

מכרואידיק

הגדרה: זוג סדור (E, I) של קבוצות סופיות שבה
 $I \subseteq 2^E$ נקרא מכרואידיק אם הוא מקיים
שתי תכונות:

(1) אם $A \in I$ ו- $B \subseteq A$ אזי $B \in I$.
(תכונת היררכיה)

(2) אם $A, B \in I$ ו- $|A| < |B|$, אז קיים
 $e \in B \setminus A$ כזה ש- $A \cup \{e\} \in I$.
(תכונת ההרחבה)

$$E = \{1, 2, 3\} \quad I = \{\emptyset, \{1\}, \{2\}, \{3\}\}$$

זה לא מכרואידיק

מכנים את איברי I קבוצות בלתי תלויות

הגדרה: במכרואידיק, כל קבוצה בלתי תלויה מקסימלית
ביחס להכלה נקראת בסיס.

טענה: כל הבסיסים במכרואידיק הם שולי גודל.

טענה: (תכונת ההחלפה) אם $A, B \in I$ הם שני בסיסים
אזי לכל $e \in A \setminus B$ קיים $f \in B \setminus A$ כזה ש-
 $A \setminus \{e\} \cup \{f\}$ הוא בסיס של המכרואידיק.

הוכחה: תהי $A' = A \setminus \{e\}$. $|A| = |B|$ ולכן

$|A'| < |B|$. למ $y \in B \setminus A'$ $f \in I$ $f \in I$ $f \in I$

ש. $B \setminus A' = B \setminus A$ $y \notin B$

$A' \setminus A = \emptyset$. זה חייב להיות כי

$|A' \setminus A| = |B \setminus A|$ ולכן אם $|A'| < |B|$ $C \in I$

אז $A' \setminus A \subset C$ אבל אז, לא ייתכן

ש B בסיס כי $|A| < |B|$.

הצעה: אפשר לבחור את f כך ש $f \in I$
 $f \in B \setminus A$ הוא בסיס.

היינו הצגה חד-חד-ערכית $\phi: A \setminus B \rightarrow B \setminus A$
עבורה אם $x \in A \setminus B$, $\phi(x) \in B \setminus A$
הוא בסיס.

שאלה:

1. אם $I = 2^E$ אזי (E, I) הוא מטראז' I

(E הוא הבסיס היחיד של המטראז' הזה)

2. תהי E קבוצה סופית של וקטורים מעל שדה F

וגדיר I כך: $F \subseteq E$ נמצאת ב- I

אם F וקטורים ב- F הם תלויים ליניארית.

אזי (E, I) הוא מטראז'. הוא נקרא
המטראז' הווקטורי:

$$|F| < |G|$$

$$F, G \in I$$

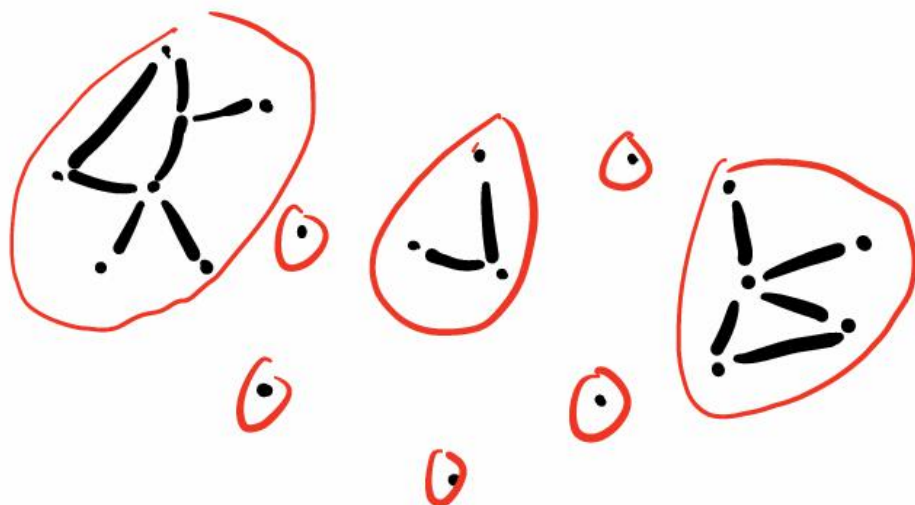
לא ייתכן שזוהי $G \in \mathcal{G}$, $\text{span}(F) \in \mathcal{G}$.
 כי $\dim(\text{span}(F)) = |F|$. אבל בתת מרחב ליניארי
 ממימד $|F|$ קבוצה של וקטורים בסיס
 בעלת $|F|$ יחידה. (מטראיד סגור ליניארי כגון מטראיד ליניארי).
 3. יהי $G = (V, E)$ גרף סופי לא מכוון.
 נגדיו $I \subseteq 2^E$ כאלון הבא:

$F \subseteq E$ נמצאת ב- I אם אין חזקה ב- G של
 הקשתות שלו ב- F . אזי (E, I)
 הוא מטראיד. (מטראיד המגדלים של G)
 אם $|V| = n$ וזאת גרף שהוא יסודי
 ריבוי קטירי אזי מס' הקשתות הוא $\geq n$.
 4. נגד קבוצה סופית E וחלקיה שלה לקבוצות זרות
 $E = E_1 \cup E_2 \cup \dots \cup E_m$. כאן n מספרים טבעיים
 $k_1, k_2, \dots, k_m$ שמקיימים $|E_i| \leq k_i$ אם i .
 נגדיו $I = \{F \subseteq E : \forall i, |F \cap E_i| \leq k_i\}$
 אזי (E, I) הוא מטראיד טקסו מטראיד
 חלקה.

