שיעור 1

27/10/14

שלשלאות הסתברותיות P והסתברותיות NP

הבעיה PM

קלט: גרף דו-צדדי $G=(V,N,E)$, $|V|=|W|$

פלט: 1 אם קיים $\pi \in S_{|V|}$ כך ש- $\forall i.\ (i,\pi(i)) \in E$, ו-0 אחרת.

$PM \in P$ ($\Leftarrow$ max-flow = min-cut, אלגוריתם פולינומי)

נראה אלגוריתם הסתברותי:

- נבנה מטריצה $M_{n\times n}$, שבה כל תא הוא:

$$M_{ij} = \begin{cases} 0 & (i,j) \notin E \\ x_{ij} & (i,j) \in E \end{cases}$$

- נגדיר $A \subseteq \mathbb{Z}$ שגודלה $2n$, למשל $A=\{1,\dots,2n\}$.

- נגדיר $a_{ij} \in_R A$ מספרים אקראיים, ונסמן $M(a) = M$ שבו x_{ij} הוחלף ב-a_{ij}.

- נחשב $\det(M(a))$.

אלגוריתם ⇔ הדטרמיננטה $\neq 0$.

הגדרה דטרמיננטה:

נסמן $M =$

$$\det(M) = \det(x_1 \dots x_m)$$

כאשר $x_{ij} = 0$ אז $(i,j) \notin \text{Diag}(M)$

$$= \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{i=1}^{n} x_{i,\pi(i)}$$

$$= \sum_{\pi \in S_n} \text{sgn}(\pi) \cdot x_{\pi(1),1} \dots x_{\pi(n),n}$$

$M = M^T$ אז M

אם $M \neq M^T$

אז $\det(x_1 \dots x_m) \equiv 0$ אם M

משפט דטרמיננטה:

אם M היא מטריצה כך ש, משפט דטרמיננטה

אז $M \in M$

$\det(M)$ הוא פולינום $= x_1 \dots x_m$ שבו x_i מוחלף ב $(x_m - x_i)$

(כלומר אפס אם M לא מוגדרת היטב)

$\deg(p) \leq n$ אז

משפט שוורץ-זיפל: יהי F שדה, ויהי $0 \neq P \in F[Y_1, \ldots, Y_m]$

$$|A| > \deg(P) \cdot |F \setminus A| \quad ,\quad A \subseteq F$$

אזי $\Pr_{a_1, \ldots, a_m \in_R A}[P(a_1, \ldots, a_m) = 0] \leq \frac{\deg(P)}{|A|}$

האלגוריתם RP

קבוצת L השפה $\exists$ אלג' M הסתברותי כך שלכל x

$$x \in L \Rightarrow \Pr_r[M(x,r) = 1] \geq \frac{1}{2}$$

$$x \notin L \Rightarrow \Pr_r[M(x,r) = 0] = 1$$

סימון: RP

$L \in RP$: $\Leftarrow$ $\exists$ אלג' $M \in RP$ כך ש...

- שימו לב, שאם נריץ את האלגוריתם k פעמים אז הסיכוי שכולן יחזירו 0 הוא לכל היותר $\frac{1}{2^k}$
- מכאן נובע, שאפשר להכניס את האלגוריתם לתוך לולאה

מחלקות סיבוכיות:

$$Log \subseteq P \subseteq RP \subseteq BPP \subseteq PSPACE$$

הגדרה: (מעגל בוליאני)

גרף מכוון חסר מעגלים (DAG)

קודקוד - קלט

קודקודים עם דרגת כניסה 0 - שערי קלט.

כל שער פנימי הוא אחד מהשערים הבאים:

- שער המכפלה
- שער החיבור
- שער השלילה (יש קודקוד יחיד עם דרגת כניסה 1 וגם יציאה אחת).

הגדרה: שפה L שייכת למחלקה $SIZE(s(n))$ אם קיימת סדרת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ כך שלכל n, גודל C_n קטן או שווה ל-$s(n)$.

הגדרה: שפה L שייכת למחלקה $P/poly$ אם קיימת סדרת מעגלים $\{C_n\}_{n\in\mathbb{N}}$ כך שלכל n, C_n מחשב את L על קלטים באורך n.

משפט: $L \in P$ אם ורק אם L מתקבלת על ידי מכונת טיורינג (TM) שרצה בזמן פולינומי.

