0(Y)(YB)^l XQ_1(Y)(YB)^l \dots (YB)^l XQ_m(Y).$$

Interesujące nas własności takiego równania wynikają z twierdzenia 32.1. Aby dowieść możliwość eliminacji t z równania $R_1(x, y, t)$, wystarczy tak dobrać N, by $N \geqslant 1 + \frac{G}{|\,YB\,|}$. Liczba G w tym wzorze powinna zostać zdefiniowana w następujący sposób:

$$G = \max\{|\,|\,P_0(Y)XP_1(Y)\dots P_i(Y)\,| - |\,Q_0(Y)XQ_1(Y)\dots Q_i(Y)\,|\,| : i \leqslant k\}$$

dla $k = \min\{n, m\}$. Liczba G nie zależy od X i może zostać zdefiniowana wzorem postaci

$$G = \max\{a_i + b_i|\,Y\,| : i \leqslant k\},$$

gdzie a_i oraz b_i są pewnymi liczbami całkowitymi. Kosztem zwiększenia G możemy przyjąć, że są to liczby naturalne. Nietrudno zauważyć, że eliminacje t z równania R_1 jest możliwa od granicy n takiej, że Zauważmy, że

$$\frac{G}{|\,YB\,|} \leqslant \frac{\max\{a_i + b_i|\,Y\,| : i \leqslant k\}}{|\,YB\,|} \leqslant \frac{\max\{\frac{a_i}{|\,Y\,|} + b_i : i \leqslant k\}}{1 + \frac{|\,B\,|}{|\,Y\,|}} \leqslant \max\{a_i + b_i : i \leqslant k\}.$$

Stąd wynika, że eliminacje t z równania R_1 jest możliwa od $N \geqslant 1 + \max\{a_i + b_i : i \leqslant k\}$.

32.14 Sprowadzanie do równań typu $xy \dots \to yx \dots$

Przypuśćmy, że $a \geqslant 1$ i $c \geqslant 2$, i rozważamy równanie typu $x^a y \dots \to y^c x \dots$, które ma postać $xu \to yBv$, gdzie B jest słowem stałym i pierwsza litera v jest zmienną y.

Równoważność (18) i wykazane możliwości eliminacji parametrów pozwalają równanie to zastąpić równaniami $(yB)^t xu(x/(yB)^{t+1}x) = v(x/(yB)^{t+1}x)$ dla $t \leqslant n$ z dodatkowym warunkiem $x < y$, oraz równaniami z jedną zmienną (którymi możemy nie zajmować się). Interesujące nas równania są typu $y^t x(y^{t+1}x)^{a-1}y \dots = y^{c-1}y^{t+1}x \dots$, czyli $y^t xy \dots = y^t y^c x \dots$ Teraz możemy przenieść prefiksy typu y^t na koniec równania. Nie zmienia to długości rozwiązań (więc nadal $x < y$) i prowadzi do równania typu $xy \dots = y^c x \dots$, które ma postać

$$xy \dots = py^c x \dots \quad \text{lub} \quad pxy \dots = y^c x \dots .$$

W pierwszym przypadku usunięcie prefiksu p prowadzi do równania typu $y^c x \dots \to xy \dots$ W drugim porównujemy długości px i y, i są możliwe dwie sytuacje. Jeżeli $|\,x\,| < |\,y\,| \leqslant |\,px\,|$, to podstawienie za y wyrażenia postaci xp' dla $p' \leqslant p$ prowadzi do równania z jedną zmienną. Jeżeli $|\,px\,| < |\,y\,|$, to skrócenie y o prefiks p prowadzi do równania typu $y^c x \dots \to xy \dots$

Powtarzając ponownie przedstawione przekształcenia możemy dowolne równanie zastąpić równaniami typu $yx \dots \to xy \dots$ i pewnymi równaniami z jedną zmienną.

32.15 Sprowadzanie do równań $xAy \ldots \to yBx \ldots$, gdzie $|\,A\,| = |\,B\,|$

Równanie typu $yx \ldots \to xy \ldots$ dzielimy na dwie części i na chwilę zastępujemy układem dwóch równań. Pierwsze z równań jest postaci $xayc = ybx$ lub $xay = ybxc$. Przyjmijmy, że drugie jest równe $u = v$. Zauważmy, że $|\,ac\,| = |\,b\,|$ lub odpowiednio $|\,a\,| = |\,bc\,|$.

W równaniu $xayc = ybx$ zmienną x skracamy wykonując albo podstawienie $x := c'$ dla pewnego $c' \leqslant c$, albo podstawienie $x := xc$. W pierwszym przypadku wyjściowe równanie zastępujemy równaniem ze zmienną y, w drugim – równaniem $ybxv(x/xc) \to xcayu(x/xc)$.

Dla drugiego równania też mamy dwa przypadki: albo $|\,y\,| > |\,xc\,|$, albo $|\,x\,| < |\,y\,| \leqslant |\,xc\,|$. W pierwszy przypadku postępuje jak wyżej, a to zastąpić wyjściowe równanie równaniem postaci $yBx \ldots \to xAy \ldots$ dla słów A i B tej samej długości. W drugim przypadku wyjściowe rownanie zastępujemy równaniem ze zmienną x.

Ostatecznie, dowolne równanie w słowach z dwoma zmiennymi można zastąpić równaniami prostymi (na przykład równaniami z jedną zmienną) i równaniami postaci $yBx \ldots \to xAy \ldots$ ze słowami A i B tej samej długości.