שאלה: אם יש חפיפה כלשהי בין הקבוצות
 $E_1, E_2, \dots, E_m$, האם דאגה הצורה של I , (E, I)
 הוא תמיד מטראיד?

תשובה: נניח שכל $E_i \subseteq E_j$ או $E_j \subseteq E_i$ או $E_i \cap E_j = \emptyset$.
 האם אז דאגה הצורה של I , (E, I) מטראיד?

$I = \{F \subseteq E : \text{הקבוצה } F \text{ מכילה את כל הקשתות של } E \text{ שבהן } F \text{ היא תת-קבוצה}\}$



(E, I) הוא מרחב ויקטורי (המרחב ויקטורי של הקבוצות)

נניח שנתונה פונקציה מסקל חלופית על איברי המרחב (E, I) :

$$N : E \rightarrow \mathbb{N}$$

הפונקציה מסקל חלופית על איברי המרחב (E, I) :

המרחב (E, I) הוא פרוצדורה יחידה של פונקציה

הפונקציה מסקל חלופית על איברי המרחב (E, I) :

(E) מונה באופן מפורש

אלמנטים החמור

מחייבים את אברי E בסדר לא זוגי של מסקל. מחייבים את קבוצה חלופית. חלופים על האקסיומים E לפי סדר המיון. מוסיפים תמונה של אבר שמסלולו I .

טענה: הפסל של האלגוריתם הוא בהכרח דסים.

הוכחה: נניח $F = \{f_1, f_2, \dots, f_m\}$ הפסל של האלגוריתם
(לפי הסדר שבו האסמא אישים לטל). יהי $e \in E \setminus F$.
נניח שהעצם e אחרי f_k ולפני f_{k+1} (אם $k=m$)
לפי השדרת האלג' $I \not\subseteq \{f_1, f_2, \dots, f_k, e\}$. אז אם א"ש, לפי
תכונת היריאה, אם $I \not\subseteq \{f_1, \dots, f_m, e\}$. לכן, קב'
בית מקסימלית ביתם לטל, ולכן זה דסים.

טענה: פסל האלג' F הוא דסים בתל מוקד מקסימלי.

הוכחה: נובית באינדוקציה זה מספר הצדדים של האלג'
שכל שלל הקב' שהאלג' מחזיק מוביל דססים
אלג'מלי. (כלומר, היצע הוא לטל $m, m-1, \dots, 0, i$,
הקבוצה $\{f_1, \dots, f_m\}$ מוביל דססים אלג'מלי).

יהי F' דסים אלג'מלי כלשהו.

דסים האינדוקציה הוא $\emptyset \subseteq F'$.

נניח כי $\{f_1, f_2, \dots, f_i\} \subseteq F'$ עבור $i < m$

ונראה כי אם $\{f_1, \dots, f_{i+1}\}$ מוביל דססים אלג'מלי.

מקרה א': $f_{i+1} \in F'$ ולכן סיימנו.

מקרה ב': $f_{i+1} \notin F'$.

$$\{f_1, \dots, f_i\} \subseteq F'$$

אם $\{f_1, \dots, f_{i+1}\} \not\subseteq F'$ ואם העצם אלו לפני f_{i+1} ,
מתקיים $e \notin F'$: $e \in I \not\subseteq \{f_1, \dots, f_{i+1}\}$

נתבונן ב- $\{f_1, \dots, f_{i+1}\} \setminus F'$.

$$\{f_1, \dots, f_{i+1}\} \setminus F' = \{f_{i+1}\}$$

לפי תבונת ההחלפה, קיימת $f_{i+1} \in F' \setminus \{f_1, \dots, f_{i+1}\}$

עבור

$$\{f_{i+1}\} \cup \{f_1, \dots, f_i\} \setminus F' \text{ גם הוא זמין}$$

מכיון ש- e חייב להיות שייך לזוג.

אז f_{i+1} זמין שבו האלמנט e נמצא.

$$\text{האזורים, מתקיים } w(f_{i+1}) \leq w(e).$$

$$\text{לכן } F'' = F' \cup \{f_{i+1}\} \setminus \{e\} \text{ חייב גם}$$

הוא להיות זמין אופטימלי. הזמין הפה

מכאן את $\{f_1, \dots, f_{i+1}\}$.

סברא: הראנו שכל מרחב S של E הוא זמין. זמין S של E מקסימלי.

משפט (Radon+Edmonds): נטור מרחב קבוצות (E, I)

מקסימלית את תבונת הירישה, אז אלגוריתם החזון

מוביל $F \in I$ גדול מכל מקסימלי. עזרה כך

פונקציה מקבלת $E \rightarrow \mathbb{N}$, w , אז (E, I) הוא מרחב S .