NC^k הוא אוסף כל השפות ש-

שניתנות להכרעה ע"י מעגלים אוניפורמיים $\{C_n\}$

בעומק $O(\log^k n)$ וגודל n, עם שערים unbounded fan-in, כלומר AC.

$$NC^1 \subseteq L \subseteq NL \subseteq AC^1 \subseteq NC^2 \subseteq \dots \subseteq NC \subseteq P.$$

$$NC = \bigcup_k NC^k = \bigcup_k AC^k$$

CREW $PRAM(n^{O(1)})$ זמן $O(\log^k n)$ $\Leftrightarrow$ NC^k

משפט:

AC^0

parity AC^0

1) add, boolean-matrix-mult $\in AC^0$

2) parity, mult $\in NC^1$

בעיה: parity, mult $\notin AC^0$.

3) $NC^k \subseteq DSPACE(O(\log^k n))$

סיבוכיות סטנדרטית

מסקנות אלגוריתמים מעל שדה כללי F

DAG, שורש יחיד עם label 0, כל קודקוד שאינו שורש ולא עלה מקבל label $+$, שורשי הפונקציה עם label שווה למספר המשתנים.

מסקנה: אלגוריתמי AC ו AC_0 מתאים פולינום (מ-n משתנים) מעל F.

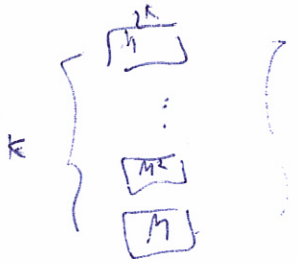
הגדרה: VNC^k, VAC^k אותן הגדרות כמו קודם רק עם $M^{(2^k)}$ במקום M^2.

דוגמא: $Det \in VAC^1$ מעל $\mathbb{R}$.

הוכחה: מהגדרת M מעל F. כלומר עבור M מטריצה $n \times n$ של $\{x_{ij}\}$.

VAC^0 = M^2 מטריצה.

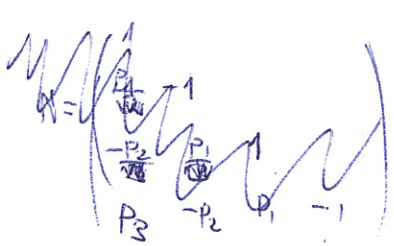
VAC = $M^{(2^k)}$

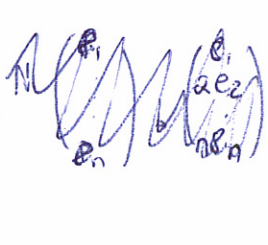


VAC^1 = k מטריצות $M^{(2^k)}$ מטריצה.

VAC^1 מחשבים M^k ואז מחשבים $P_k = \sum \lambda_i^k = Tr(M^k)$ ואת המטריצה

$$\sigma_k = \sum_{i_1 < \dots < i_k} \lambda_{i_1} \cdots \lambda_{i_k}$$





$$\begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = N \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

$$N = \begin{pmatrix} 1 & & & 0 \\ P_1 & -2 & & \\ P_2 & -P_1 & 3 & \\ P_3 & -P_2 & P_1 & -4 \\ & & & \ddots \end{pmatrix}$$

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = N^{-1} \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

N N

$$A_C^{-1} = N^{-1}$$

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & 0 \\ 0 & B^{-1} \end{pmatrix}$$

$$d(n) = d\left(\frac{n}{2}\right) + O(1) = O(\log n)$$

$$D = \underbrace{-B^{-1} C A^{-1}}_{A_C^{-1} \text{ של } D}$$

A_C^{-1} חישוב

A_C^{-1} חישוב:

Unbounded +
Bounded *

(depth $O(\log n)$).

מסקנה יהיו A ו־B מטריצות דומות. אזי

(רישום)
הוכחה

$$\sum \lambda_i^k = \operatorname{tr}(A^k)$$

מ־A ו־B יש אותם ערכים עצמיים (עם ריבוי אלגברי).

$$\sum \lambda_i = \operatorname{tr}(A)$$

λ_1 ערך עצמי של A ו־B עם ריבוי אלגברי k ו־m בהתאמה.

כלומר λ_1 הוא שורש של p_A ו־p_B בדיוק k ו־m פעמים.

λ_1 הוא ערך עצמי של A ו־B עם ריבוי גיאומטרי n ו־l בהתאמה.

