A számítástudomány alapjai 2014. I. félév

12. gyakorlat. Összeállította: Fleiner Tamás (fleiner@cs.bme.hu)

Tudnivalók

Def: Az algoritmus fogalmát nem definiáljuk, de algoritmusra úgy gondolunk, mint valamiféle elméleti számítógépen futtatott programra, mely egy, az input által megadott feladatot old meg, a megoldás az algoritmus outputja, és az algoritmus a működése során bizonyos, az inputtól és az addigi működéstől függő lépéseket tesz meg. Minden A algoritmushoz egy Π problémához tartozik, Π azokból a konkrét feladatokból áll, amelyeket A meg tud oldani. (Feltesszük, hogy A minden értelmes inputra helyes eredményt ad.) Különböző algoritmusok is tartozhatnak ugyanahhoz a Π problémához. Egy algoritmus *inputja* az algoritmus bemenete: ez jelöli ki, hogy a szóban forgó Π problémának pontosan melyik feladatáról is van szó. Az input *mérete* az inputot leíró bitek száma. Tetszőleges A algoritmushoz tartozik egy f_A függvény: $f_A(n)$ azt adja meg, hogy legfeljebb hány lépést tesz meg az A algoritmus a legfeljebb n hosszúságú inputokon. Lényegtelen tehát, ha az A algoritmus a legfeljebb n hosszúságú inputok $99,999\%$-án néhány lépésben végez, $f_A(n)$ a legrosszabbul viselkedő (legfeljebb n hosszúságú inputhoz tartozó lépésszám.

Példa: Ha az algoritmus inputja egy pozitív egész n szám, akkor az input mérete az n bináris alakjában található jegyek száma, azaz $1 + \lceil \log_2(n) \rceil$. Ha az input egy n csúcsú egyszerű $G = (V, E)$ gráf, akkor G-t a szomszédossági mátrixával megadva az input mérete n^2. (Vannak persze értelmesebb megadások is, sőt, szinte csak azok vannak. Éllistával pl. az input mérete $konst \cdot (n+m)$, ahol m a G éleinek száma.)

Def: Az A algoritmus *polinomidejű* (néha *polinomiális* vagy *hatékony*), ha létezik olyan $p(n)$ polinom, amelyre $f_A(n) \leq p(n)$ teljesül minden $n \geq 1$-re.

Példa: A BFS algoritmus hatékony, hiszen egy n élű m csúcsú gráfot (amelyet meg lehet adni n^2 méretű vagy $konst \cdot (n+m)$ méretű inputtal) a lépésszámra $f_{BFS}(n) \leq c \cdot (n+m)$ teljesül alkalmas c konstansra, tehát $p(n) = c' \cdot n$ megfelelő polinom, ahol c' alkalmas konstans.

Def: *Döntési probléma* az olyan probléma, amelynek az outputja egyetlen bit (azaz az input tkp egy igen/nem kérdés). A P problémaosztályt azon döntési problémák alkotják, amelyekre létezik polinomidejű algoritmus.

Példa: P-beli probléma az, hogy az input által megadott irányítatlan gráf összefüggő-e. A BFS algoritmus ugyanis polinomidejű, és ennek a futtatásakor kidrül, hogy G összefüggő-e. P-beli az a probléma is, hogy az input által megadott G gráfnak van-e Euler körsétája. Elhagyhatjuk ugyanis az izolált pontokat, ellenőrizhetjük egy BFS-sel, hogy a maradék gráf összefüggő-e, és minden élről legfeljebb n (csúcsszámnyi) lépésben ellenőrizhető, hogy páros-e a fokszáma. Ha minden fok páros és G izolált pontoktól eltekintve összefüggő, akkor G-nek van Euler körsétája, egyébként nincs.

Def: NP-beli probléma alatt olyan döntési problémát értünk, melyre az „igen" válaszra van polinomidejű bizonyíték. $co-NP$-beli probléma pedig az, melyre a „nem" válaszra van polinomidejű bizonyíték.

Példa: NP-beli az a HAM döntési probléma, melynek bemenete egy egyszerű G gráf, és az output akkor „igen", ha G-nek van Hamilton köre. (Ha ugyanis valaki megmutatja a Hamilton kört, akkor az bizonyítja a Hamilton kör létezését, és azt ellenőrizni, hogy a mutatott élhalmaz kör és minden csúcsot tartalmaz, szintén polinomidőben elvégezhető.)

$co-NP$-beli az a probléma, melynek bemenete egy n pozitív egész, és az output akkor „igen", ha n prím. (Ha ugyanis az n-et nemtriviális módon két egész szorzatára tudjuk bontani, akkor ez egyúttal bizonyíték arra, hogy n nem prím. Az is kell, hogy a szorzás polinomidőben elvégezhető.)

Állítás: $P \subseteq NP \cap co-NP$.

Biz: : Ha $\Pi \in P$, akkor Π-re van polinomidejű algoritmus, és annak futása polinomidejű bizonyíték.

Gyakorlatok

1. Ismételjük át, hogy az egész számok összeadására és szorzására van polinomidejű algoritmus.
2. Négyzetreemelések segítségével számítsuk ki $10^{133}(mod 13)$ értékét, azaz határozzuk meg, milyen maradékot ad 13-mal osztva a 10^{133}. Határozzuk meg ugyanezt most az Euler-Fermat tételre támaszkodva.
3. A Π probléma inputja egy G páros gráf, G színosztályai és egy k szám. Az output akkor „igen", ha G-nek van k méretű párosítása, azaz $\nu(G) \geq k$. Határozzuk meg, hogy Π a P, NP és $co-NP$ problémaosztályok melyikének tagja.