

סיבוכיות

© ארזים

23 במאי 2017

1 אלגוריתמים הסתברותיים

בשיעור שעבר התחלנו לדבר על אלגוריתמים הסתברותיים.

הגדרה 1.1 המחלקה $BPP(\alpha, \beta)$ מכילה את כל השפות A שלהן יש פולינום r ומכונת טירינג $M(x, y)$ עם $|y| \leq r(|x|)$ כך שמתקיים:

1. M רצה בזמן לכל היותר $r(|x|)$.

2. אם $x \in A$ אזי

$$\mathbb{P}_y(M(x, y) = 1) \geq 1 - \beta$$

3. אם $x \notin A$ אזי

$$\mathbb{P}_y(M(x, y) = 1) \leq \alpha$$

ראינו בשיעור שעבר את השוויונות הבאים:

$$\begin{aligned} RP &:= BPP\left(0, \frac{1}{2}\right) = BPP\left(0, \frac{1}{2^n}\right) \\ BPP &:= BPP\left(\frac{1}{3}, \frac{1}{3}\right) = BPP\left(\frac{1}{3^n}, \frac{1}{3^n}\right) \end{aligned}$$

אפשר לחזק את זה.

תרגיל נניח כי $0 < \alpha, \beta \leq 1$ כך שקיים קבוע c עבורו

$$1 - \beta \geq \alpha + \frac{1}{n^c}$$

אזי

$$BPP = BPP(\alpha, \beta)$$

הגדרה 1.2 מכונת טיורינג הסתברותית היא מכונה עם אחד מהשינויים השקולים הבאים:

1. במקום פונקציית מעברים δ יש שתי פונקציות δ_0, δ_1 ובכל שלב בהסתברות $\frac{1}{2}$ בוחרים את מי מהן להפעיל.
2. יש סרט נוסף עם ראש שזז רק ימינה. בכל שלב נכתב על הסרט מימין לראש 0 או 1 (כל אחד בהסתברות $\frac{1}{2}$).
3. δ היא מהצורה

$$\delta : (\Gamma \times Q) \times (\Gamma \times Q \times \{\leftarrow, \rightarrow\}) \rightarrow [0, 1]$$

כך שבהינתן מצב מתוך $\Gamma \times Q$, הפונקציה δ היא פונקציית הסתברות עליו. כלומר, לכל q_0, γ_0 מתקיים

$$\sum_{(g,q,d) \in \Gamma \times Q \times \{\leftarrow, \rightarrow\}} \delta((\gamma_0, q_0), (g, q, d)) = 1$$

עבור $t : \mathbb{N} \rightarrow \mathbb{R}$, מכונת טיורינג הסתברותית מכריעה שפה A בזמן t אם לכל $x \in \{0, 1\}^*$ מתקיים

$$\begin{aligned} x \in A &\Rightarrow \mathbb{P}(M(x) = 1) \geq \frac{2}{3} \\ x \notin A &\Rightarrow \mathbb{P}(M(x) = 0) \geq \frac{2}{3} \end{aligned}$$

מחלקת השפות המתקבלת כך נקראת $\text{BPTIME}(t)$, ומגדירים

$$\text{BPP} = \bigcup_c \text{BPTIME}(n^c)$$

נראה אלגוריתם רנדומי עבור 2SAT. נבחר השמה באקראי. במשך $1000n^2$ צעדים, אם בידינו השמה לא מספקת, בוחרים פסוקית שלא הסתפקה, ובוחרים באקראי את אחד המשתנים בה. משנים את הערך שלו.

ניתוח זמן ריצה בבירור פולינומיאלי. אם יש לנו נוסחא לא ספיקה, תמיד נדחה. אם אי פעם נמצא השמה מספקת אז נקבל - נרצה לדעת באיזו הסתברות זה קורה.

רעיון תהי ρ השמה מספקת כלשהי. אנחנו בחרנו השמה x_0 , שהיא באיזשהו "מרחק" d מההשמה ρ , כאשר מרחק בין שתי מחרוזות הוא כמות הקואורדינטות ביניהן ששונות. אם הרצנו את האלגוריתם t צעדים, ההסתברות שלא נגיע למרחק 0 היא שווה להסתברות שמספר הצעדים המקרבים לא עולה על מספר הצעדים המרחיקים ביותר מאשר d . כמות הצעדים המרחיקים לא יכול לעלות ביותר מאשר $n - d$ ממספר הצעדים המקרבים. נחשב את ההסתברות לכשלוך (דחיה של נוסחה ספיקה) - k יסמן את כמות הצעדים המרחיקים:

$$P \leq \sum_{k=\frac{t}{2}-\frac{d}{2}}^{\frac{t}{2}+\frac{n-d}{2}} \binom{t}{k} \frac{1}{2^k} \frac{1}{2^{t-k}} \leq n \cdot \binom{t}{\frac{t}{2}} \frac{1}{2^t} \approx \theta\left(\frac{n}{\sqrt{t}}\right)$$

