נושאי השיעורים הקרובים

אלגוריתמים
24/3/2008, ב
18:10 (1)
אדם מתן
adam@matan.name

1. סיום לרימה: הוכחת זמן ריצה של Edmonds-Karp
2. התחלת DFT, FFT
3. קריפטוגרפיה (הגדרה) - (נושאי מגניב לאללה, RSA, מפתח ציבורי ופרטי וכו' יאללה.

האלגוריתם של Edmonds-Karp בוחר בכל איטרציה מסילת הרחבה מינימלית. נראה כי זמן הריצה הוא $O(|E|^2 \cdot |V|)$.

כאשר מספר האיטרציות: $O(|E| \cdot |V|)$ וכל איטרציה מוצאת מסילת הרחבה בחיפוש רוחב ב $O(|E|)$ צעדים.

נשאר להוכיח 2 למות שמגדירות את החסם על מספר האיטרציות.

למה 2

הגדרה: צלע בעלת קיבול שיורי מינימלי במסילת הרחבה נקראת צלע קריטית.

הלמה אומרת שכל צלע $u,v \in E$ יכולה לשמש צלע קריטית לכל היותר $O(|V|)$ פעמים. לכן מספר האיטרציות חסום ע"י $O(|E| \cdot |V|)$.

למה 1

הגדרה: לכל $v \in V$ נגדיר $\delta_i(v)$ המרחק של v מהקודקוד המקור ברשת השיורית G_{F_i}.

אזי $\delta_{i+1}(v) \geq \delta_i(v)$ לכל i ולכל v.

24/3/2008, ב

18:22 (2)

אדם מתן
adam@matan.name

הוכחת למה 1:

נניח בשלילה כי קיים i וקיים $v\in V$ כך ש: $\delta_{i+1}(v)<\delta_i(v)$. בה"כ נבחר v להיות הקודקוד הקרוב ביותר ל-s המקיים את זה. נתבונן במסילה מינימלית מ-s ל-v ב $G_{F_{i+1}}$.

מתקיים:

$$\delta_{i+1}(v)=\delta_{i+1}(u)+1$$

וכמו כן:

$$\delta_{i+1}(u)\ge\delta_i(u)$$

לכן:

$$\delta_i(v)>\delta_{i+1}(v)=\delta_{i+1}(u)+1\ge\delta_i(u)+1$$

$$\delta_i(v)>\delta_i(u)+1$$

כי אחרת אפשר היה להגיע ל u, לעשות עוד צעד ולהגיע ל v אבל המרחק ביניהם 1 (אני מקווה שהבנתי את ההסבר נכונה).

לכן הצלע $\overrightarrow{(u,v)} \notin G_{F_i} \iff f_i(u,v)=c(u,v)$

ומצד שני $\overrightarrow{(u,v)} \in G_{F_{i+1}} \iff f_{i+1}(u,v)<c(u,v)$

ולכן מתקיים:

$$\Delta F_{i+1}=f_{i+1}-f_i$$

שלילית בצלע $\overrightarrow{(u,v)}$

אלגוריתמים

24/3/2008, ב

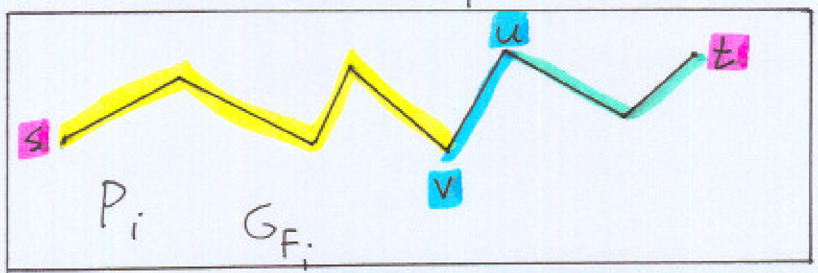
18:32 (3)

