Bonyolultságelmélet zárthelyi megoldások

December 14, 2006

1 Feladat. *Egy $B(x_1, \ldots, x_n)$ Boole formulát robusztusnak nevezünk, ha vagy nem kielégíthető, vagy legalább 2^n olyan $x \in \{0,1\}^n$ sorozat van, ami kielégíti. Mutassuk meg, hogy randomizált algoritmussal polinomiális időben eldönthető, hogy a formula kielégíthető-e.*

Megoldás. Egy véletlen $x \in \{0,1\}^n$ sorozatra

$$\Pr(B(x)=0) = \begin{cases} 1, & \text{ha } B \text{ nem kielégíthető,} \\ \leq 1 - \frac{1}{n^2}, & \text{ha } B \text{ kielégíthető.} \end{cases}$$

Ha kn^2-szor megismételjük, akkor

$$\Pr(\forall x B(x)=0) = \begin{cases} 1, & \text{ha } B \text{ nem kielégíthető,} \\ \leq \left(1 - \frac{1}{n^2}\right)^{kn^2} < e^{-k}, & \text{ha } B \text{ kielégíthető.} \end{cases}$$

Tehát vagy találunk a kipróbált x-ek között megoldást, vagy a formula nagy valószínűséggel nem kielégíthető.

2 Feladat. *Egy n hosszúságú $x \in \{0,1\}^n$ sorozatból egy $2n$ hosszúságú $g(x)$ sorozatot képezünk úgy, hogy minden jegye után beszúrjuk a későbbi jegyek kináris összegét.*

(a) Ha x-et véletlenül egyemletes eloszlás szerint választjuk, mekkora lesz nagy valószínűséggel a $g(x)$ sorozat Kolmogorov-bonyolultsága?

(b) Mutassuk meg, hogy van olyan $1 \leq k \leq n$, hogy az első k jegyből a következő jegy $1/2$-nél lényegesen nagyobb valószínűséggel megjósolható.

Megoldás. (a) Mivel x-ből a $g(x)$ algoritmikusan kiszámítható és viszont, következik, hogy van olyan c konstants, melyre

$$|\mathbf{K}(g(x)) - \mathbf{K}(x)| \leq c$$

minden x-re. Mivel nagy valószínűséggel $|\mathbf{K}(x) - |x||$ korlátos, így nagy valószínűséggel $|\mathbf{K}(g(x)) - |x||$ is korlátos.

(b) Legyen $g(x) = y_1 \ldots y_{2n}$, ekkor bármely k-ra $y_{2k} = y_{2k-1} \oplus y_{2k-2}$.

3 Feladat. *Bizonyítsuk be, hogy ha $f : \{0,1\}^* \to \mathbb{Z}_+$ olyan rekurzív függvény, melyre $f(x) \leq \mathbf{K}(x)$ minden x-re, akkor f korlátos.*

Megoldás. Ha f nem korlátos, akkor minden k-ra definiálva van az

$$x_k = \min\{x : \ f(x) \geq k\}$$

sorozat (ahol $\{0,1\}^*$-ot nagyság szerint növekvően rendezzük), és ez algoritmikusan (türelmes próbálgatással) ki is számítható. Ebben a leírásban az egyetlen nem-konstans hosszúságú a k szám, ezért

$$\mathbf{K}(x_k) \leq \log k + \text{konstans}.$$

De másrészt

$$\mathbf{K}(x_k) \geq f(x_k) \geq k,$$

ami ellentmondás, ha k elég nagy.

4 Feladat. *Legyen minden $1 \leq i < j \leq n$ indexpárhoz $x_{i,j}$ egy Boole-változó. Ezek minden értékadása egy olyan gráfnak felel meg, melynek csúcsai az $1, \ldots, n$ számok. Legyen $B(x_{1,2}, x_{1,3}, \ldots, x_{n-1,n})$ az a Boole-függvény, melynek értéke 1, ha a gráf összefüggő, és 0, ha nem.*

(a) Mekkora a $D_0(B)$ és $D_1(B)$ nemdeterminisztikus döntési fa bonyolultság?

(b) Bizonyítsuk be, hogy a determinisztikus döntési fa bonyolultság $D(B) = \binom{n}{2}$.

(c) Hány konjunkcióból áll a B egy diszjunktív normálalakja?

Megoldás. (a) Ha a gráf nem összefüggő, akkor egy komponense és a többi csúcs közötti minden párról tudni kell, hogy nem megy köztük él. Ez a legrosszabb esetben $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n+1}{2} \rceil = \lfloor \frac{n^2}{4} \rfloor$ párt jelent, tehát $D_0(B) = \lfloor \frac{n^2}{4} \rfloor$. Ha a gráf összefüggő, akkor egy feszítő fa éleiről kell tudni, hogy élek, így $D_1(B) = n - 1$.

(b) Barkochbaként tekintve, legyen a válaszoló stratégiája az, hogy nemet mond, hacsak nem muszáj neki igent mondani (mert különben már a csúcsok egy nemüres, valódi részhalmaza és a komplementere között minden élről tudná a kérdező, hogy hiányzik).

Tegyük fel, hogy nincs még minden pár lekérdezve, de a kérdező máris tudja a választ. A fenti stratégia alapján a válasz csak az lehet, hogy a gráf összefüggő. Legyen uv egy nem lekérdezett él. Mivel a kérdező már tudja, hogy a válasz az, hogy a gráf összefüggő, ezért van olyan u-t és v-t összekötő P út, melynek minden éléről már kiderült, hogy a gráfban van. Legyen xy az út egy éle. Amikor xy-t kérdezte, akkor igenlő választ kapott, vagyis a stratégia szerint kellett, hogy legyen olyan a csúcsok egy nemüres, valódi S részhalmaza, hogy $x \in S$, $y \notin S$, és az S-ből kilépő többi élről már kiderült, hogy nincs a gráfban. De $P \setminus \{xy\} \cup \{uv\}$ olyan x-et y-nal összekötő út, melynek nincs ilyen éle, ami ellentmondás.

(c) B legegyszerűbb diszjunktív normálalakja

$$\vee_F \wedge_{e \in F} x_e,$$

ahol F végigfut az adott pontokon értelmezett fák élhalmazain. Ilyen fa a Cauchy formula szerint n^{n-2} van.

5 Feladat. *Mutassuk meg, hogy ha $P = NP$, akkor nem létezik egyirányú függvény.*

Megoldás. Tegyük fel, hogy f egyirányú. Legyen $\mathcal{L} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : \exists z \leq x, f(z) = y\}$. Ekkor $\mathcal{L}$ nyilván NP-ben van. Ha P-ben volna, akkor adott y-hoz bináris kereséssel meg tudnánk találni a legkisebb olyan z-t, melyre $f(z) = y$, vagyis f nem volna egyirányú.