הוכחה: נניח כי (E, I) אינו מרחב S , בפרט,

קיימת שתי קבוצות $A, B \in I$ זמין $|A| < |B|$

ושניהן מקסימליות ביחס לכל S $S = A \cup B$

$$S = \{e_1, e_2, \dots, e_{|A|}, \dots, e_{|S|}\} \quad \text{משקל}$$

$\underbrace{\hspace{10em}}_A$

לגדיר באנקציה משקל:

$$w(e) = \begin{cases} 1 + \varepsilon_i & e = e_i \quad i=1, \dots, |S| \\ 0 & e \notin S \end{cases}$$

נרצה ש- $\varepsilon_1 > \varepsilon_2 > \dots > \varepsilon_{|S|}$ וכן $\sum_i \varepsilon_i < 1$
 לדוגמה, ניתן לקחת $\varepsilon_i = 2^{-i}$

הכלל של אלמ' החמור $\{e_1, e_2, \dots, e_{|A|}\}$
 אולי גת'וסבת ע'ר אחרים שלא נמצאים ב-S-2
 ומשקלם 0. מנהל הפיתוח:

$$\sum_{i=1}^{|A|} (1 + 2^{-i}) < |A| + 1$$

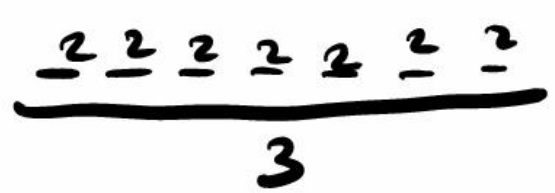
הפיתוח האופטימלי הוא לקחת את כל
 אלמ' B : משקל הפיתוח הזה הוא ערך
 ממש - n
 $|A| + 1 \leq |B|$

נניח כי (E, I) אינו מחווא'ד. אם כן, מכיון
 שחבולת הידועה מתקיימת, חייב להיות שחבולת
 ההרקה לא מתקיימת. כלומר, קיימת קבוצת
 $A, B \in I$ עבורן $|A| < |B|$ אבל קט $e \in B \setminus A$,
 $A \cup \{e\} \notin I$. ניתן לומר גם שכל $e \in A \setminus B$,
 $B \cup \{e\} \notin I$. מכאן מתקיים ש- A, B מקסימלית זיכוס
 אולם בתוך הקבוצה $S = A \cup B$.

צילום מאלתר!

בעיית שיפוט קטעים:
 E - אוסף של קטעים על הישר הממשי.
 $F \subseteq E$ נמצאת ב- I ואם הקטעים ב- F לא
 חופפים זה לזה.

אלמ' החמקן לא עוקד עבורו ב' בוקצית מסוף:



נתון: $G = (V, E)$ סופי. לא מכוון וקשיח

פונקציה $W: E \rightarrow \mathbb{N}$ מעידה חילוקית על הקשתות

מטרה: למצוא תת-גרף קשיח שבוורט את כל הצמתים ומשקלו מינימלי

בהכרח, תת-גרף כזה הוא Φ בורט

הערה: חתך בגרף הוא קבוצת הקשתות שמחברות בין הקצוות/צומים בסט הצומים של חתך. כל צמת הגרף לשת קבוצה לא חיקו (דוגמה)

טענה: גרף קשיח חסר מחצלים עם n קצוות/צומים מכיל בדיוק $n-1$ קשתות.

טענה: אם M מוסיפים Φ T קשת שמחברת בין שני קצוות/צומים שונים, קצותיהם יסמנו S ו- T וקשת e יוצרת ציקל C המכיל את T ו- e .

מסקנה: יהי $T \subseteq E$ קשת תהי $e \notin T$

אם $T \in \mathcal{T}$ קשת כלשהי במשולב הנוצר

מ- T ו- e T $\cup \{e\}$ $V(T)$ e T $\cup \{e\}$ $V(T)$

משפט: יהי $F \subseteq E$ חתך ב-G ויהי $e \in F$

קטת בעלת מטקל $w(e)$ מינימלי ב-F. אזי
בהכרח יש צפ"ח שמכיל את e .

הוכחה: נניח בעלת טקל e נכון. יהי T

צפ"ח. בהכרח איננו מכיל את e . אם
נאסף את e ו- T ייסזר מחדש C .

ח"כ להכיל לבחור את קטת $M-F$.

יהי $e \neq f$ שזו קטת טל C . בהכרח

$T \in f$ וזכר $w(f) \geq w(e)$. אבל $f \in T$

אם e בורח, ומשקלם אינו גבוה יותר

ממשקל T .

אבחנה: יהי T שזו בורח. יהי $e \in T$. החרת

e מחלקת את צמת T לשני רכיבים

קשיים על חיקים וזכרן מציורה חתך

F_e בורח. בהכרח $e \in F_e$. אם T צפ"ח

אזי בהכרח e קטת בעלת מטקל מינימלי.

בחתך זה, אחת ניתן להחליפה בקשת
קלה יותר ב- F_e וזו סתירה לכך ש- T צפ"ח.

משפט: יהי C מעגל בסיס E - G ,
 ויהי $e \in C$ קשת שמחקה מידה בין קשתות
 המעגל. אזי, קיים ענף שאינו מכיל את e .