אדם מתן

adam@matan.name

פי $\Delta f_{i+1}(v,u)$ ⟸ (v,u) שייכת למסילת ההרחבה

P_i במצב i, ולכן $\delta_i(u)=\delta_i(v)+1$



קיבלנו שני נתונים סותרים:

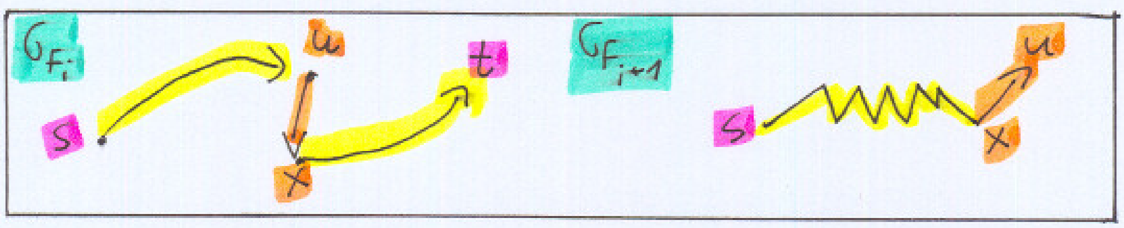
א. $\delta_i(v)\geq\delta(u)+1$

ב. $\delta_i(u)=\delta_i(v)+1$

⟸ סתירה והוכחה ∎.

הוכחת למה 2:

נניח כי צלע (u,v) הינה קריטית בשני מצבים i ו-y, ונראה כי $\delta_y(u)\geq\delta_i(u)+2$. לכן (u,v) צפויה להיות צלע קריטית לכל היותר $O(|V|)$ פעמים.



הערה: מההוכחה של למה 1 נובע, בפרט, כי אם לא ניתן להגיע מ-s ל-u ב-G_{f_i} אז לא ניתן להגיע מ-s ל-u ב-$G_{f_{i+1}}$. ואמנם נניח בשלילה כי כן ניתן להגיע מ-s ל-u במצב $i+1$, ונניח גם כי u הקודקוד הקרוב ביותר ל-s שמקיים זאת.

אלכס כמעט אומר שזו "שאלה טובה למבחן".

אלגוריתמים
24/3/2008, ב
17:08 (4)
אדם מתן
adam@matan.name

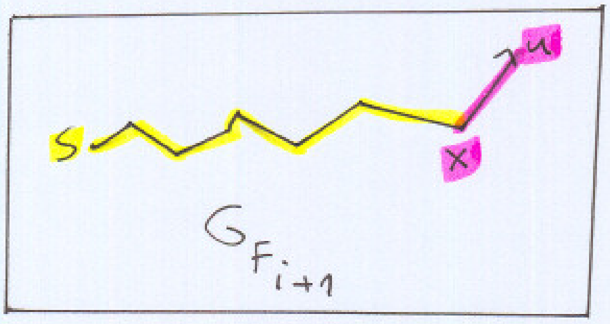
תוספת ללמה 1: אם עבור $u\in V$ $\delta_i(u)=\infty$

(כלומר לא ניתן להגיע מ-s ל-u) אז $\delta_{i+1}(u)=\infty$.

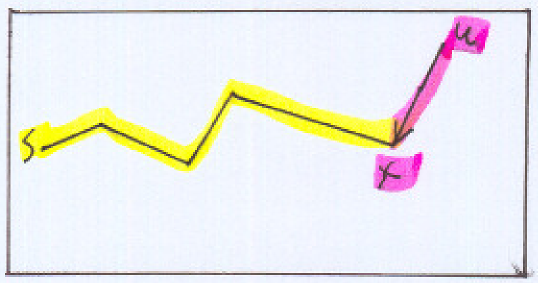
נניח בשלילה: כי $\delta_i(u)=\infty$! $\delta_{i+1}(u)<\infty$, ונניח בה"כ

כי u הוא הקודקוד הקרוב ביותר ל-s בזמן i+1 המקיים

זאת.



