Egzamin ze złożoności obliczeniowej – teoria. 11.6.2012

Imię i nazwisko:

Proszę wskazać i wyjaśnić ewentualne błędy w poniższych rozumowaniach. Odpowiedź powinna się zmieścić na tej kartce. Można zaznaczyć bezpośrednio w tekście miejsca uznane za błędne.

1. Udowodnimy, że $P/poly \subseteq NP$. Weźmy dowolny język w NP. Zgodnie z definicją, dla dowolnego słowa w mamy podpowiedź (ang. *advice*) wielomianowej długości, ktora pozwala w wielomianowym czasie rozstrzygnąć, czy $w \in L$. Tę podpowiedź możemy wykorzystać jako świadka (ang. *witness*) dla słowa w, co wystarczy dla wykazania, że $L \in NP$.

2. Udowodnimy, że $NP \subseteq BPP$. Powiemy, że algorytm probabilistyczny A jest jednostronny (ang. *one–sided*) jeśli $\forall x$

$$
\begin{aligned}
x \in L &\implies Pr(A = yes) = 1 \\
x \notin L &\implies Pr(A = yes) \leq p,
\end{aligned}
$$

dla pewnego $p < 1$. Jeśli algorytm jest *one–sided*, to powtarzając go $q(n)$ razy dla pewnego wielomianu $q(n)$, uzyskamy $p^{q(n)} < \frac{1}{4}$. A zatem, język rozpoznawany przez taki algorytm jest w BPP.

Rozważmy problem, czy dwa obwody logiczne C_1 i C_2 (o tej samej liczbie zmiennych) *są* równoważne. Algorytm losuje wartościowanie w i daje odpowiedź wg tego czy $C_1(w) = C_2(w)$. Jeśli obwody są równoważne, to algorytm nigdy się nie pomyli, a zatem jest *one–sided*. Tak więc powyższy problem jest w BPP. Ale jest to przecież dopełnienie problemu NP-zupełnego (wszak obwody spełnialne to obwody nierównoważne *false*). Skoro BPP jest zamknięte na dopełnienia (było na ćwiczeniach!) wnioskujemy, że pewien problem NP-zupełny jest w BPP, a zatem całe NP jest zawarte w BPP.

3. Udowodnimy $DSPACE(n^2) \subseteq DSPACE(n)$, obalając podejrzane „Twierdzenie o hierarchii" (*Theorem 6* w notatkach). Problem ewaluacji obwodow boolowskich może być oczywiście rozwiązany w pamięci liniowej, a zatem również problem prawdziwości skwantyfikowanych obwodów (*Q-Boole-Sat* z rodziału 7 notatek) może być rozwiązany w pamięci liniowej. Ale na wykładzie stwierdzono, że problem ten jest zupełny w klasie $PSPACE$, czyli jest najtrudniejszym problemem w $PSPACE$. Skoro więc ten problem jest rozwiązywalny w pamięci liniowej to dotyczy to każdego problemu w $PSPACE$, czyli w szczególności $DSPACE(n^2) \subseteq DSPACE(n)$. W Twierdzeniu o hierarchii trzeba było założyć, że $S_2(n) - S_1(n)$ rośnie wykładniczo.