דוגמה: זרימה ברשת אפשר לבטא כך: * $G=(V,A)$ גרף מכוון

* $c: A\to\mathbb{N}$ פונ' קיבול
* $s,t\in V$ מקור ובור

המשתנים יהיו ערך הזרימה $f(u,v)$ על הקשתות המכוונות $(u,v)\in E$.

נרצה למקסם את:

$$\max\left\{\sum_{\substack{v\in V\\ \{s,v\}\in A}} f(s,v) - \sum_{\substack{v\in V\\ \{v,s\}\in A}} f(v,s)\right\}$$

אילוץ הקיבול: $$\text{s.t}\quad \forall (u,v)\in A\quad f(u,v)\le c(u,v)$$

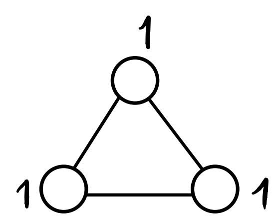
אילוץ שימור החומר: $$\wedge\quad \forall u\in V/\{s,t\}\quad \sum_{\substack{v\in V\\ \{v,u\}\in A}} f(v,u) = \sum_{\substack{v\in V\\ \{u,v\}\in A}} f(u,v)$$

אי-שליליות הזרימה: $$\wedge\quad \forall (u,v)\in A\quad f(u,v)\ge 0$$

שאלה: האם תמיד יש פתרון אופטימלי בשלמים?

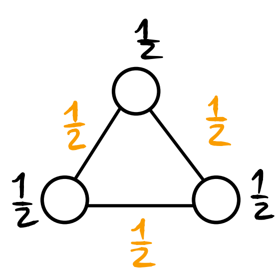
- לא! לדוגמה, התכנית לחישוב z^*.

דוגמה:



כל המשקלים 1

כיסוי בצמתים קל ביותר הוא 2.



לעומת זאת, $z^*=\frac{3}{2}$

ההצבה של $\frac{1}{2}$ לכל המשתנים

מראה ש- $z^*\le\frac{3}{2}$

הפתרון הדואלי שמציב $\frac{1}{2}$ לכל המשתנים מראה ש- $z^*\ge\frac{3}{2}$.

(כי $u^*\ge\frac{3}{2}$)

בעיית אלגוריתמי הירוב - תחזיות

מקבלים תחזיות של n מומחים שמפרסמים כל יום מה יקרה למחרת.
(למשל - "ירד גשם או לא ירד גשם) כאשר התחזית היא בינארית: 0 או 1.
אנחנו נחליט כל יום החלטה בהתאם לתחזית ונרצה לא להכשל יותר
מהמומחה הכי טוב.

אלגוריתם פשוט: נחזיק קבוצה X של מומחים
בהתחלה X הם כל המומחים
נחליט עפ"י דעת הרוב בקבוצה X
אם טעינו, נוריד את המומחים שטעו מ-X
אם X ריקה, נאתחל שוב את X עם כל המומחים

משפט: אם המומחה הטוב ביותר שוגה K פעמים $(K\geq 0)$, אזי,
האלגוריתם שוגה לכל היותר $(K+1)\log_2 n$ פעמים.

הוכחה: באינדוקציה על K.
בסיס האינדוקציה: $K=0$, בכל פעם שהאלגוריתם שוגה, מסירים מ-X לפחות
חצי מהמומחים שם. יש מומחה שאינו שוגה כלל ולכן X אף פעם לא ריקה.
לכן מספר השגיאות שלנו הוא $\log_2 n = (0+1)\log_2 n$ (כי $|X|=n$ בהתחלה).
צעד האינדוקציה: נניח שהטענה נכונה אם המומחה הטוב ביותר שוגה פחות מ-K
פעמים. נניח שהמומחה ה-i שוגה סה"כ K פעמים. נתבונן בצעדי האלגוריתם
עד ש-X מתרוקנת בפעם הראשונה. עד לנקודה זו, האלגוריתם שגה לכל היותר
$\log_2 n$ פעמים. כמו כן, i שגה לפחות פעם אחת.

החל מנק' כזו, i שוגה לכל היותר K-1 פעמים. לכן, לפי הנחת האינדוקציה, האלג' לא ישגה יותר מ-$K\log_2 n$ פעמים. סה"כ מקבלים: $(K+1)\log_2 n$ שגיאות של האלג' לכל היותר.

תרגול 10 - "רוב ממושקל"

אלגוריתם מוצלח יותר:

נסמן מחדש את התחזיות להיות 1+ או 1-.

ונסמן ב-c_i^t את התחזית של המומחה ה-i בצעד ה-t.

נחזיק לכל מומחה משקל w_i^t ונאתחל: $w_i^1=1$ לכל i.

התחזית שלנו בצעד ה-t: הסימן של $\sum_i w_i^{(t)}c_i^{(t)}$ ⊛

עדכון: לכל מומחה i שטעה: $w_i^{(t+1)}=\frac{1}{2}w_i^{(t)}$

ולכל מומחה i שצדק: $w_i^{(t+1)}=w_i^{(t)}$

נסמן ב-m_i^t את מס' הטעויות של המומחה ה-i ב-t הצעדים הראשונים.

נסמן ב-$M(t)$ את מס' הטעויות של האלג' ב-t הצעדים הראשונים.

משפט: לכל מומחה i ולכל t מתקיים: $M(t)\le \frac{1}{\log_2(\frac{4}{3})}\left(m_i^{(t)}+\log_2 n\right)$

הוכחה: נסמן פונקציית פוטנציאל $\phi(t)=\sum_i w_i^{(t)}$

לפי האתחול: $\phi(1)=n$

לכל מומחה i ולכל t מתקיים: $\phi(t+1)=\sum_i w_i^{(t+1)} > w_i^{(t+1)} = 2^{-m_i^{(t)}}$

<u>מה קורה כאשר האלגוריתם שוגה?</u>

מ-⊛ נסיק שמשקל המומחים ששגו הוא לפחות חצי מהכולל.

אם שגינו בצעד ה-t אז: $\sum_{\text{i שגה}} w_i^{(t)} \ge \frac{1}{2}\sum_i w_i^{(t)}$

לכן $\sum_i w_i^{(t+1)} = \frac{1}{2}\sum_{i\ \text{שטעו}} w_i^{(t)} + \sum_{i\ \text{שלא טעו}} w_i^{(t)} \le \frac{3}{4}\sum_i w_i^{(t)}$

$$2^{-m_i^{(t)}} \le \left(\frac{3}{4}\right)^{M(t)} \cdot \Phi(1) = \left(\frac{3}{4}\right)^{M(t)} \cdot n \Longrightarrow 2^{-m_i^{(t)}} \le \left(\frac{3}{4}\right)^{M(t)} \cdot n \xRightarrow{\log_2()}$$

$$-m_i^{(t)} \le \log\left(\frac{3}{4}\right) M(t) + \log_2 n \Longrightarrow \overset{\text{העברת אגפים}}{\left(\underbrace{-\log_2\left(\frac{3}{4}\right)}_{\log_2\left(\frac{4}{3}\right)}\right)} M(t) \le m_i^{(t)} + \log_2 n$$

$$\xRightarrow{\text{העברת אגפים}} M(t) \le \frac{1}{\log_2\left(\frac{4}{3}\right)}\left(m_i^{(t)} + \log_2 n\right)$$

ננסה לשפר באופן יותר מתון: $w_i^{(t+1)} = \frac{1}{1+\varepsilon} w_i^{(t)}$ עבור $\varepsilon>0$.