הוכחה: יהי T ענף. אם $e \notin E(T)$, אז המעגל
 מתקיים. אם $e \in E(T)$, אז הסורת e מ- T מחלקת
 את T לטני רכיבים קשירים לא חזקים, נניח
 T_1, T_2 . $V = V(T_1) \cup V(T_2)$. צמתי C נחלקים
 בין שני הרכיבים הללו, כי קצות e הרכיבים האלו.
 כמו כן, C חוצה את החתך E בין $V(T_1)$ ו- $V(T_2)$.
 לפחות פזאיים (זה מעגל) ועל כן יש קשת $e \neq f$
 $f \in C$, שמקורה בין צמתי e - $V(T_1)$ לצמתי e - $V(T_2)$.
 ביכרה $f \notin E(T)$ (כי $e \in E(T)$ והחתך הוא צר
 ע"י הסרת e מ- T). כמו כן, על פי ההנחה,
 $w(f) \leq w(e)$. אז $T - e + f$ הוא ענף פזאיים,
 ומשקלו אינו גדול יותר מאשר T .

ש.ל.ה. ד.מ.צ.א.ת. ע"פ מ"

נ.ח. ש.ק.ש.ל.ת. ה.ה.ה. י.ד.ו.ל.ת. ל.ה.י.ת. צ.ה.א.ת.
ב.כ.ח.ו.ל. א.ו. ב.א.ד.א.מ. א.ו. ל.א. צ.ה.א.ת.

ה.כ.ל.ה. ה.כ.ח.ו.ל.: ב.י.ח.ר.י.מ. ח.י.ת. $F \subseteq E$ ש.א.ן
ב.ו. א.ל. ק.ש.ת. כ.ח.ו.ל.ה. ו.צ.ו.ק.ע.י.ם $E \subseteq F$ ה.ע.ל.ת.
מ.ש.ק.ל. מ.י.נ.מ.ל.י. ב.י.ן. ק.ש.ל.ת. F ב.כ.ח.ו.ל.

ה.כ.ל.ה. ה.א.ד.א.מ.: ב.י.ח.ר.י.מ. מ.ע.ל. C ש.א.ן. ב.ו. א.ל.
ק.ש.ת. א.ב.א.מ.ה. ו.צ.ו.ק.ע.י.ם $E \subseteq C$ ה.ע.ל.ת. מ.ש.ק.ל.
מ.י.ב.י. ב.י.ן. ק.ש.ל.ת. C ב.א.ד.א.מ.

מ.ש.כ.ל.: ל.ב.ע.י.ל. א.ת. ה.כ.ל.י.ם. ה.ע.ל.ו. ב.ס.ד.
ל.ב.ש.ה.ו. כ.ל. ע.ו.ד. י.ש. כ.ל. ש.א.ב.ש.ר. ל.ה.ע.ע.י.ל. א.ל.י.
כ.א.ש.ר. ע.ו.צ.ר.י.ם.

- (1) כ.ל. ה.ק.ש.ל.ת. צ.ה.א.ת.
(2) ה.ק.ש.ל.ת. ה.צ.ה.א.ת. ב.כ.ח.ו.ל. ב.ן. ע"פ מ".

ה.א.ב.ח.ה.: ה.א.ש.י.ת. נ.א.כ.י.ח. ב.א.י.נ.ב.ק.צ.י.ה. ה.
מ.ס.ב.ר. ה.צ.ע.ד.י.ם. ש.ת.מ.י.ד. י.ש. ע"פ מ" ש.מ.כ.י.ל. א.ת.
כ.ל. ה.ק.ש.ל.ת. ה.כ.ח.ו.ל.ת. ו.א.ל. ק.ש.ת. א.ל.ד.א.מ.ה.
ב.ס.י.ם. ה.א.י.נ.ב.ק.צ.י.ה. ב.ה.ת.ח.ל.ה. א.ן. ק.ש.ל.ת. צ.ה.א.ת.
ו.י.ב.ן. ה.ל.ע.ה. ב.א.ד.א.ל. ל.ב.א.ה.

צדד הא'בוקצה: יהי T צדד שמקיים את
הנחת הא'בוקצה (מכאן את כל הקטלות הכחולות
עד כה ואף קשת אדומה). הצדד הא'בוקצה
אפשרות:

- (א) מפעילים את הכלל הכחול עד חתך F . יהי
 $e \in F$ הקשת שנבחרה להיבצע בכחול. אם $e \in E(T)$,
סיימו. אחרת, הוספת e ל- T יוצרת מעגל
פשוט C . במעגל זה יש לבחור קשת אחת $f \neq e$,
זכורה $f \in F$. צדד הכלל הכחול, קשת זו
אינה צבועה בכחול. כמו כן, $w(f) \geq w(e)$,
צדד בחירת e . אז $T - f + e$ הוא צדד
שמעקלו לכל היותר המעקל של T , ולכן זה צדד.
(ב) מפעילים את הכלל האדום עד מעגל פשוט C .
יהי $e \in C$ הקשת שנבחרה להיבצע באדום. אם
 $e \notin E(T)$, סיימו. אחרת, נבחרן בחתך F_e
(שמושיה צ"י החלוקה של T לשני רכיבים קטנים
כאשר מסירים את e מ- T). יש ק- C לבחור
קשת אחת נוספת $f \neq e$ כך ש- $f \in F_e$.
 $f \notin E(T)$, אחרת T מכיל מעגל. f אינה
צבועה באדום, אחרת לא היינו מפעילים את הכלל
האדום עד C . דפי בחירת e , $w(f) \leq w(e)$.
לכן, $T - e + f$ הוא צדד שמעקלו לא גדול
ממעקל T , וזהו כן הוא צדד.