כלומר $\dim E_A(\lambda_1) = n$ ו־$\dim E_B(\lambda_1) = l$.

משפט תהי $A \in M_n(\mathbb{C})$. אזי A דומה למטריצת ז'ורדן.

הוכחה ראו בקורס אלגברה לינארית 2.

מסקנה יהי $A \in M_n(\mathbb{C})$. אזי

$$p_A(\lambda) = \prod (\lambda_i - \lambda) = \sum \binom{n}{i} (-\lambda)^i$$

כאשר λ_i הם הערכים העצמיים של A.

הגדרה יהי $A \in M_n(\mathbb{C})$. הפולינום האופייני של A הוא $p_A(\lambda) = \det(A - \lambda I)$.

כאשר יש ריבוי אלגברי:

14/11/13

- הגדרת קבוצה חסומה

- אין קבוע שגדול $\frac{B}{A}$ ← סוגר מצד A וגדול B

3. מצאו דוגמאות

.. אבל מתקיים $z^{\frac{1}{3}} \leq z^{\frac{2}{3}}$,$z \geq 1$

יש הוכחה שקיים $O(g)$ ואומרת f חסומה (אפשר בדרך שלנו)

2. יש הוכחה (אפשר בדרך שלנו) שקיים f חסומה

כלומר נשאר עוד שאלה מהגדרה $\Rightarrow$ אז מתקיים

מקיים אחד מהבאים, ואין אחד

f חסומה $(z)O$,ואומרת

f חסומה בקשת Im/Re bounded

f חסומה בקשת Im/Re bounded from above

1. יש חסם עליון Im/Re bounded from above

פתרון תרגיל

RNC^k ...

... $C(x,y)$ ... , ...

RNC^k ב

$x \in L \Rightarrow \Pr_{y}(C(x,y)=1) \geq \frac{2}{3}$ ... $x \notin L \Rightarrow \Pr_{y}(\quad) \leq \frac{1}{3}$ =0

$PM \in RNC^*$:הערה

RNC^k - ... ...

... ...

... $O(\log^k n)$ ...

... PM ... ...

... $RNC^k \overset{?}{=} Pspace(O(\log^k n))$ ...

PIT

C מעגל חלוקתי, F שדה

טענה: $C \equiv 0 \Leftrightarrow$ C מחשב פולינום אפסי שדרגת כל מונום בו לכל היותר $\deg(C)$.

מסקנה: $\text{PIT} \in \text{coRP}$

הוכחה: נתון $C(x_1, \ldots, x_n)$

נגריל A שגודלה פולינומי

$r_1, \ldots, r_n \in A$

ונחשב $C(r_1, \ldots, r_n)$

אם התקבל 0 – נניח ש

אם התקבל $\neq 0$ – נניח ש

$C \not\equiv 0$

$\Pr[\text{error}] \leq \frac{\deg(C)}{|A|}$

כמה $\deg(C)$?

נניח שגודל המעגל m (מספר השערים בו).

אז $\deg(C) \leq 2^m$.

כי כל שער כפל – לכל היותר מכפיל את הדרגות.

Primality testing

טענה $(x+1)^n = x^n+1 \pmod n$ ⟺ n ראשוני

הוכחה אם n ראשוני: $f(x)=(x+1)^n - x^n - 1$

פולינום ממעלה $\le n-1$ (כי x^n מתבטל)

ומצד שני ב-F_n (שהוא שדה) מתקיים, כי לכל $a \in F_n$

מפמ"ק $a^n=a$, ולכן $(a+1)^n - a^n - 1 = a+1-a-1=0$

אבל f ממעלה $\le n-1$ עם n שורשים ולכן $f\equiv 0$.

כלומר f פולינום האפס.

אם n אינו ראשוני, נניח $k|n$ k הראשוני הכי קטן שמחלק את n (ראשוני).

אז $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{1\cdots k}$

$k|n$ ולכן $k\nmid n-i$ עבור $i=1,\ldots,(k-1)$

ולכן אם $n=k^i a$ $(a,k)=1$

אז $k^i \nmid \binom{n}{k}$, ולכן $\binom{n}{k}\not\equiv 0 \pmod n$.

ולכן המקדם של x^k אינו אפס ב-$f(x)$. $f\not\equiv 0$.

אלגוריתם הסתברותי: PIT משתנה אחד.