נקבל: $\left(\frac{1}{1+\varepsilon}\right)^{m_i^{(t)}} \le \Phi(t+1) \le \left(1-\frac{\varepsilon}{2(1+\varepsilon)}\right)^{M(t)} \cdot n \xRightarrow{\ln()}$

$$(-\ln(1+\varepsilon))\, m_i^{(t)} \le \left(-\ln\left(\frac{2+2\varepsilon}{2+\varepsilon}\right)\right) M(t) + \ln(n) \xRightarrow{\text{העברת אגפים}}$$

$$M(t) \le \overset{\le 1+\varepsilon}{\frac{\ln(1+\varepsilon)}{\ln\left(\frac{2+2\varepsilon}{2+\varepsilon}\right)}}\, m_i^{(t)} + \overset{\le \frac{1}{\varepsilon}}{\frac{1}{\ln\left(\frac{2+2\varepsilon}{2+\varepsilon}\right)}} \cdot \ln(n)$$

יום ראשון 30.5.21

מקרא:
- דוגמה
- הוכחה
- טענה
- משפט
- הגדרה

אלגוריתמים
שבוע 10- הרצאה 19
אלגוריתמים הסתברותיים

המשקל בע"ית המומחים:

נניח שבכל יום מוטלים על המומחים קנסות בקטע $[-1,+1]$. באופן שרירותי

נסמן ב- $c_i^t \in [-1,+1]$ את הקנס המוטל על המומחה ה-i ביום ה-t.

האלגוריתם בוחר בכל יום t, התפלגות p^t על המומחים לפני שחושפים את הקנסות. כלומר, לכל i, $p_i^t \geq 0$ וכמו כן $\sum_{i=1}^{n} p_i^t = 1$.

וביום ה-t האלגוריתם משלם $\sum_{i=1}^{n} p_i^t c_i^t$.

סה"כ הקנסות שמשלם האלג' על פני T הם: $\sum_{t=1}^{T}\sum_{i=1}^{n} p_i^t c_i^t$

נרצה להשוות התשלום הזה לתשלום של המומחה הטוב ביותר: $\min_{i=1,..,n}\sum_{t}^{T} c_i^t$

נחזיק משקלים לכל המומחים, נסמן ב-w_i^t את המשקל של המומחה ה-i בתחילת היום ה-t.

ההתפלגות שהאלג' "משחק" היא: $p_i^t = \frac{w_i^t}{\sum_{j=1}^{n} w_j^t}$

המשקלים מתעדכנים אחר חשיפת הקנסות באופן הבא: $w_i^{t+1} = (1-\varepsilon c_i^t) w_i^t$

עבור $0 < \varepsilon$ שנקבע מראש. מתחילים עם $w_i^1 = 1$ לכל i.

משפט בהנחה ש-$0 < \varepsilon \leq \frac{1}{2}$ מתקיים אחרי T צעדים, לכל מומחה i:

$$\underbrace{\sum_{t=1}^{T}\sum_{i=1}^{n} c_i^t p_i^t}_{\text{התשלום של האלגוריתם}} \leq \underbrace{\sum_{t=1}^{T} c_i^t}_{\text{התשלום של המומחה ה-}i} + \underbrace{\varepsilon \sum_{t=1}^{T} |c_i^t| + \frac{1}{\varepsilon}\ln(n)}_{\text{התשלום הנוסף של האלג' במקרה הגרוע}}$$

הוכחה: נגדיר $\phi(t)=\sum_{i=1}^{n} w_i^t$. אז:

על פי כלל העדכון

$$\phi(t+1)=\sum_{i=1}^{n} w_i^{t+1} = \sum_{i=1}^{n} w_i^t(1-\varepsilon c_i^t) = \phi(t) - \varepsilon \sum_{i=1}^{n} w_i^t c_i^t \overset{(*)}{=}$$

$$\phi(t) - \varepsilon\cdot\phi(t)\sum_{i=1}^{n} p_i^t c_i^t = \phi(t)\left(1-\varepsilon\sum_{i=1}^{n} p_i^t c_i^t\right) \overset{1-x\le e^{-x}}{\le} \phi(t)\cdot e^{-\varepsilon\sum_{i=1}^{n} p_i^t c_i^t}$$

כאשר: $p_i^t = \frac{w_i^t}{\phi(t)} \Rightarrow w_i^t = p_i^t\cdot\phi(t)$ $(*)$

נתחיל מאיבר מסוים ונפתח רקורסיבית עד $\phi(1)$:

(1)

$$\phi(T+1) \le \phi(1)\cdot e^{-\varepsilon\sum_{t=1}^{T}\sum_{i=1}^{n} p_i^t c_i^t} = n\cdot e^{-\varepsilon\overbrace{\sum_{t=1}^{T}\sum_{i=1}^{n} p_i^t c_i^t}^{\text{מחיר האלג' ב-T הצעדים הראשונים}}}$$

אנו רוצים חסם תחתון שמערב את המחיר של המומחה ה-i, אז ניתן לכתוב:

(2)

$$\phi(T+1) \ge w_i^{T+1} \overset{(*)}{=} \prod_{t=1}^{T}(1-\varepsilon c_i^t) \overset{(*)}{\ge} (1-\varepsilon)^{\sum_{t|c_i^t\ge 0} c_i^t}(1+\varepsilon)^{\sum_{t|c_i^t<0} c_i^t}$$

כאשר: $(*)$

$$\alpha\in[0,1] \Rightarrow (1-\varepsilon)^{\alpha} \le 1-\varepsilon\alpha$$

$$\alpha\in[-1,0] \Rightarrow (1+\varepsilon)^{-\alpha} \le \underbrace{1-\varepsilon\alpha}_{\ge 1}$$

$(*)$ אמרנו ש-w_i^t מתחיל ב-1 ומתעדכן כל פעם לפי הקנס של המומחה ה-i.

מ-(1) ו-(2) נקבל כי:

$$(1-\varepsilon)^{\sum_{t|c_i^t\ge 0} c_i^t}(1+\varepsilon)^{\sum_{t|c_i^t<0} c_i^t} \le \phi(T+1) \le n\cdot e^{-\varepsilon\overbrace{\sum_{t=1}^{T}\sum_{i=1}^{n} p_i^t c_i^t}^{\text{מחיר האלג' ב-T הצעדים הראשונים}}} \Rightarrow \ln()$$

$$\ln(n) - \varepsilon \sum_{t=1}^{T}\sum_{i=1}^{n} p_i^t c_i^t \geq \ln(1-\varepsilon)\sum_{t|c_i^t\geq 0} c_i^t - \ln(1+\varepsilon)\sum_{t|c_i^t<0} c_i^t \quad \Longrightarrow \quad \cdot\left(-\frac{1}{\varepsilon}\right) \; + \ln(n)$$

$$\sum_{t=1}^{T}\sum_{i=1}^{n} p_i^t c_i^t \leq \frac{1}{\varepsilon}\ln(n) + \frac{\ln\left(\frac{1}{1-\varepsilon}\right)}{\varepsilon}\cdot\sum_{t|c_i^t\geq 0} c_i^t + \frac{\ln(1+\varepsilon)}{\varepsilon}\sum_{t|c_i^t<0} c_i^t \leq^{(*)}$$

$$\leq \frac{1}{\varepsilon}\ln(n) + \sum_{t=1}^{T} c_i^t + \varepsilon\cdot\sum_{t=1}^{T} |c_i^t|$$

$$\forall \varepsilon \in \left[0, \tfrac{1}{2}\right] \quad \begin{aligned} \ln\left(\frac{1}{1-\varepsilon}\right) &\leq \varepsilon + \varepsilon^2 = \varepsilon(1+\varepsilon) \\ \ln(1+\varepsilon) &\leq \varepsilon - \varepsilon^2 = \varepsilon(1-\varepsilon) \end{aligned} \quad (*)$$

יום שלישי 1.6.21

מקרא:
דוגמה - 🔵 הוכחה - 🔴
טענה - 🟠 משפט - 🟢
הגדרה - 🔴

אלגוריתמים
שבוע 10 - הרצאה 20
אלגוריתמים הסתברותיים

אלגוריתם המשקול הכפלי

מחזיקים משקלים של המומחים, w^t, בוחרים בהתפלגות p^t את המומחים שהוא: $p_i^t = \frac{w_i^t}{\sum_{j=1}^{n} w_j^t}$ ומעדכנים $w_i^{t+1} = (1-\varepsilon c_i^t) w_i^t$ עבור $\varepsilon \in (0, \frac{1}{2}]$.