זכש'ו נאר פלצן שהצעה על כולם להיפסך
 לפי שכל הקטנות צבאות. לית השלילה שזה
 קיה, צומר צדד חלק מהקטנות ולא ניתן להמשיך.
 יפ. ד עכ"נ שמכיל את כל הקטנות הצבאות
 בבתם ואף קשת אלומה. יהי e קשת כשה
 שאר הצבאה. אם $e \in E(T)$, אז החתך F_e
 לא מכיל אף קשת כחמה (כי כל אלו נמצאות
 ב- $E(T)$ ו- $F_e = E(T) \cap F_e$. זה החתך הציג אפס
 להפסיל את הכול הפחול. אם $e \notin E(T)$ אז
 הוספת e ל- T סוגרת מעגל בשל C
 ששאר הקטנות שלו ב- $E(T)$. לכן, אין ב- C
 אף קשת אלומה, ולכן אפשר להפסיל את C את
 הכול האדם.

אם כל הקטנות צבאות, אז הקטנות הפחולות
 חייבות להיות עכ"נ, אחת הציג שמכיל
 אותו מכיל אם קשת אלומה.

מסקנה: האלגוריתמים של Prim ושל
 Kruskal מחזקים עכ"נ

דוגמה 1 - מפתור האיחור

קלט: רשימה של n משימות, כל משימה נתונה עם ידי זוג מספרים סבביים (p_j, d_j) כאשר p_j משך הזמן שהמשימה דורשת ו- d_j הוא מועד הסיום הנדרש.

פלט: שיבוץ תקין של המשימות סביב הזמן, כלומר, פונקציה $f: \{1, \dots, n\} \rightarrow [0, \infty)$ המקיימת לכל זוג משימות i, j ,

זמן הקצוץ

$$(t(i), t(i) + p_i) \cap (t(j), t(j) + p_j) = \emptyset$$

כך שהשיבוץ יהיה MN מצביע את העיכוב האחרון

$$L_{\max}(t) = \max_{j \in \{1, \dots, n\}} \underbrace{\max\{0, t(j) + p_j - d_j\}}_{L_j}$$

האלגוריתם - earliest due date (EDD)

נמין את המשימות לפי מועד הסיום הנדרש.
(בה"כ $d_1 \leq d_2 \leq \dots \leq d_n$)

נשקף את המשימות לפי סדר:
הכאשר קצמן s .

אחרי שיבוץ המשימה ה- j ייתבצמן $t(j)$ נשקף את המשימה ה- $j+1$ ייתבצמן $t(j+1) = t(j) + p_j$

סיבוכיות: $O(n \log n)$ $t(j+1) = p_1 + p_2 + \dots + p_j$

משפט: EDD ממנעה את L_{max} .

הוכחה: נהגון השיבוץ כשהוא שמנעה את

L_{max} . הצי העלת הכעלות, אין "רווחים"

השיבוץ הזה - המשמח הוא שום מתחלה בזמן

וב משמח אחריה מתחלה מיד עם סיום המשמח

הקלזמת. אם סדר המשמחות אינו זהה עכ

של EDD, אז חייב להיות זוג משמח-עוקבות j, i

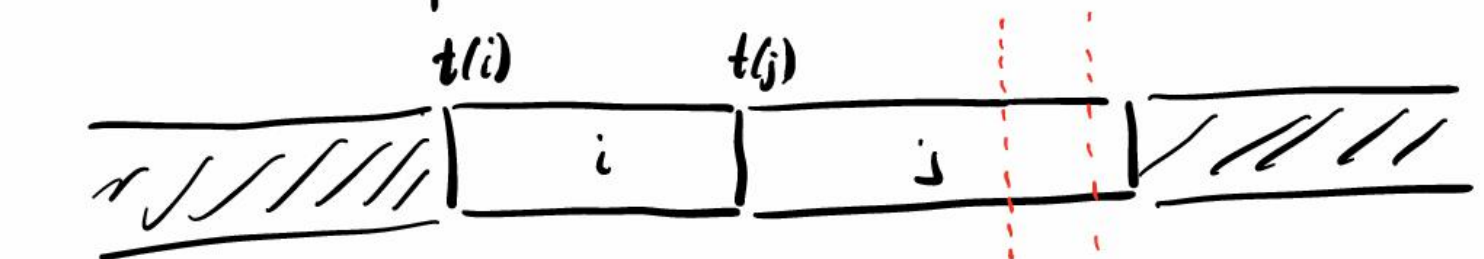
ע"י t (כאמור): $t(j) = t(i) + p_i$ זקרון $i < j$.

נראה שהחלפת הסדר ביניהן איננה משפיעה את

L_{max} . זה מוכיח את המשפט כי אפשר לעצ

החלפות כאלו עד שמקבלים את הסדר של EDD.