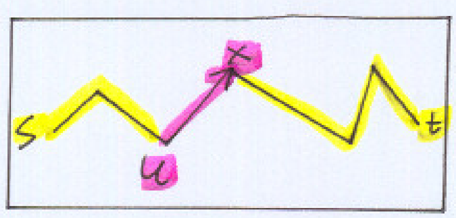
נשים לב כי ניתן להגיע מ-s ל-x בזמן i.



לכן הצלע $\overrightarrow{(x,u)}\notin G_{F_i}$ אבל $\overrightarrow{(x,u)}\in G_{F_{i+1}}$.

כמו קודם, נסיק כי מזרימים זרימה חיובית $\Delta F_{i+1}(u,x)>0$.

ז"א $\overrightarrow{(u,x)}$ שייכת למסלול ההרחבה p.

$\delta_i(u)<\infty \Longleftarrow$ 

הוכחת למה 2:

		f_0
$\delta_0(u)$	(u,v)	
		f_1
$\delta_i(u)$	(u,v)	f_i
		f_{i+1}
$\delta_j(u)$	(u,v)	$f_t=f^*$ אופטימלית

בריצה יש הרבה איטרציות
קיים משתנה להיות
אינסופית.

24/3/2008, ב

19:14 (5)

אדם מתן
adam@matan.name

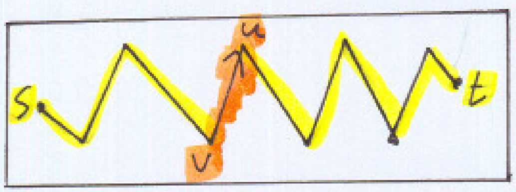
הערה קטנה: התרשים בעמוד הקודם למטה הופיע כבר כמה פעמים, אך לא הבנתי אותו ולכן לא העתקתי. כדאי להביט בסיכומים אחרים.

אם $f(\overrightarrow{u,v})$ הרוויה בזמן i, אז $(\overrightarrow{u,v}) \in G_{f_{i+1}}$, כי בזמן i+1 $c(u,v) = f_{i+1}(u,v)$.

ואם $(\overrightarrow{u,v})$ הרוויה בזמן j, צ"ל $(\overrightarrow{u,v}) \in G_{f_j}$.

צ"ל קיים זמן k $i+1 \le k \le j$ כך ש:

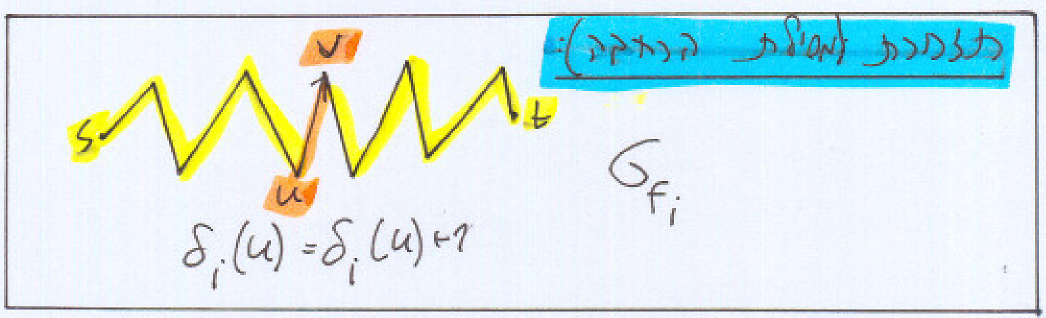
$\Delta f_k(\overrightarrow{v,u}) > 0$



צ"ל לפי למה 1

$\delta_j(u) \ge \delta_k(u) = \delta_k(v) + 1 \ge \delta_i(v) + 1 = \delta_i(u) + 2$

∎



סוף זרימה ברשתות!