הוכחנו: לכל T,

משפט: בהנחה ש-$0 < \varepsilon \leq \frac{1}{2}$ מתקיים אחרי T צעדים, לכל מומחה i:

$$\underbrace{\sum_{t=1}^{T} \sum_{i=1}^{n} c_i^t p_i^t}_{\text{התשלום של האלגוריתם}} \leq \underbrace{\sum_{t=1}^{T} c_i^t}_{\text{התשלום של המומחה ה-}i} + \underbrace{\varepsilon \sum_{t=1}^{T} |c_i^t| + \frac{1}{\varepsilon} \cdot \ln(n)}_{\text{התשלום הנוסף של האלג' במקרה הגרוע}}$$

עבור i כלשהו

הקנס של המומחה הטוב ביותר

הסטייה שלנו מהאופטימום $\leq \varepsilon \cdot T + \frac{1}{\varepsilon} \ln(n)$

כל זה הוא מקרה פרטי של המשפט עבור ε אידיאלי:

אם נבחר $\varepsilon = \sqrt{\frac{\ln(n)}{T}}$ השגיאה פרופורציונית ל- $\sqrt{T \ln(n)}$

$\Leftarrow$ כלומר, השגיאה הממוצעת לצעד היא פרופורציונית ל: $\frac{1}{T} \cdot \sqrt{T \ln(n)} = \sqrt{\frac{\ln(n)}{T}}$

הערה: יש וריאציה של שיטת המשקול הכפלי שנקראת Hedge שבה עדכון המשקלים הוא $w_i^{t+1} = w_i^t \cdot e^{-\varepsilon c_i^t}$.

$1 - \varepsilon c_i^t$ (או השוויון $1 - x \leq e^{-x}$)

נתבונן בתכנית הלינארית הבאה (שכבר ראינו):

משקלים חיוביים של צמתים

$$\begin{cases} \min \sum_{v\in V} w_v x_v \\ s.t.\ \forall (u,v)\in E \quad x_u+x_v \geq 1 \\ x \geq 0 \end{cases}$$

בעיית כיסוי הצמתים

נניח שאנו רוצים לפתור את התכנית הנ"ל, די לפתור את בעיית ההכרעה הבאה:
האם קיים $x\geq 0$ עבורו לכל קשת $(u,v)\in E$ מתקיים $x_u+x_v\geq 1$ וגם $\sum_{v\in V} w_v x_v \leq \beta$ עבור קלט β.

בהינתן פתרון לבעיית ההכרעה הנ"ל, אפשר לפתור את התכנית הלינארית ע"י חיפוש בינארי על β (ובכך נמצא את β שיהווה את האופטימום).

לכן ניתן להתחיל את הבעיה המקורית בבעיה הבאה:
נבדוק האם קיים $x\geq 0$ עבורו מערכת אי שיוויונים לינאריים $Ax\geq b$ מתקיימת, עבור מטריצת אילוצים A ווקטור b.

אין פה בעיית אופט' לכן לא מדובר באלג' קירוב אלא על אלג' שפותר בעיה קרובה (כמו 3-SAT מהתרגול)

<u>פתרון מקורב לבעיית ההכרעה הנ"ל:</u>
- נכריע בוודאות שאין x כזה. או
- נמצא $x\geq 0$ עבורו לכל אי-שיוויון i יתקיים $A_i x\geq b_i-\delta$ עבור $\delta>0$ כלשהו.

<u>נשים לב:</u> אם האלג' מחזיר לא - אז כזה גם לא באלג' האמיתי!
ואם מחזיר כן, אז מתקיים משהו קרוב לדרישה - עד כדי δ.

נסמן את מס' האילוצים ב-m ואת מס' המשתנים ב-n. מימדים: $A\in\mathbb{R}^{m\times n}, x\in\mathbb{R}^n, b\in\mathbb{R}^m$

מפתרון מקורב לבעיית ההכרעה, נרצה למצוא פתרון קרוב לאופטימלי לתכנית הלינארית.

ניתן לעשות זאת באופן הבא:

*נשים לב שאם $b_i \geq 1-\rho$ לכל i ו-δ מאוד קטן בערך $1-\delta$, אז אם $x \geq 0$ מקיים $Ax \geq b - \begin{bmatrix} | \\ \delta \\ | \end{bmatrix}$ אז $x' = \frac{1}{1-\delta}$ מקיים $Ax' \geq b$.

(בהנחה למשל, שהמקדמים במטריצה A חיוביים).

כי המטרה הוכפלה ב-$\frac{1}{1-\delta}$.

נצטרך להוכיח שקיים בידינו אלג' O לבעיה פשוטה יותר:

בהינתן התפלגות p על השורות של A, לבדוק האם קיים $x \geq 0$ עבורו $\sum_{i=1}^{m} p_i A_i \cdot x \geq \sum_{i=1}^{m} p_i b_i$ ⊛

מדובר בהנחה שנצטרך על מנת לפתור את הבעיה בעתיד

עוד נניח שאם קיים פתרון x כזה (שפותר את ⊛) אנחנו מוצאים x עבורו לכל i $|A_i \cdot x - b_i| \leq \rho$ עבור איזשהו פרמטר ρ (שנקרא הרוחב של הבעיה).

עוד הנחה כזאת

שימו לב: אם קיים $x \geq 0$ עבורו $Ax \geq b$ אז x הנ"ל מקיים את אי-השוויון

$$\sum_{i=1}^{m} p_i A_i x \geq \sum_{i=1}^{m} p_i b_i \quad ⊛$$

ρ - כמה ה-x שלי רחוק ממקום הפתרון

כל מה היה כדי שנוכל לנסח את המשפט:

משפט: בהינתן $\delta > 0$, אלג' O עם $\rho \geq \frac{\delta}{2}$, קיים אלג' שקורא ל-$O$ לכל היותר $O(\frac{\rho^2}{\delta^2} \log m)$ פעמים ומחזיר $x \geq 0$, עבורו לכל $i = 1,..,m$ מתקיים $A_i \cdot x \geq b_i - \delta$, או מכריז נכון שאין $x \geq 0$ עבורו $Ax \geq b$.

הוכחה: בהינתן $x \ge 0$ כלשהו, נגדיר קנסות לאילוצים: $c_i(x) = \frac{1}{\rho}(A_i \cdot x - b_i)$

$c_i(x) \in [-1,+1]$

האלג' יבצע איטרציות של עדכון x. בתחילת האיטרציה ה-t האלג' מחזיק התפלגות p^t על האילוצים (השורות של A), ובהתחלה זו התפלגות אחידה.

<u>עדכון ההתפלגות:</u> ראשית, מוצאים $x^t \ge 0$ שמקיים $\sum_{i=1}^{m} p_i^t A_i x^t \ge \sum_{i=1}^{m} p_i^t b_i$

(אם מצאנו כזה, אז הוא בתוך הרוחב המוגדר: $[-\rho,+\rho]$).

אם אין כזה, אז אין פתרון $x \ge 0$ שמקיים $Ax \ge b$ וניתן להכריז שאין פתרון.

אחרת, מתעדכנים p^{t+1} לפי שיטת המשקול הכפלי עם המחירים $c_i^t = c_i(x^t)$.