השיבוץ לפני ההחלפה נראה כך:

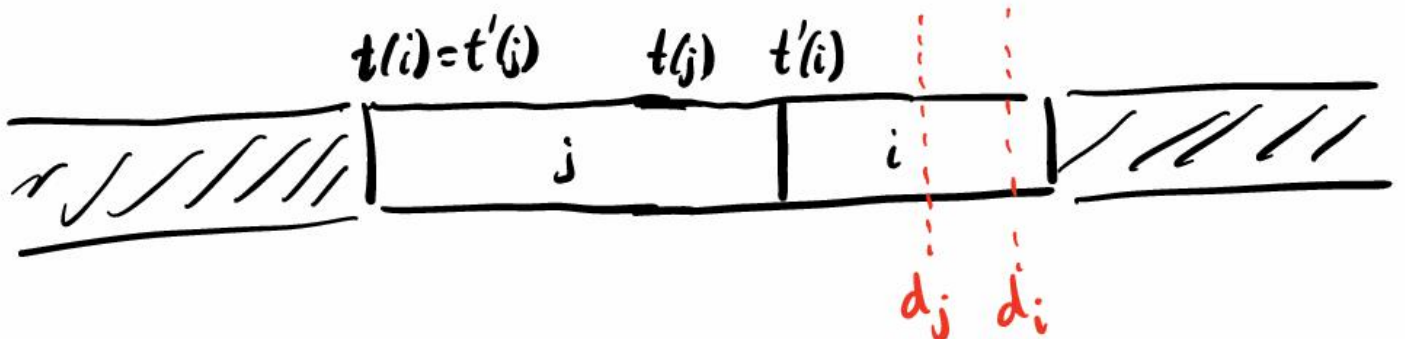


$L_i = 0$ $L_j > 0$

זה לא קה"כ

$d_j \leq d_i$

אז אחרי ההחלפה:



d_j d_i

נסמן את הערכים אחרי ההחלפה בקטנים

נשים עקב כי L_j עמא עקד ואילו L_i עמא קטן.

קפיד: $L'_j \leq L_j \leq L_{max}$, אקד עס

$$L'_i = \max\{0, t(i) + p_i - d_i\} = \max\{0, t(j) + p_j - d_i\} \leq \\ \leq \max\{0, t(j) + p_j - d_j\} = L_j \leq L_{max}$$

לכך $L_{max} \leq L'_{max}$ (העיקרים עס טאק האטילאק)
 עס מעתים).

פארה 2 - העיית הדיבראק

המחברת מחשה העיכרון הירטטלי. מחולק

עצמים. פיסית, יש עיכרון מהיר עס

קידום עס א דפים וטאר הדפים

מורעקים העיכרון איטי (דיסק טאו פלאט אקד).

המחבר ניש ערעם העיכרון המחיר ווע

כן יש ערעם דפים עזין בין העיכרון
 האיטי עמחיר.

הקדם: סדרת דפים שרונים לעשת אוליהם,

עס פסיד העישה $\sigma_1, \sigma_2, \dots, \sigma_t, \dots, \sigma_m$

יש סה"כ $a > 0$ דפים ווע $t, \dots, \dots, \dots$

(אשעי עמחור ולבקט דף יתרי ערעם אחת עסמרה)

הפלט: עבור $t = 1, 2, \dots, K$ שם מקדים
 קדם שאנו בציכרון המהיר, ציין איזה
 קדם יש ייצוגי מציכרון המהיר (ה- t -ים)
 הרימונים והדפים הנצרכים תלויים במידת
 בהחלטת הקדמות).

האלגוריתם של Belady: נסמן ב- C_t
 את קבוצת הדפים בציכרון המהיר כאשר מתקף
 t . אם $C_t \neq \emptyset$ אז נתלים אלו
 בדף $\sigma \in C_t$ זכורו $\sigma_t = \sigma$: $\min\{t' > t : \sigma \in C_{t'}\}$
 הוא מירבי (כלומר, הדף שהזמן שיקטו אלו
 שלב הוא המאוחר ביותר).

משפט: האלגוריתם של Belady מתעב פיתרון
 שמספר הדפולים שלו מינימלי.

הוכחה: נחלק בפיתרון כלשהו לסדרה, ויהי
 t הצעד הראשון שבו הפיתרון היה שונה
 מהפיתרון של Belady. כלומר, תוכן הציכרון
 המהיר C_t היה בשני הפתרונות כאשר מקדים
 את הדפולים $\sigma \in C_t$, אולם האלג' של Belady
 בחר את $\sigma \in C_t$ ואילו S בחר את $\sigma' \in C_t$,
 כאשר $\sigma \neq \sigma'$.

לדיר פיתרון אחד S' כדלקמן:

לפני צעד t , S' זהה ל- S (למעט ל-Belady).
בצעד t , S' זורק את S .

אחרי צעד t , S' זהה ל- S , למחט המנויים הקטנים!

ולאם בצעד $t > t'$ מתקיים $S' \neq S$, $S - S'$
לא מוזיק את S' והוא זורק את S , אז
חייב להיות ש- S' לא מוזיק את S' . בלוקה זה
 S' זורק את S' ומכאן ואילך $S - S'$
צהים.

