Lineáris különbözőségek

Ivanyos Gábor
MTA SZTAKI

2010 december 13

A feladat

- **Titok:** $u = (\mu_1, \ldots, \mu_n)$ n dimenziós vektor $\mathbb{Z}_3^n$-ből

  $\mathbb{Z}_3$ = az egész számok modulo 3
- **Gombnyomásra kapunk:**

  véletlen $v_i = (a_{i1}, \ldots, a_{in})$ vektorokat,

  az u-ra **nem merőleges** ($\sum_{i=1}^{n} a_{ij}\mu_j \neq 0$ $\mathbb{Z}_3$-ban)

  $\mathbb{Z}_3^n$–beli vektorok közül egyforma valószínűséggel
- **Feladat:** keressük meg u-t gyorsan

"gyors"=n-ben polinom sok gombnyomás+egyéb művelet

Különbözőségek nyelvén

Oldjuk meg a

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &\neq 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &\neq 0 \\ &\vdots \\ a_{\ell 1}x_1 + a_{\ell 2}x_2 + \ldots + a_{\ell n}x_n &\neq 0 \end{aligned}$$

különbözőség-rendszert $\mathbb{Z}_3$-ban!

Háttér: rejtett eltolás

- **Adottak:** $f_0, f_1 : \mathbb{Z}_3^n \to \{$ 0-1 sorozatok$\}$
  kiértékelő orákulummal $(x \mapsto f_i(x))$
  - f_0, f_1 injektívek
  - $\exists u \in \mathbb{Z}_3^n$, amelyre $f_1(v) = f_0(v+u)$ minden $v \in \mathbb{Z}_3^n$,
- **Feladat:** keressük meg u-t (gyorsan).
- A **rejtett részcsoport** problémához fontos eszköz
- Bizonyos **kvantum-számítógépes** eljárás éppen
  u-ra nem merőleges véletlen vektorokat ad
- Részletek: K. Friedl, G. Ivanyos, F. Magniez, M. Santha, P. Sen: Hidden translations and orbit coset in quantum computing (STOC 2003)

  és G. Ivanyos: On solving systems of random linear disequations (QIC 2008).

Hasonló feladat - tanulás zajos környezetben

- **Eredeti probléma:** adott $\ell \gg n$ "véletlen" egyenlet $\mathbb{Z}_2$-ben

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{\ell 1}x_1 + a_{\ell 2}x_2 + \ldots + a_{\ell n}x_n &= b_\ell, \end{aligned}$$

aminek az $u = (\mu_1, \ldots, \mu_n)$ vektor a megoldása.

Az egyenletek 10%-ának a jobboldala meghibásodott (azaz valójában $\sum_{j=1}^{n} a_{ij}\mu_j = 1 - b_i$), csak nem tudjuk, melyek ezek.

Feladat: keressük meg u-t.

NP-nehéz

Tanulás zajos környezetben - könnyített feladat

S. Arora, R. Ge: Learning Parities with Structured Noise (*ECCC TR10-066 (2010)*)

- adott $\ell \gg n$ "véletlen" egyenlet $\mathbb{Z}_2$-ben az $u = (\mu_1, \ldots, \mu_n)$ vektorra:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{\ell 1}x_1 + a_{\ell 2}x_2 + \ldots + a_{\ell n}x_n &= b_\ell, \end{aligned}$$

$\ell/100$ **százas blokkra** osztva. Mindegyik blokkban legfeljebb 10 hiba van. Feladat: keressük meg u-t.

- Ez (és számos hasonló) polinomidőben megoldható (Ibid.)

Eldöntési változat

- **Gombnyomásra kapunk:**

  vagy (1)

  véletlen $v_i \in \mathbb{Z}_3^n$ vektorokat,
  egyforma valószínűséggel

  vagy (2)

  csupa u-ra nem merőleges $v_i \in \mathbb{Z}_3^n$ vektorokat
  (akármilyen eloszlással)

- **Feladat:** döntsük el, melyik eset áll

Visszavezetés az eldöntési változatra

- Hívjuk meg az eldöntési algoritmust. Ha a válasz (1), készen vagyunk.
- Fedjük le $\mathbb{Z}_3^n$-t 4 hipersíkkal:
  $U_0 =$ az $(a_1, a_2, \ldots, a_{n-2}, a, 0)$ alakú vektorok
  $U_1 =$ az $(a_1, a_2, \ldots, a_{n-2}, a, a)$ alakú vektorok
  $U_2 =$ az $(a_1, a_2, \ldots, a_{n-2}, a, 2a)$ alakú vektorok
  $U_\infty =$ az $(a_1, a_2, \ldots, a_{n-2}, 0, a)$ alakú vektorok
- $i = 0, 1, 2, \infty$-re hívjuk meg az eldöntési algoritmust U_i-re,

  (a mintában kapott vektorokat U_i-re vetítsük le)
- Leszállunk U_i-re aszerint, hogy melyik i-re kaptuk a (2) választ

  (szintlén levetítjük a mintában kapott vektorokat)

Az eldöntési változat megoldása

- Összegyűjtünk egy elég nagy $v_1, \ldots, v_\ell$ mintát
- Ha nincs olyan u, ami egyikre sem merőleges, a válasz (1)
- Ha van, a válasz (2)
- $\ell = O(n \log n)$ méretű minta elvileg elég a jó eséllyel korrekt válaszhoz.
- **Baj:** Ilyen u létezésének eldöntése NP-teljes
  - Gráfok 3-színezhetősége visszavezethető erre
- **Megoldás:** Nagyobb mintát veszünk.