(ופרמטר עדכון $\varepsilon > 0$).

נשים לב, בכל צעד t:

$$\sum_{i=1}^{m} c_i^t p_i^t = \frac{1}{\rho}\sum_{t=1}^{T}(A_i x^t - b_i)p_i^t \overset{\text{כי x מקיימות}}{\geq} 0$$

מנגד, לפי מה שהוכחנו בנוגע לשיטת המשקול הכפלי:

$$0 \le \sum_{t=1}^{T}\sum_{i=1}^{m} c_i^t p_i^t \le \underbrace{\frac{1}{\rho}\sum_{t=1}^{T}(A_i x^t - b_i)p_i^t}_{\text{הקנס שמשלם האילוץ ה-i}} + \underbrace{\varepsilon\sum_{t=1}^{T}\frac{1}{\rho}|\underbrace{A_i x^t - b_i}_{\le 1}| + \frac{1}{\varepsilon}\ln(n)}_{\text{הסטייה והיא מקיימת: } \le \varepsilon T}$$

נניח שהי' לנו רק את החלק ⊛, אז היינו מקבלים:

$$0 \le \frac{1}{T}\sum_{t=1}^{T}\cancel{\frac{1}{\rho}}(A_i x^t - b_i)p_i^t = A_i \cdot \Big(\underbrace{\frac{1}{T}\sum_{t=1}^{T}x^t}_{\text{פתרון לבעיה שרצינו לפתור}}\Big) - b_i$$

נסמן $\bar{x} = \frac{1}{T}\sum_{t=1}^{T}x^t$, נכפיל את ⊛+⊛ ב-$\frac{\rho}{T}$ ונקבל: $0 \le A_i\bar{x} - b_i + \varepsilon\rho + \frac{\rho\ln(n)}{\varepsilon T}$

נבחר $T = \left\lceil \frac{4\rho^2}{\delta^2}\ln(m) \right\rceil$ ו-$\varepsilon = \frac{\delta}{2\rho}$ ואז נקבל ש-$\varepsilon\rho = \frac{\delta}{2}$ וגם $\frac{\rho\ln(n)}{\varepsilon T} = \frac{\delta}{2}$

ואז בסה"כ: $0 \le A_i\bar{x} - b_i + \delta$, כלומר: $A_i\bar{x} \ge b_i - \delta$ כנדרש.

*אם נריץ מספיק איטרציות, גם אם ה-x^t הוא לא מספיק טוב, אז הממוצע כן יהיה טוב.

למה קיים אלגוריתם O עבור התכנית הליניארית: $\min \sum_{v\in V} w_v x_v$?

$$\text{s.t. } \forall (u,v)\in E \quad x_u+x_v \ge 1$$
$$x\ge 0$$

נתונים לנו ערכים $p_{uv}\ge 0$ עבור $\{u,v\}\in E$ שמקיימים $p=\sum_{\{u,v\}\in E} p_{uv} \le 1$

צריך למצוא $X: V\to[0,1]$ עבורו מתקיים:

$$\sum_{\{u,v\}\in E} p_{uv}(x_u+x_v) - (1-p)\sum_{v\in V} w_v x_v \ge p-(1-p)\beta$$

או להוכיח שאין X כזה.

נסמן $q_{uv}=\frac{p_{uv}}{1-p}$. כלומר, צריך להוכיח:

$$\sum_{v\in V}\Big(w_v - \sum_{u\mid\{u,v\}\in E} q_{uv}\Big)x_v \le \beta - \sum_{\{u,v\}\in E} q_{uv}$$

6.6.21 יום ראשון

מקרא:
הוכחה -
דוגמה -
משפט -
טענה -
הגדרה -

אלגוריתמים
שבוע 11 - הרצאה 21
אלגוריתמים הסתברותיים

נזכר בבעיה מהשיעור הקודם:

כיסוי בצמתים
$$\begin{cases} \min \sum_{v\in V} w_v x_v \\ s.t\ \forall \{u,v\}\in E\ \ x_u+x_v\geq 1 \\ x\geq 0 \end{cases}$$

מה אומר לחשב האורקל O שאנחנו צריכים כדי לפתור את התכנית על באופן מקורב?

$$\forall\{u,v\}\in E\ \ x_u+x_v\geq 1 \qquad p_{uv}\geq 0$$

המשקל שניתן לאילוץ

$$-\sum_{v\in V} w_v x_v \geq -\beta \qquad p\geq 0$$

$$(1-p)+\sum_{\{u,v\}\in E} p_{uv}=1$$

$$\sum_{\{u,v\}\in E} p_{uv}(x_u+x_v) - p\sum_{v\in V} w_v x_v \geq \sum_{\{u,v\}\in E} p_{uv} - (1-p)\beta$$

נניח ש- $(1-p)\neq 0$ ונגדיר: $q_{uv}=\dfrac{p_{uv}}{1-p}$

(אם $1-p=0$ הבעיה טריוויאלית)

$$\sum_{\{u,v\}\in E} q_{uv}(x_u+x_v) - \sum_{v\in V} w_v x_v \geq \sum_{\{u,v\}\in E} q_{uv} - \beta$$

המקדם של x_v הוא: $\sum_{u\mid\{u,v\}\in E} q_{uv}$

$$\sum_{v\in V}\Big(\sum_{u\mid\{u,v\}\in E} q_{uv} - w_v\Big)x_v \geq \sum_{u\mid\{u,v\}\in E} q_{uv} - \beta$$

האורקל O צריך למצוא X שמקיימות הדרישות האלו $(X_v\geq 0)$ או להוכיח שאין X כזה.

ההשמה הבאה אופטימלית במובן הזה: אם קיים פתרון x עבורו $x_v \in [0,1]$ לכל $v \in V$:

אם $\sum_{u \mid \{u,v\} \in E} q_{uv} - w_v \leq 0$: נקבע $x_v = 0$

אחרת: נקבע $x_v = 1$

אם ההצבה מקיימת את אי-השוויון הנ"ל, סיימנו.

אחרת, אין הצבה של ערכים x עבורם $x_v \in [0,1]$ לכל $v \in V$ שמקיימת את אי השוויון.

אלגוריתמים הסתברותיים

ישנן בעיות רבות שאיננו יודעים לפתור באופן דטרמיניסטי, מתוך אלו - יש מעט כאלו שניתן לפתור באמצעות אלגוריתם הסתברותי.

* אלגוריתם הסתברותי עובד טוב כאשר ישנו אחוז מספיק טוב (גודל קבוע) של פתרונות נכונים שניתן למצוא מתוכו.

אנחנו נראה דוגמאות לאלג' הסתברותיים שלחלקם יש פתרון דטרמיניסטי, אבל אולי יותר יעלות בחלק מהמקרים.

בעיית חתך גדול ביותר Max-Cut

נתון גרף לא מכוון $G=(V,E)$

רוצים למצוא $F \subseteq E$ עם מספר קשתות מירבי.

__תזכורת:__ F הוא קבוצת הקשתות בין שני הצדדים של חלוקה כלשהי של V לשתי קבוצות $S, V/S = \phi$.

אלג' הסתברותי פשוט לקירוב הבעיה:

שלב 1: נבחר קשת כלשהי, $\{u,v\}\in E$ ונשים את u ו-v בצדדים שונים של החתך.

שלב 2: לכל $w\in V/\{u,v\}$ נגריל צד באופן בלתי תלוי בהגרלות אחרות, ובהתפלגות אחידה.

מספר הטלות המטבע של האלגוריתם (ההגרלות) הוא $|V|-2$.
מרחב המדגם יהיה $2^{|V|-2}$, אקספוננציאלי בגודל הקלט.