(ii) אם $S' = S$ אז $S - S'$ זורק קטן "ס":
אם $S = S'$, אז S' לא חייב לעשות צעד (כי
בשלם זה עדיין S' מוזיק ע"י S')
ואחרי צעד זה $S - S'$ זהה ל- S . לעומת זאת,
אם $S \neq S'$, אז S' זורק את S' ומכאן
את S ואם אחרי צעד זה $S - S'$ צהים.

כדי שצדן אחר יעשה
צעד ב- S' לפני

אחרי הרנספורמציה, S' זהה ל- S Belady עד
צעד $t+1$ ולא משלם יותר מ- S . ולפי
לחמסיק סאינדקציה עד שמקלים פיתרון שזהה
ל- S Belady ואין משלם יותר מהפיתרון המקורי
מהתחלה איתו.

קציית שיפוף קטעים

קלט: רשימה של n קטעים מסומים על הישר, כל אחד נתון על ידי זוג סדר של נקודת התחלה ונקודת סיום:

$$(s_1, t_1) \quad (s_2, t_2) \quad \dots \quad (s_n, t_n)$$

בה"כ הנקודות הן מספרים שלמים

פלט: רשימה באורך מירבי של קטעים ללא חופסים

האלגוריתם: נמין את הקטעים בסדר עולה. אז של זמן סיום (בה"כ $t_1 \leq t_2 \leq t_3 \leq \dots \leq t_n$) נעבר על הרשימה הממוינת לפי סדר ונוסיף עפ"י כל קטע שאינו חופף עם קטעים הקודמים על הקחנא.

סיבוכיות: המיון דורש $O(n \log n)$ פעולות. המעבר על הרשימה הממוינת דורש $O(n)$ פעולות. כדי לבדוק תביעה, די לבדוק מול הקטע האחרון שנקחנא: אם בודקים את (s_j, t_j) והקטע האחרון שנקחנא היה (s_i, t_i) , אז נ"ל, $i < j$, אין תביעה אם $s_j > t_i$. עכן, בדיוק התביעה לוקחת $O(1)$ פעולות וסה"כ $O(n)$ פעולות. עכל הקטעים.

סה"כ: (חפלה) 0 בעלות.

סיביות המקום: $O(1)$ (דגומס) (קדם)

המיון דורש משתנה נוסף וקצת תחביר
דורש עזבאר את נקודת הסיום של הקדם
האחרון בפעם נוסף כה.

מה סברנו? - בעלות השמה והשוואה של
מספרים טבעיים ותא' זיכרון שמכילים כל
אחד מספר טבעי.

לבולת האלמנטים: נסמן ב- A את קבוצת הקלים
בביטוי של האלמנטים.

משפט: אם קבוצה I של קלים שאינם חופפים
זה עם זה, $|A| \geq |I|$.

הוכחה: נניח כי $A = \{(s_{i_1}, t_{i_1}), \dots, (s_{i_k}, t_{i_k})\}$

1- $I = \{(s_{j_1}, t_{j_1}), \dots, (s_{j_l}, t_{j_l})\}$ כאשר

$$t_{i_1} \leq t_{i_2} \leq \dots \leq t_{i_k}$$

$$t_{j_1} \leq t_{j_2} \leq \dots \leq t_{j_l}$$

זמנו להראות כי $k \geq l$.

נניח כי נובח האינדוקציה של r שהקלים

$$(s_{i_1}, t_{i_1}), \dots, (s_{i_r}, t_{i_r}), (s_{j_{r+1}}, t_{j_{r+1}}), \dots, (s_{j_l}, t_{j_l})$$

אינם חופפים זה עם זה.

ב.ס.ס האנאליזה: $r=1$. אם כי הכלל של האנאליזה
 $t_i \leq t_j$ ולכן אם נחליף את הקטע (s_j, t_j)
 בקטע (s_i, t_i) , אפשר לשמור על סדר הקטעים.
 ב-I. (s'_i, t'_i) , $s'_j \geq t'_j \geq t_i$, (s_{j_m}, t_{j_m}) וכו'.

צגה האנאליזה: מניחים לבנות $r-1$ ואז כותבים r -
 אם נמח את האנאליזה, הקטעים

$(s_{j_1}, t_{j_1}), \dots, (s_{j_r}, t_{j_r}), \dots, (s_{i_r}, t_{i_r}), \dots, (s_{i_1}, t_{i_1})$
 אינם חופפים. דבר, כאשר האנאליזה בוחן
 את (s_{i_r}, t_{i_r}) אם הקטע (s_{j_r}, t_{j_r})
 זמין לבחירה, ואם כן $t_{i_r} \leq t_{j_r}$, ואם כן ניתן
 להחליף את (s_{j_r}, t_{j_r}) ב- (s_{i_r}, t_{i_r}) ואז
 כל הקטעים לא יהיו חופפים זה לזה.

מסקנה: אם $k > l$, אז הקטעים

$A = (s_{i_1}, t_{i_1}), \dots, (s_{i_k}, t_{i_k}), (s_{j_{k+1}}, t_{j_{k+1}}), \dots, (s_{j_l}, t_{j_l})$
 אינם חופפים זה לזה. בפרט, אחרי שהאנאליזה
 בוחן ב- (s_{i_k}, t_{i_k}) , הקטע הבא עדיין זמין.
 כלומר, אפשר להמשיך האנאליזה סיים את הניתוח.

