Tudunk gyorsan egyenletes eloszlásban számot generálni mod 3 vagy **NP**-beli problémát megoldani?

Andó Szabolcs

Témavezető: Pálvölgyi Dömötör

Eötvös Loránd Tudományegyetem, Természettudományi Kar

2021. április 7.

Alapkérdés

Alaphelyzet

Van egy szubrutinunk, mely generál egyenletes eloszlásban egy egész számot $\{1, 2, ..., 2^n\}$ halmazból. Szeretnénk ezt használva generálni egyenletes eloszlásban egy számot a $\{1, 2, 3\}$ halmazból.

Állítás

Ez a probléma megoldható várható polinomiális időben.

Például ha n páros, akkor $2^n - 1$ osztható 3-mal.

- Ha a generált számunk legfeljebb $2^n - 1$, akkor ezt redukáljuk modulo 3, és ez lesz az outputunk;
- ha nem, újra generálunk.

Mi van akkor, ha legrosszabb esetben is polinomiális időben szeretnénk generálni?

Válasz

Ekkor a probléma oszthatósági megfontolásokból megoldhatatlanná válik.

GEN-3

Fő kérdés

Van egy szubrutinunk, mely generál egyenletes eloszlásban egy egész számot $\{1, 2, ..., 2^n\}$ halmazból, és kapunk valamiféle nehéz számítási problémát. Szeretnénk generálni egyenletes eloszlásban egy számot a $\{1, 2, 3\}$ halmazból, VAGY megoldani a nehéz problémát.

Definíció

A **GEN**-3 azon számítási problémák osztálya, melyek esetén az előző kérdésre igenlő választ kapunk.

Példa

Ha a nehéz probléma egy egyirányú permutáció dekódolása, és n páros, akkor a következő a megoldás.

- Legyen $f : \{1, 2, ..., 2^n\} \to \{1, 2, ..., 2^n\}$ egyirányú premutáció, és inputként kapunk egy $f(x)$-et.
- Generáljunk egy r véletlen egész számot $[1, 2^n]$-ből.
- Ha $f(r) = f(x)$, akkor készen vagyunk
- Ha nem, akkor véletlen számot generálunk a következő módon:

$$\text{output} = \begin{cases} f(r) \pmod 3, & \text{ha } f(r) < f(x) \\ f(r) - 1 \pmod 3, & \text{ha } f(r) > f(x) \end{cases}$$

Függvényproblémák

- Mit értünk számítási feladat alatt?
- Emlékezzünk vissza az **NP** nyelvosztály definíciójára: $L \in \mathbf{NP}$, ha minden $x \in L$-hez létezik polinomiális y tanú, mely mutatja, hogy $x \in L$.
- Ehhez kapcsolódik a függvényprobléma definíciója: minden $x \in \Sigma_0^*$ szóra vagy keresni kell egy y tanút (lehet több is), vagy ki kell írni, hogy nem létezik tanú.

NP-teljes feladatok

Igaz-e *minden* **NP**-beli feladatra, hogy **GEN**-3-ban van?

Kérdés

Másképp fogalmazva: igaz-e az **NP**-teljes feladatokra, hogy **GEN**-3-ban vannak?

- A válasz: ha **NP** és co-**NP** különböző, akkor nem.
- Ha a SAT-hoz tartozó függvényprobléma benne lenne **GEN**-3-ban, akkor belátható, hogy UNSAT $\in$ **NP**.
- A tanú egy $x \in$ UNSAT elemhez a tanú a "pénzfeldobások" értéke, mely esetén a randomizált Turing-gépünk azt írja ki, hogy $x \notin$ SAT.
- (Ilyen futás létezik oszthatósági megfontolások miatt.)

PPA-3

Definíció

Legyen az A probléma a következő: adott egy polinomiális futási idejű Turing-gép, mely egy páros gráfot reprezentál, és a gráfban adott egy csúcs, melynek foka nem osztható 3-mal. Feladatunk, hogy találjunk egy másik ilyen csúcsot. Erre az A problémára visszavezethető feladatok osztálya **PPA**-3.

- A fenti A-val polinomiálisan ekvivalens B feladat: adott egy (polinomiális) Turing-gép, mely kiszámol egy $f : \{1, 2, ..., 2^n\} \to \{1, 2, ..., 2^n\}$ függvényt, melyre $f^3 = \mathrm{id}$. Feladatunk f egy fixpontjának megtalálása.
- Belátható: $B \in$ **GEN**-3.

Következmény

PPA-3 $\subseteq$ **GEN**-3.

TFNP

Definíció

Egy függvényprobléma **TFNP**-ben van, ha minden x szóhoz létezik tanú.

Állítás

PPA-3 $\subseteq$ **TFNP**.

Ugyanis ha egy páros gráfban van olyan csúcs, melynek foka nem osztható 3-mal, akkor van benne még egy.

TFNP-beli feladatok

Állítás

Ha $R \in \mathbf{TFNP}$, és minden x esetén *előre tudjuk*, hogy hány tanú van, továbbá a tanúk száma nem osztható 3-mal, akkor $R \in \mathbf{GEN}$-3.

Állítás

Ha $R \in \mathbf{TFNP}$ olyan, hogy minden x esetén a tanúk száma felülről becsülhető x hosszának egy polinomjával, akkor $R \in \mathbf{GEN}$-3.

Köszönöm szépen a figyelmet!