משפט: יהי F החתך שנוצר ע"י האלגוריתם. אזי: $E[|F|] > \frac{|E|}{2}$

הוכחה: עבור קשת $\{u,v\}\in E$ נסמן ב-C_{xy} את משתנה האינדיקטור למאורע $\{x,y\}\in F$ (האם הצלע בחתך או לא)

מתקיים:

$$E[|F|] = \sum_{\{x,y\}\in E} Pr[C_{xy}=1] =$$

(כי $|F| = \sum_{\{x,y\}\in E} C_{xy}$ ו- $E[C_{xy}] = Pr[C_{xy}=1]$)

ובנוסף:

$$Pr[C_{xy}=1] = Pr\left[\begin{matrix}\text{x בצד של u} \\ \text{y-ו בצד של v}\end{matrix} \vee \begin{matrix}\text{x בצד של v} \\ \text{y-ו בצד u}\end{matrix}\right] = \frac{1}{2}$$

ולכן: $\frac{|E|}{2} < \frac{|E|-1}{2} + 1 = E[|F|]$ כנדרש.

הצלע $\{u,v\}$ בטוח בחתך

יום שלישי 8.6.21

מקרא:
דוגמה - 🔵 הוכחה - 🔴
טענה - 🟠 משפט - 🟢
הגדרה - ⚪

אלגוריתמים
שבוע 11 - הרצאה 22
אלגוריתמים הסתברותיים

מסקנה: $E[|F|]$ הוא קירוב בפקטור 2 לגודל של חתך מקסימום.

הוכחה: חתך מקסימום מכיל לכל היותר את כל הקשתות.

ננסה לחשב את ההסתברות בצורה יותר מדויקת:

כל קשת שמצב הראשונה נחתכת בהסתברות של לפחות חצי.

הקשתות שלא נחתכות

$$E[|F|] \overset{\uparrow}{=} \frac{|E|-1}{2}+1 = \frac{|E|}{2}+\frac{1}{2} \Longrightarrow E[|E\setminus F|] \overset{\nearrow}{=} \frac{|E|}{2}-\frac{1}{2}$$

מס' שלם
מס' של צלעות

$$Pr\left[|F|<\frac{|E|}{2}\right] = Pr\left[|F|\le\frac{|E|}{2}-1\right] = Pr\left[|E\setminus F|\ge \underbrace{\frac{|E|}{2}+1}_{E[|F|]}\right]$$

נשתמש באי"ש מרקוב:

יהי X מ"מ ממשי שמקבל רק ערכים אי שליליים.

נסמן ב-μ את התוחלת של X, ונניח ש-$\mu>0$. אז לכל $\alpha\ge 1$:

$$Pr[X\ge\alpha\mu]\le\frac{1}{\alpha}$$

הוכחה: של אי"ש מרקוב

$$\mu = E[X] \overset{\nearrow}{\ge} Pr[X<\alpha\mu]\cdot 0 + Pr[X\ge\alpha\mu]\cdot\alpha\mu$$

$$E[X] = \int_0^\infty D(x)\,x\,dx \ge \underbrace{\int_0^{\alpha\mu} D(x)\cdot 0\,dx}_{Pr[X<\alpha\mu]\cdot 0} + \underbrace{\int_{\alpha\mu}^{\infty} D(x)\cdot\alpha\mu\,dx}_{Pr[X\ge\alpha\mu]\cdot\alpha\mu}$$

נחזור למקרה שלנו: $\mu = \frac{|E|}{2} - \frac{1}{2}$, $\alpha\mu = \frac{|E|}{2}+1$

$$\alpha = \frac{(|E|+2)/2}{(|E|-1)/2} = \frac{|E|+2}{|E|-1} = 1+\frac{3}{|E|-1}$$

נקבל

$$\Pr\left[|F| < \frac{|E|}{2}\right] = \Pr\left[|E\setminus F| \ge \frac{|E|}{2}+1\right] \le$$

$$\le \frac{|E|-1}{|E|+2} = 1-\frac{3}{|E|+2}$$

כלומר, בהסתברות של לפחות $\frac{3}{|E|+2}$ האלגוריתם מחשב חתך F שגודלו לפחות $\frac{|E|}{2}$.

אם נחזור על האלגוריתם באופן בלתי תלוי $\frac{|E|+2}{3}$ פעמים, וניקח את התוצאה הטובה ביותר F_{max}, אזי:

$$\Pr\left[F_{max} < \frac{|E|}{2}\right] \le \left(1-\frac{3}{|E|+2}\right)^{\frac{|E|+2}{3}} \overset{(*)}{\le} e^{-1} < \frac{1}{2}$$

$$\forall \varepsilon \in (0,1) \quad (1-\varepsilon)^{\frac{1}{\varepsilon}} \le e^{-1} \quad (*)$$

הצלחה: להשיג חתך בגודל של לפחות $\frac{|E|}{2}$

כלומר, הסתברות ההצלחה כעת היא לפחות $1-e^{-1}$, כלומר גדולה מחצי.
אם נחזור על האלג' $k\cdot\frac{|E|+2}{3}$ פעמים, אזי נקבל הסתברות כישלון שהיא לכל היותר e^{-k}.

* רצינו להדגים ניתוח של אלגוריתמים הסתברותיים, לכן לקחנו את max-cut.
קיימים אלגוריתמים דטרמיניסטיים פשוטים למציאת 2-קירוב ל-max-cut.

הערה: אותו רעיון מאפשר פתרון של עוד בעיות, למשל הבעיה הבאה:

בעיית Max-2Lin2

נתון אוסף משוואות לינאריות מעל $\mathbb{Z}_2$ (דוגמה למשוואה כזו $x_2 \oplus x_3 \oplus x_4 \oplus x_{30} = 0$)
רוצים למצוא הצבה של ערכי 0,1 למשתנים עבורה מס' המשוואות שמתקיימות מקסימלי.

זו הכללה של max-cut:

נגדיר משתנים x_v לכל צומת $v \in V$
לכל קשת $\{u,v\} \in E$ נוסיף משוואה לינארית $x_v \oplus x_u = 1$
המשוואה מתקיימת אמ"מ $x_u \neq x_v$. לכן, פתרון הוא חתך שבו $S = \{u \in V \mid x_u = 0\}$
ומס' המשוואות שמתקיימות הוא בדיוק מספר הקשתות שנחתכות.

במקרה הכללי, אם נגריל את המשתנים בהתפלגות אחידה ובאופן ב"ת, מה ההסתברות שמשוואה מתקיימת?
- נשים לב שבכל הצבה בשלושת המשתנים הראשונים ולכל הצבה ב-x_{30} יש בדיוק
  בחירה אחת לקיום המשוואה: $x_1 \oplus x_3 \oplus x_4 \oplus x_{30} = 0$
  לכן ההסתברות לקיום המשוואה היא $\frac{1}{2}$.
ומכאן תוחלת מס' המשוואות המקיימות הוא חצי מכל המשוואות.