מה לגבי 3SAT? נחזור על אותו תהליך - ההבדל העיקרי הוא שכעת אנחנו יכולים להבטיח רק שבהסתברות $\frac{1}{3}$ נתקרב להשמה מספקת. זה נותן אלגוריתם עם זמן ריצה שהוא פולינום כפול 3^n . נראה שאפשר לקבל אלגוריתם עם זמן ריצה בערך פולינום כפול $(\frac{4}{3})^n$ - האלגוריתם הטוב ביותר הידוע היום הוא עם בסיס 1.32 לאקספוננט.

ניתוח נניח שהמרחק ההתחלתי של ההשמה שבחרנו מהשמה מספקת ρ הוא d . נחשב את הסיכוי שתוך $3d$ צעדים, נגיע אל ρ .

$$\binom{3d}{d} \frac{1}{3^{2d}} \frac{2^d}{3^d}$$

סך הכל ההסתברות היא

$$\begin{aligned} \sum_{d=0}^n \frac{\binom{n}{d}}{2^n} \binom{3d}{d} \frac{1}{3^{2d}} \frac{2^d}{3^d} &\approx c \sum_{d=0}^n 2^{-n} \binom{n}{d} \frac{2^d}{3^{3d}} \underbrace{\frac{1}{\sqrt{d}} \frac{3^{3d}}{2^{2d}}}_{\approx \binom{3d}{d}} = \\ &= c \sum_d 2^{-n} \binom{n}{d} \frac{1}{2^d} \frac{1}{\sqrt{d}} \geq \frac{c}{\sqrt{n}} 2^{-n} \sum_d \binom{n}{d} 2^{-d} = \\ &= \frac{c}{\sqrt{n} 2^n} \left(1 + \frac{1}{2}\right)^n = \frac{c}{\sqrt{n}} \frac{3^n}{4^n} = p \end{aligned}$$

כמו שרצינו. אם נחזור על האלגוריתם $\frac{1}{p}a$ פעמים, ההסתברות שניכשל הכל הפעמים היא

$$(1-p)^{\frac{a}{p}} = \frac{1}{e^a}$$

לכן בזמן ריצה פולינומיאלי כפול $(\frac{4}{3})^n$ נמצא השמה מספקת בהסתברות ממש טובה.

משפט 1.3 (אדלמן) לשפות מתוך BPP יש מעגלים פולינומיאליים. במילים אחרות, אם $A \in \text{BPP}$ אז יש קבוע b וסדרת מעגלים C_n עם $|C_n| \leq n^b$ המכריעה את A .

הוכחה: כמו שראינו, $\text{BPP} = \text{BPP}(\frac{1}{2^{2n}}, \frac{1}{2^{2n}})$, כלומר על קלטים באורך n ההסתברות לטעות היא לכל היותר $\frac{1}{2^{2n}}$. תהי $A \in \text{BPP}$, ותהי M מכונת טירינג הסתברותית המקבלת אותה עם טעות לכל היותר 2^{-2n} על קלטים באורך n . נטען שלכל n יש מחרוזת y באורך פולינומי באורך x כך שמתקיים

$$\begin{aligned} x \in A &\Rightarrow M(x, y) = 1 \\ x \notin A &\Rightarrow M(x, y) = 0 \end{aligned}$$

זה נכון כי אפשר לבחור את y באקראי, ואז

$$\begin{aligned} \mathbb{P}_y(\exists x \in A, |x| = n, M(x, y) = 0) &\leq \frac{1}{2^{2n}} 2^n = \frac{1}{2^n} \\ \mathbb{P}_y(\exists x \notin A, |x| = n, M(x, y) = 1) &\leq \frac{1}{2^n} \end{aligned}$$

לכן נקבל כי

$$\mathbb{P}_y (\forall x, |x| = n \ M(x, y) \text{ is correct}) \geq 1 - 2^{-n} - 2^{-n} > 0$$

ולכן בפרט קיים y שכזה.

■ המעגל לקלטים באורך n ייקח את y הזה ויסמלץ את $M(x, y)$ על קלט x .