אלגוריתמים
24/3/2008, ב
19:28 (6)
אדם מתן
adam@matan.name

FFT & DFT

Discrete Fourier Transform
Fast Fourier Transform

עבודה עם פולינומים:

$$P(x)=\sum_{i=0}^{n-1} a_i x_i$$

$$Q(x)=\sum_{i=0}^{n-1} b_i x_i$$

בהינתן שני פולינומים P,Q, נרצה לחשב את:

(1) החיבור $R=P+Q$ (2) הכפל $R=P\cdot Q$

(3) הצבת ערך (אינטרפולציה): בהינתן x_0, נרצה לחשב $P(x_0)$.

המטרה: יעילות כפונקציה של n (מספר איברי הפולינום)

(1) **חיבור:** ניתן לבצע ב $O(n)$ פעולות:

$$R(x)=(P+Q)(x)=\sum_{i=0}^{n-1}(a_i+b_i)x^i$$

נניח כי שהפולינום מיוצג על ידי סדרת המקדמים שלו:

$$P\longleftrightarrow(a_0 \ldots\ldots a_{n-1})$$

$$Q\longleftrightarrow(b_0 \ldots\ldots b_{n-1})$$

$$P+Q\longleftrightarrow(a_0+b_0, \ldots, a_{n-1}+b_{n-1})$$

אלגוריתמים

24/3/2008, ק

14:35 (ד)

אדם מתן
adam@matan.name

③ **הצבת ערך בפולינום:** נתונה $P \leftrightarrow (a_0 \ldots a_{n-1})$

לביצוע בזמן $O(n)$ באופן הבא: נחשב את:

$1, x_0, x_0^2, \ldots, x_0^{n-1}$ בזמן $O(n)$ ואז

ואז נחשב את

$$P(x_0) = a_0 + a_1 x_0 + \ldots + a_{n-1} x_0^{n-1}$$

זמן $O(n)$

וסה"כ זמן $O(n)$ פעמיים שזה כמובן $O(n)$.

② **כפל:** פעולת הכפל עולה $\Omega(n^2)$ פעולות. לראות כי

$$P = \sum_{i=0}^{n-1} a_i x^i \qquad Q = \sum_{j=0}^{n-1} b_j x^j$$

$$R = P \cdot Q = \sum_{k=0}^{2n-2} c_k x^k$$

לזה כיוון $C_k = \sum_{i=0}^{k} a_i b_{k-i}$ והסיגמאות המקוננות מביאות

וזמן n^2.

דוגמה:

$P = x - 1 \quad (-1, 1, 0)$ — מקדמי x^0, x^1, x^2

$Q = x^2 + x + 1 \quad (1, 1, 1)$

$$P \cdot Q = \sum_{k=0}^{4} c_k x^k = (x-1)(x^2+x+1)$$

(a_1, a_0 מעל $(x-1)$; b_2, b_1, b_0 מעל (x^2+x+1))

כפי שהוגדר:

נחשב את C_2:

$$C_2 = a_1 + b_1 + a_0 \cdot b_2$$

ונציב את ה-C-ים בנוסחאות של $\sum_{k=0}^{4}$.

אלגוריתמים

24/3/2008, ב

19:44 (8)

אדם מתן
adam@matan.name

$$R=(a_{n-1}x^{n-1}+\dots+a_1x+a_0)(b_{n-1}x^{n-1}+\dots+b_1x+b_0)$$

צ״ל החישוב לפי הנוסחה הנ״ל של C_k לוקח $\Omega(k)$ פעולות
וסה״כ מס׳ הפעולות לכפל הוא:

$$\Omega\left(\sum_{k=0}^{n-1} k\right)=\Omega(n^2)$$

לכן כאשר $a_i=0$ עבור $i<0$ או $n\le i$ וכנ״ל b_i
ניתן אלגוריתם לביצוע של כל הפעולות בזמן $O(n\log n)$