עבור בעיה יותר מורכבת:

בעיית חתך מינימום גלובלי Min-Cut

נתון גרף סופי לא מכוון $G=(V,E)$

רוצים למצוא חתך $F\subseteq E$ שגודלו <u>מינימלי</u>

*אפשר בקלות לפתור את הבעיה ע"י $|V|-1$ חישובים של זרימת מקסימום.
(נבחר איזושהי צומת וננסה את כל יתר הצמתים בתור הצומת בצד השני)

אלגוריתם הסתברותי פשוט לבעיית Min-Cut

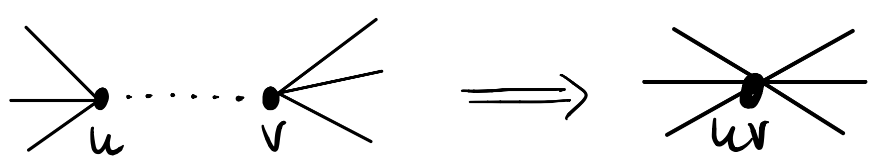
נגדיר לשם כך פעולה של <u>כיווץ קשת</u>:

תהי $e=\{u,v\}\in E$. כיווץ של e מייצר גרף חדש $G/e=(V',E')$ כאשר:

* $V'=V\setminus\{u,v\}\cup\{uv\}$ - החלפנו את u,v בקודקוד שנקרא uv.
* $E'=\{f\in E \mid f\cap\{u,v\}=\emptyset\}\cup\{\{uv,w\}\mid(\{u,w\}\in E\vee\{v,w\}\in E)\wedge w\notin\{u,v\}\}$

- כלומר הורדנו את הקשתות עם u או v וחיברנו את שכניהם הקודמים בקשתות חדשות עם הקודקוד החדש uv.

<u>המחשה של כיווץ:</u>



כה יכול להיווצר קשתות מקבילות (כלומר מחוברת גם ל-u וגם ל-v בגרף המקורי).

האלגוריתם:

* כל עוד יש ב-G יותר משני קודקודים:
* נבחר קשת e בהתפלגות אחידה ונחליף את G ב-G/e.

בסיום, יש שני צמתים וכל אחד מהם מייצג קבוצה לא ריקה של צמתים בגרף הקלט.
החלוקה של הגרף המקורי בקלט לשתי קבוצות לא ריקות לפי התוצאה מגדירה חתך.
אוסף הקשתות המקבילות בין שני הצמתים בתוצאה בסוף, זה החתך.

האלגוריתם מצליח אם״ם החתך שקיבלנו הוא חתך מינימלי.

טענת עזר: אם $F \subseteq E$ הוא חתך מינימום ב-G, אז $|E(G)| \geq \frac{|V| \cdot |F|}{2}$

הוכחה: אם F חתך מינימום אז הדרגה המינימלית של צומת ב-G הוא לפחות $|F|$. כלומר, $\min_v d(v) \geq |F|$.
סכום הדרגות בגרף שווה ל-$2|E(G)|$ והוא גדול או שווה ל-$|V| \cdot |F|$.

מסקנה: אחרי הכיווץ הראשון נקבל ש: $Pr[F \subseteq E(G/e)] \geq 1 - \frac{2}{|V|}$

הוכחה למסקנה:

גדלי הקבוצות

$$Pr[F \subseteq E(G/e)] = Pr[e \notin F] = \frac{|E(G) \setminus F|}{|E(G)|} \geq \frac{|E(G)| - |F|}{|E(G)|} = 1 - \frac{|F|}{|E(G)|} \geq$$

$$1 - \frac{|F|}{|V| \cdot |F| / 2} = 1 - \frac{2}{|V|}$$

נסמן ב-F את התוצאה בסוף ונסמן ב-F_{min} איזשהו חתך מינימום.

משפט: $Pr[F = F_{min}] \geq \prod_{k=3}^{|V|} \left(1 - \frac{2}{k}\right)$

יום ראשון 13.6.21

מקרא:
הוכחה -
דוגמה -
משפט -
טענה -
הגדרה -

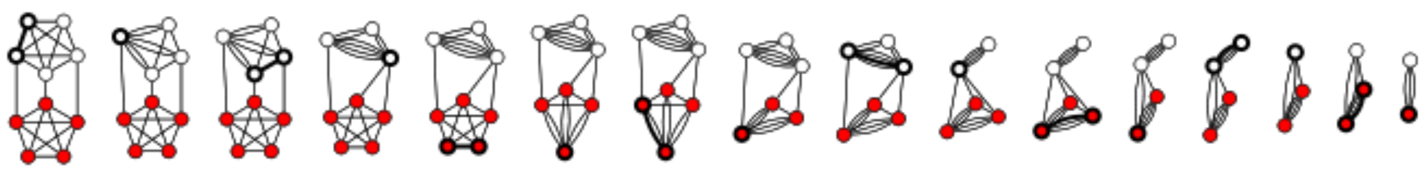
אלגוריתמים
שבוע 12 - הרצאה 23
אלגוריתמים הסתברותיים

האלגוריתם של Karger:

* כל עוד יש ב-G יותר משני קודקודים:
* נבחר קשת e בהתפלגות אחידה ונחליף את G ב-G/e.

תשובת האלג' - הקשתות המקבילות בין שני הקודקודים הנותרים (שכן ירושה מהגרף המקורי)

דוגמת הרצה:



הגדרנו את G/e להיות הגרף לאחר כיווץ הקשת e.

ואת F_{min} - חתך מינימום ספציפי

והראנו כי: אחרי הכיווץ הראשון נקבל ש: $Pr[F \subseteq E(G/e)] \geq 1-\frac{2}{|V|}$

משפט: תהי $F \subseteq E(G)$ התשובה של האלג', אז: $Pr[F=F_{min}] \geq \prod_{K=3}^{|V|}\left(1-\frac{2}{K}\right)$

הוכחה: נסמן $|V(G)|=n$ ונוכיח באינדוקציה על n.

בסיס האינדוקציה: $n=2$ ובמקרה כזה הטענה טריוויאלית (קשת אחת).

נניח שהטענה נכונה לכל גרף בעל $n-1$ קודקודים ונוכיח עבור G עם n קודקודים.

צעד האינדוקציה: תהי e הקשת המקרית שהאלג' בחר.

$$Pr[F=F_{min}] = Pr_G[F_{min} \subseteq E(G/e)] \cdot Pr_{G/e}[F=F_{min} \mid F_{min} \subseteq E(G/e)]$$

$$\geq \underbrace{\left(1-\frac{2}{n}\right)}_{\text{טענה משלב הקודם}} \cdot \underbrace{\prod_{k=3}^{n-1}\left(1-\frac{2}{k}\right)}_{*} = \prod_{k=3}^{n}\left(1-\frac{2}{k}\right)$$

$*$ - עפ"י הנחת האינדוקציה על G/e שהוא גרף עם $n-1$ קודקודים.
אם F_{min} שרד, אז הוא חתך מינימום ב-G/e.

מסקנה: $Pr[F=F_{min}] \geq \frac{1}{\binom{n}{2}}$

הוכחה:

$$\prod_{k=3}^{n}\left(1-\frac{2}{k}\right) = \prod_{k=3}^{n}\left(\frac{k-2}{k}\right) = \frac{1\cdot 2\cdot 3\cdot \ldots \cdot (n-2)}{3\cdot 4\cdot 5\cdot \ldots \cdot n} = \frac{2}{(n-1)\cdot n} = \frac{1}{\binom{n}{2}}$$

$$\binom{n}{2} = \frac{n(n-1)}{2} \implies Pr[F=F_{min}] \geq \frac{2}{n(n-1)}$$

מסקנה: בכל גרף G על n קודקודים מספר חתכי המינימום הוא לכל היותר $\binom{n}{2}$.

מסקנה: נשים לב כי: $\frac{1}{n^2} \geq \frac{2}{n(n-1)}$ (לנוחות). כלומר, הסיכוי שהאלגוריתם "יכשל" הוא לכל היותר $1-\frac{1}{n^2}$.

אם נריץ את האלג' באופן בלתי תלוי N פעמים ונקח את החתך הקטן ביותר מבין N החתכים שקיבלנו, סיכויי הכשלון הם לכל היותר: $\left(1-\frac{1}{n^2}\right)^N \leq e^{-N/n^2}$

כלומר, אחרי n^2 נסיונות, מצליחים בהסתברות של לפחות $1-e^{-1}$.

הסיבוכיות: $O(mn^2)$ כאשר m הוא מספר הקשתות ב-G.

