Finite model theory – homework 1

Wojciech Przybyszewski

November 15, 2021

Problem 5

Próbując rozwiązać zadanie zauważyłem, że rozważany problem jest EXPTIME-trudny, a nawet EXPH-trudny (hierarchia wykładnicza). Nie widać jednak, żeby ten problem należał do którejś z tych klas. Z drugiej strony widać należenie problemu do EXPSPACE, ale nie wydaje się, żeby ten problem był EXPSACE-trudny. Potrzeba więc jakiejś klasy złożoności pomiędzy EXPH i EXPSPACE.

Klasy EXPH i EXPSPACE można scharakteryzować w terminach alternujących maszyn Turinga. Obie te klasy są rozpoznawane przez alternujące maszyny Turinga działające w czasie wykładniczym, z tym że w EXPH mamy ograniczenie na stałą liczbę alternacji, a w EXPSPACE takiego ograniczenia nie ma (liczba alternacji może być wykładnicza). Pokażemy, że problem model checkingu dla SO jest zupełny w klasie problemów rozpoznawanych przez alternującą maszynę Turinga działającą w czasie wykładniczą z maksymalnie wielomianową liczbą alternacji (oznaczmy ją $\mathcal{C}$). !

Najpierw pokażemy, że rozważany problem należy do $\mathcal{C}$. Jest to w gruncie rzeczy bardzo proste – załóżmy, że dostajemy na wejściu formułę φ i strukturę $\mathbb{A}$. Spychając wszystkie negacje w dół (prawa de Morgana) możemy założyć, że wszystkie NNF negacje w φ są w literałach (wielomianowy pre-processing). Sprawdzenie prawdziwości φ w $\mathbb{A}$ jest w gruncie rzeczy oczywiste – maszyna $\mathcal{M}$ analizuje po kolei formułę i widząc węzeł $\exists_{R^{(k)}}$ wchodzi w stan egzystencjalny i zgaduje jakąś relację R arności k wypisując ją na taśmie (potrzebuje na to $|\mathbb{A}|^k$ bitów). Oczywiście jeśli relacja R jest gdzieś używana w formule, to $k \leq |\varphi|$, więc zużywamy nie więcej niż $|\mathbb{A}|^{|\varphi|}$ bitów i mieścimy się w czasie wykładniczym (a jeśli R w formule używana nigdzie nie jest, to pomijamy jej zgadywanie). Podobnie jeśli trafiamy na węzeł $\forall_{R^{(k)}}$ to wchodzimy w stan uniwersalny i wypisujemy jakąś relację R. Węzły $\vee$ i $\wedge$ rozwiązujemy poprzez odpowiednio stan egzystencjalny wybierający jakiś dysjunkt albo stan uniwersalny wybierający każdy koniunkt. Prawdziwość literałów sprawdzamy korzystając z zapisanych na taśmie relacji i stałych. Oczywiście w ten sposób wykonujemy co najwyżej $|\varphi|$ alternacji, czyli rozważany problem rzeczywiście należy do $\mathcal{C}$.

Teraz trochę trudniejsza część, czyli $\mathcal{C}$-trudność wspomnianego problemu. Weźmy dowolny problem z $\mathcal{C}$, który rozstrzyga maszyna $\mathcal{M}$ i jego instancję w. Napiszemy formułę φ, która jest prawdziwa w dwuelementowej strukturze nad sygnaturą złożoną z dwóch symboli stałych 0 i 1 (odróżniających oba te elementy) wtedy i tylko wtedy, gdy maszyna $\mathcal{M}$ akceptuje w. Ponadto φ będzie wielomianowej długości od $\mathcal{M}$ i w. Pomysł jest całkiem podobny do pokazywania PSPACE-trudności problemu QBF. Oznaczmy $|w| = n$. Maszyna $\mathcal{M}$ działa w czasie $2^{p(n)}$ dla pewnego wielomianu p. Oznacza to, że $\mathcal{M}$ nie zapisuje więcej niż $2^{p(n)}$ bitów. Zawartość taśmy możemy więc reprezentować jako relację R arności $p(n)$ – zawartość l-tego bitu taśmy dostajemy patrząc na zapis binarny l i sprawdzając prawdziwość $R(bin(l))$.

Wiemy już jak kodować konfiguracje maszyny $\mathcal{M}$ (pewnie przydałoby się jeszcze trzymać, gdzie jest głowica i jej stan, ale to da się prosto zrobić niewiele zwiększając arność R), napisanie formuły sprawdzającej, czy R koduje konfigurację początkową też jest proste. Podobnie jest proste napisanie formuły, $\psi(R, R')$, która sprawdza, czy w jednym kroku da się przejść z konfiguracji R do R' (dla prawie wszystkich $p(n)$ bitów prawdziwość R i R' jest taka sama, a w tych kilku miejscach, gdzie są inne, mamy poprawną tranzycję). Wykorzystując ten sam trik co do pokazania PSPACE-trudności QBF możemy napisać formułę $\psi_{p(n)}(R, R')$, która sprawdza, czy da się dojść z R do R' w $2^{p(n)}$ krokach bez żadnej alternacji i $\psi_{p(n)}$ ma wielomianowy rozmiar od wejścia.

Końcówka jest już prosta – mając takie formuły do sprawdzenia, czy dana relacja opisuje konfigurację początkową i takie, które mówią o przejściu w czasie wykładniczym z jednej konfiguracji do drugiej, możemy napisać formułę, która mówi, że słowo w jest akceptowane przez $\mathcal{M}$ – konkretnie istnieje bieg z konfiguracji początkowej do jakiejś k_1 długości co najwyżej $2^{p(n)}$, że potem dla dowolnego biegu z k_1 do k_2 w co najwyżej $2^{p(n)}$ krokach, że potem istnieje jakiś bieg z k_2 do k_3 i tak dalej, aż do $k_{q(n)}$, gdzie q jest wielomianem ograniczającym liczbę alternacji (bez straty ogólności możemy założyć, że początkowy stan jest egzystencjalny). To kończy dowód (lekko szkicowy) $\mathcal{C}$-zupełności problemu model checkingu dla logiki drugiego rzędu.