Különbözőségből egyenlet

- Észrevétel:

$$a_1\mu_1 + \ldots + a_n\mu_n \neq 0 \Leftrightarrow (a_1\mu_1 + \ldots + a_n\mu_n)^2 = 1$$

(kis Fermat modulo 3)

- $0 \neq u = (\mu_1, \ldots, \mu_n)$-re legyen

$$P_u(x_1, \ldots, x_n) := \sum_{i,j=1}^{n} \mu_i\mu_j x_i x_j - 1$$

másodfokú polinom $x_1, \ldots, x_n$-ben
- Ha a (2) eset áll fenn, akkor minden mintabeli $v = (a_1, \ldots, a_n)$ vektorra $P_u(v) = 0$.
- Ha az (1) eset áll fenn, akkor nincs olyan legfeljebb másodfokú nem azonosan 0 $P \in \mathbb{Z}_3[x_1, \ldots, x_n] \in$ polinom, amelyre $P(v) = 0$ minden $v \in \mathbb{Z}_3^n$-re.

Elfogynak a polinomok

- **Tétel:** Ha $\ell = \Omega(n^2 \log n)$, egyenletesen véletlen $v_1, \ldots, v_\ell \in \mathbb{Z}^n$ vektorokra jó eséllyel **hatékonyan bizonyíthatóan** nem létezik olyan legfeljebb másodfokú nem azonosan 0 P n-változós polinom, amelyre $P(v_i) = 0$ minden $i = 1, \ldots, \ell$-re.

  Bizonyítás. $v = a_1, \ldots, a_n$-re

  $$behely_v(P) := P(a_1, \ldots, a_n)$$

  egy lineáris függvényt definiál a legfeljebb másodfokú polinomok $\mathcal{P}$ terén.

Elfogynak a polinomok 2

$v_1, \ldots, v_t \in \mathbb{Z}_3^n$ esetén azon $P \in \mathcal{P}$ polinomok, amelyekre $P(v_i) = behely_{v_i}(P) = 0$ $(i = 1, \ldots, t)$, $\mathcal{P}$-nek egy alterét alkotják.

Ez az altér jó eséllyel szűkül lépésenként: ha $0 \neq P \in \mathcal{P}$ olyan, hogy $P(v_i) = 0$ $(i = 1, \ldots, t)$, akkor annak a valószínűsége, hogy $P(v_{t+1}) \neq 0$ legalább $\frac{1}{3}$. (Schwartz–Zippel-lemma AKA általánosított Reed–Muller-kódok. kódtávolsága). (Természetesen igaz ez a $P(v_i) = 0$ feltétel nélkül is.)

Következésképpen az (1) esetben $\Omega(n^2 \log n)$ lépésben jó eséllyel az azonosan 0 lesz az egyetlen $\mathcal{P}$–beli P polinom, amelyre $P(v_i) = 0$ $(i = 1, \ldots, \ell)$ és ez hatékonyan bizonyítható is. □

Az eldöntési változat megoldása 2

- Összegyűjtünk egy elég nagy $v_1, \ldots, v_\ell$ mintát

$$\ell = \Omega(n^2 \log n)$$

- Ha nincs olyan legfeljebb másodfokú $0 \neq P \in \mathbb{Z}[x_1, \ldots, x_n]$ polinom, amire $P(v_1) = \ldots = P(v_\ell) = 0$, a válasz (1)
- Ha van, a válasz (2)

- Az ilyen P polinomok együtthatóvektorai a $v_1, \ldots, v_\ell$ vektoroktól függő lineáris egyenletrendszer megoldásai.

Megjegyzések

- Általánosítható $\mathbb{Z}_3^n$ helyett $\mathbb{Z}_q^n$-re (q prímhatvány)
  - Futási idő $(n+q)^{O(q)}$
  - Részletek: G. Ivanyos: On solving systems of random linear disequations (QIC 2008).
- Nyitott kérdések:
  - $\mathbb{Z}_6^n$-re polinomidejű megoldás?
  - $(nq)^{O(1)}$ vagy akár $2^{\log n \log q}$ idejű módszer? (q prím)
  - Értelmes közös általánosítás az Arora–Ge-féle "strukturált zaj"-modellel?