פולינומים מרובי משתנים

נתון שדה $\mathbb{F}$ ופולינום p מעל $\mathbb{F}$. נתחיל עם פולינום p במשתנה אחד, $p\in\mathbb{F}[X]$.

כזה פולינום במשתנה אחד מעל לשדה $\mathbb{F}$ שדרגתו d: $p=\sum_{i=0}^{d} a_i x^i$ (*)

שאלה: האם p הוא זהותית 0?

כלומר, אם הצבה של איבר $a\in\mathbb{F}$ ב-x מקבלים תמיד $p=0$.

תשובה: אם הפולינום מוצג כמו ב-(*), התשובה טריוויאלית. נבדוק אם כל המקדמים הם 0. אם הפולינום מוצג כך: $p=(a_1x+b_1)(a_2x+b_2)\cdots(a_dx+b_d)$

כה עדיין טריוויאלי אבל פחות, כי נדרשת פתיחת הסוגריים.

ובאופן כללי, אם p פולינום עם משתנה אחד, הבעיה קלה.

מה קורה אם p הוא פולינום במשתנים $p\in\mathbb{F}[X_1,X_2,\dots,X_n]$?

אבל p לא רשום מפורשות כסכום של מונומים:

$$\sum_{\alpha_1,\dots,\alpha_n} a_{\alpha_1,\dots,\alpha_n} X_1^{\alpha_1}X_2^{\alpha_2}X_3^{\alpha_3}\cdot\ldots\cdot X_n^{\alpha_n}$$

נניח שהפולינום נתון באופן לא מפורש ככה. לדוגמה:

$$\prod_i \left(c_0^i+c_1^iX_1+c_2^i\cdot X_2+\dots+c_n^i\cdot X_n\right)$$

15.6.21 יום שלישי

מקרא:
הוכחה - דוגמה - משפט - טענה - הגדרה

אלגוריתמים
שבוע 12 - הרצאה 24
אלגוריתמים הסתברותיים

בדיקת זהות פולינומים:

נתון שדה F ופולינום $p \in F[X_1,..,X_n]$.

הנחה: הפולינום לא בהכרח מוצג בהצגה מפורשת כסכום מונומים.
$\left(\sum_{\alpha_1,..,\alpha_n} a_{\alpha_1,..,\alpha_n} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3} \cdot \ldots \cdot X_n^{\alpha_n} \right)$ הצגה כסכום מונומים

בפועל, נניח שלכל הצבה של ערכים מ-F למשתנים $X_1,..,X_n$ אפשר לחשב את ערך הפולינום בנקודה זאת.

הגדרה: p הוא זהותית 0 אמ"ם בהצגה של p כסכום מונומים, כל המקדמים $a_{\alpha_1,..,\alpha_n}$ הם 0.

שאלה: האם p הוא זהותית 0?

הנחה: ידועה המעלה המירבית של הקלט, d. $\max\{\alpha_1+\cdots+\alpha_n \mid a_{\alpha_1,..,\alpha_n} \neq 0\}$

דוגמה לפולינום שייקח זמן אקספוננציאלי על מנת להמיר אותו לסכום של מונומים:
$$\prod_{a_0,a_1,..,a_n \in \mathbb{N}} (a_0 + a_1 X_1 + a_2 \cdot X_2 + \ldots + a_n \cdot X_n)$$

משפט Schwartz-Zippel

יהי פולינום $P \in F[X_1,..,X_n]$ שאינו זהותית 0.

תהי A קבוצה סופית של איברי F.

נגריל הצבה $X_i = a_i$ לכל $i=1,..,n$.

כאשר ה- a_iים כולם תלויים הדדית וכל אחד מתפלג אחיד ב-A.

אזי: $P[P(a_1,..,a_n)=0] \le \frac{\deg(P)}{|A|}$ כאשר $\deg P$ זה המעלה של P.

אינטואיציה:

עבור פולינום שהוא לא זהותית 0, אם נבחר קבוצה A מספיק גדולה ($|A| >> \deg(P)$) ונגריל הצבה בצורה הנ"ל, הסיכוי שנקבל 0 יחסית קטן

וכאשר נתגיר שפולינום הוא לא זהותית 0, התשובה תהיה נכונה תמיד. אם הפולינום הוא זהותית 0 אז אנו טועים ולהחזיר שהוא אינו.

הוכחה: באינדוקציה על n.

בסיס האינדוקציה: $n=1$. במקרה זה הטענה נכונה כי מספר השורשים של פולינום במשתנה אחד ממעלה d שאיננו זהותית 0 הוא לכל היותר d

הנחת האינדוקציה: נניח שהטענה נכונה עבור $n-1$ ונוכיח עבור n.

צעד האינדוקציה: נרשום את הפולינום בצורה הבאה:

$$P(X_1,..,X_n) = \sum_{i=0}^{d} X_1^i P_i(X_2,..,X_n)$$

P אינו זהותית 0 ולכן קיים i עבורו P_i אינו זהותית 0.

נבחר i מקסימלי כזה. המעלה של P_i היא לכל היותר $d-i$.

לפי הנחת האינדוקציה: $\mathbb{P}[p(a_1,..,a_n)=0]\le \frac{d-i}{|A|}$

אם $p_i(a_1,..,a_n)\neq 0$ אז $\sum_{j=0}^{d} x_1^j p_j(a_2,..,a_n)$ הוא פולינום במשתנה אחד

שאינו זהותית 0 (כי המקדם של x_1^i אינו 0), ומעלתו הוא i.

לכן,

$$\mathbb{P}\left[\sum_{j=0}^{d} a_1^j p_j(a_2,..,a_n)=0 \mid p_i(a_2,..,a_n)\neq 0\right]\le \frac{i}{|A|}$$

נסמן ב- E_1 את המאורע: $p(a_1,..,a_n)=0$

ונסמן ב- E_2 את המאורע: $p_i(a_2,..,a_n)=0$

ומכאן נקבל:

$$\mathbb{P}[E_1]=\mathbb{P}[E_1\wedge E_2]+\mathbb{P}[E_1\wedge \bar{E_2}]=\mathbb{P}[E_1|E_2]\cdot\mathbb{P}[E_2]+\mathbb{P}[E_1|\bar{E_2}]\cdot\mathbb{P}[\bar{E_2}]\le$$

$$\le \mathbb{P}[E_2]+\mathbb{P}[E_1|E_2]\le \frac{d-i}{|A|}+\frac{i}{|A|}=\frac{d}{|A|}$$

$\square$

<u>מסקנה</u>: אם F שדה מספיק גדול, אזי קיים אלגוריתם הסתברותי יעיל עבור <u>הבעיה הבאה</u>: נתון פולינום רב משתנים p ממעלה מירבית d, ב"ע, שמאפשר חישוב יעיל של ערכו בהינתן הצבה למשתנים.

<u>הפלט</u>: לזהות אם p הוא זהותית 0.

<u>הוכחה</u>: נבחר מ- F קבוצה A שגודלה $|A|=2d$ (כלומר, נדרוש שב- F יהיו לפחות $2d$ איברים). נגריל הצבה מקרית מ- A ונציב ב- p.

נחזור על הפעולה הנ"ל M פעמים. אם באחת ההצבות קיבלנו ערך שונה מ- 0, נחזיר ש- p <u>איננו</u> זהותית 0. אחרת, נחזיר ש- p זהותית 0.

במקרה הראשון לא טעינו.

במקרה השני, אם p אינו זהותית 0 אזי הסיכוי שבכל M הניסיונות יחזירו ערך 0 הוא לכל היותר: $\left(\frac{d}{2d}\right)^M=2^{-M}$.

הסיבוכיות: צריך להגריל M פעמים ערכים $a_1,\dots,a_n$ ולהציב את הערכים האלו ב-p.

זמן הריצה: M (סיבוכיות ההגרלה + סיבוכיות ההצבה)

במסקנה/הוכחה

שימוש: נתון גרף דו-צדדי $G=(V_L,V_R,E)$ שמקיים $|V_L|=|V_R|$. אנחנו רוצים לבדוק האם יש ב-G שידוך מושלם.

נגדיר מטריצה ריבועית M. השורות ממוספרות בקודקודי V_L והעמודות בקודקודי V_R:

$$M_{i,j}=\begin{cases} X_{i,j} & \{i,j\}\in E \\ 0 & \text{else}\end{cases}$$

המטריצה של Edmonds
(חברנו מ-EK 🙂)

הדטרמיננטה $\det(M)$ של M היא פולינום ב-2 משתנים $\{X_{ij} \mid \{i,j\}\in E\}$:

$$\sum_{\sigma: V_L \xrightarrow{1:1} V_R} (-1)^{\sigma}\cdot \prod_{i\in V_L} M_{i\sigma(i)}$$

הדבר הזה הוא זהותית 0 כאשר אין שידוך מושלם.

σ היא פרמוטציה של שידוך

1:1 פונ' חח"ע ועל

אם קיים שידוך מושלם $\sigma: V_L \xrightarrow{1:1} V_R$ אזי $\prod_{i\in V_L} M_{i\sigma(i)} = \prod_{i\in V_L} X_{i\sigma(i)}$
והמקדם של המונום הזה הוא $+1$ או -1.

לכן הפולינום $\det(M)$ הוא זהותית 0.

אם נציב ערכים למשתנים: $X_{ij}=a_{ij}$ $\forall\{i,j\}\in E$ אזי $M(\{a_{ij}\})$ היא קלה לחישוב והיא מטריצה נומרית ואזי $\det(M(\{a_{ij}\}))$ ניתנת לחישוב בזמן פולינומי.

מוטיבציה: באמצעות חישוב דטרמיננטה כך ניתן לבדוק האם יש שידוך מושלם.

אם $\det(M)=0$ - נסיק שאין שידוך מושלם, אך זה לא בהכרח נכון.

ואם $\det(M)\neq 0$ - יש שידוך מושלם.

*החל מיום שלישי כל ההרצאות והדיון חברה.

יום ראשון 20.6.21

מקרא:
דוגמה - ● הוכחה - ●
טענה - ● משפט - ●
הגדרה - ●

אלגוריתמים
שבוע 13 - הרצאה 25
אלגוריתמים הסתברותיים

* הטכניקה נקראת "טביעת אצבע".

זיהוי תבניות

נתון טקסט T - רצף של אותיות מתוך א"ב Σ, $n=|T|, d=|\Sigma|$.
נתונה גם תבנית P - רצף של אותיות מתוך Σ, $m=|P|$, נניח ש- $m<<n$. } קלט
/במצב זה הבעיה תהיה יותר "מעניינת"
רוצים למצוא את כל המופעים של P מתוך T. } פלט

אלגוריתם נאיבי:

1. עבור כל המקומות ב-T שבהם P יכולה להתחיל: $i=1,2,...,n-m+1$
2. במקום ה-i נשווה בין P לבין $T[i,...,i+m-1]$ ← קטע הטקסט בין המקום ה-i למקום ה-$i+m-1$
(אפשר להניח בה"כ $\Sigma=\{0,...,d-1\}$)

סיבוכיות הזמן: $O(n\cdot m)$ פעולות של השוואה של אותיות N- Σ או גישה לאיברים של T או P לפי אינדקס או קידום של אינדקס.
אות ניתנת לייצוג ע"י $O(\log_2 d)$ ביטים ואינדקס ניתן לייצוג ע"י $O(\log_2 n)$ ביטים.

סיבוכיות המקום: מלבד הקלט P,T והפלט צריך $O(1)$ תאי זיכרון שמחזיקים כל אחד אינדקס (סה"כ שניים).

נראה כעת אלגוריתם הסתברותי לבעיה:

האלגוריתם של Karp+Rabin

ניתן להתייחס ל-p וגם ל-$T[i,..,i+m-1]$ כאל מספר שרשום בבסיס d.

$$p = d^{m-1}\cdot p[1] + d^{m-2}\cdot p[2] + \dots + d^{0}\cdot p[m]$$

$$t_i = d^{m-1}\cdot T[1] + d^{m-2}\cdot T[2] + \dots + d^{0}\cdot T[i+m-1]$$

מכאן נובע כי ש:

$$t_i = p \iff T[i,..,i+m-1]$$

$$t_{i+1} = d t_i - d^m T[i] + T[i+m]$$

הפכנו את הבעיה של השוואות מחרוזות להשוואה של מספרים

בנתיים לא שיפרנו דבר כי אנחנו עובדים עם מספרים גדולים. $0 \le p, t_i < d^m$

המספרים האלו עלולים לדרוש $m\log_2 d$ ביטים כדי לייצג אותם.

סה"כ נקבל $O(nm\log_2 d)$ פעולות על ביטים כדי לבצע את החיפוש.

ניתן להשמיט בתנאים מסוימים

נבחר קבוצה גדולה Q של מספרים ראשוניים, נבחר $q \in Q$ באופן מקרי בהתפלגות אחידה, ונבצע את כל החישובים מודולו q.

נסמן $q_{max} = \max_{q\in Q}$. אם $\log_2 q_{max}$ קטן יחסית לאורך m ($q_{max} << 2^m$), החישובים האריתמטיים יעילים הרבה יותר.

כמובן, אם $t_i \not\equiv p \bmod q$ אז $T[i,..,i+m-1] \neq p$.

<u>מה לגבי $t_i \equiv p \bmod q$?</u>

- פה לא מובטח לנו שהתבנית p תואמת לטקסט $T[i,...,i+m-1]$. צריך לבדוק.

מספרם, אם p מופיעה ב-T, S פעמים, נשלם על הבדיקות $O(S\cdot T)$ פעולות (במקומות שבהן באמת יש מחרוזת).

מה לגבי מקומות שבהם התבנית שונה מהטקסט?

אם $t_i \neq p$, סביר שלא לכל q, נקבל $t_i \equiv p \bmod q$?

מתקיים אם q מחלק ללא שארית את $|t_i - p|$.

כלומר, q הוא גורם ראשוני של $|t_i - p|$.

כמה גורמים ראשוניים כאלו יכולים להיות? $0 \le \underbrace{|t_i - p|}_{\text{מכפלת הגורמים הראשוניים. וכל גורם } \geq 2} < d^m$

לכן, מספר הגורמים הראשוניים השונים כזה מכה קטן ממש מ-$m \log_2 d$.

לכן,

$$P[t_i \equiv p \bmod q \mid t_i \neq p] < \frac{m \log d}{|Q|}$$

כלומר, תוחלת מס' המקומות i שנבדוק לשווא היא קטנה מ-$\frac{n \cdot m \cdot \log_2 d}{|Q|}$.

כלומר, תוחלת מספר הפעולות שנבצע היא:

$$O(\underbrace{m+n}_{\text{חישוב } p \text{ ו-} t_i} + m(\underbrace{S}_{\text{מס' ההופעות של } p} + \underbrace{\frac{nm\log_2 d}{|Q|}}_{\text{מקומות שבהם לא נמצאת } p}))$$

פעולות בדיקה

נרצה $|Q| >> nm \log_2 d$.

רוצים מצד אחד הרבה ראשוניים ומצד שני שיהיו מיוצגים ע"י מעט ביטים.

כדי לבחור את Q אופשר להשתמש בצפיפות המספרים הראשוניים:

משפט:

מספר המספרים הראשוניים שקטנים מ-X הוא $\frac{X}{\ln(X)}(1 \pm o(1))$