העיון דומים לא חלופים:

מיון ע"י נקודת התחלה:
 מיון ע"י אורך:

$$-1 \quad \sum_{e \in F} w(e) \text{ מרביס מלל. (אפשרותית: } (v_e, v(e)) \leq V \text{)}$$

אוסף הארצות החקלאות והיישובים
 היישובים, אלה לא את תבולת ההחזקה.
 זה לא מסוואיז, למן אולם החמשן ל/הכרח
 ארץ.

למעשה, אולם ממש ארץ: נניח שיש ארץ
 אחת עם נפח V ומשקל 1 , ו- $1-n$ איברים
 עם נפח $\frac{V}{1-n}$ ומשקל $1-n$. אולם החמשן
 ישנם משקל 1 . האולם ממש קרוב ל- $1-n$.

זה עם הפיטה הבאה: נניח את האדריים לבי
 היחידים לייצוג נפח $\frac{w(e)}{\sqrt{e}}$, קסדר ללא צולם.
 אולם נארוז בחמשן לבי הסדר הטה.

אם זה לא נותן פיתרון אולם לבי: נניח שיש
 רק שני אדריים: איברי נפח V ונפח V
 ואיברי נפח 1 ונפח $1+n$. נקבל $1+n$
 במקום V .

אז אולי נסה כן: נדחיק את האדריים
 שני פתאום - זה יעיל וארצה של האדרי
 היוות בלתי.

זה נותן קיווה בפקטור 2:

אם נאמר שכל איבר נקודת משקל $\leq$ א/פ.מ/ר
(כ. "צב.נ"ר" המשקל ר'ח'צת נח היא מקס.מל'ר)
האיבר הוא 405 בולבא' לא מוסר יאר ממשקל
המקס.מל'ר על אי'ר

פיתרון שבהי-לברייט התמלא מאפשר לאורז חפצים באופן חלקי. אם חפץ i נארג בשיעור $[0, \epsilon] x_i$ אז הוא תופס נפח $x_i v_i$ ומחיר תועלת $x_i u_i$.

אלג' מתבונן: נמנין את החפצים בסדר $\frac{u_1}{v_1} \geq \frac{u_2}{v_2} \geq \dots \geq \frac{u_n}{v_n}$ נארג לפי הסדר כל חפץ בשיעור המירבי שלא תורם מנפח הפנוי שנותר בתמלול.

הערה: יהיה לכל היותר חפץ אחד i נארג $[0, \epsilon] x_i$.

כפרט $x = (x_1, x_2, \dots, x_n)$ כאשר $x_i \in [0, \epsilon]$

1-
$$\sum_{i \in J} v_i + \alpha v_i = V$$
 (אלג' אים כן כל החפצים נעשים α דטרמל, שגש יכול להישאר מקום חיך)

מטרה: האלגוריתם מחשב פיתרון אופטימלי.

הוכחה: יהי y פיתרון אופטימלי. נטעון. יהי i האינדקס הראשון שבו $x_i \neq y_i$. בהכרח $x_i < y_i$ כי בפיתרון x כל חפץ נארג לפי היתר בשיעור המירבי האפשרי בהינתן איכות החפצים הקודמים. נדיר פיתרון y' כדלקמן:

$$y'_j = \begin{cases} y_j & j < i \\ x_i & j = i \\ y_j - \epsilon_j & j > i \end{cases}$$

באשר $\sum_{j > i} \epsilon_j v_j = (x_i - y_i) v_i$, 1- $y_j \leq \epsilon_j$ לכל $j > i$.

זה אפשרי כי x, y תופסים את כל נפח התמלול. תוספת הכוללת $(x_i - y_i) u_i$ היא לפחות כזו

הבסד הכולל $\sum_{j > i} \epsilon_j u_j$, כי $\frac{u_i}{v_i} \geq \frac{u_j}{v_j}$ לכל $j > i$. זכר, אם y' פיתרון אופטימלי.

אז נחזור על השיט הזה עד שנקבל פיתרון זהה ל- x .

מסקנה: אם $\sum_{j=1}^n u_j \leq V$ עבורו u_j מקסימלי, אזי

$$u_i + \sum_{j=1}^n u_j \geq \text{ערך ביתרון אופטימלי}$$

הוכחה: באמצעות אי-שוויון חזק של מילר, ניתן להוכיח את הטענה. נניח u_i הוא המקסימום של u_j עבור $j=1, \dots, n$. אזי

$$\sum_{j=1}^n u_j \geq \sum_{j=1}^n u_i = n u_i$$

$$\begin{aligned} \sum_{j=1}^n u_j &= \sum_{j=1}^n u_j + u_i - u_i \leq \sum_{j=1}^n u_j + u_i \\ &\leq \sum_{j=1}^n u_j + u_i \end{aligned}$$

דוגמה פשוטה:

שיבוץ קטעים מחושקלים:

נתונים קטעים על הישר הממשי

$$(I_j = (a_j, b_j))$$

ואם החשקלים שלהם

$$I_1, I_2, \dots, I_n$$

$$w_1, w_2, \dots, w_n$$

רוצים למצוא קבוצה של קטעים לא חופפים שמקלה מקסימלית.

רעיון: נניח שהקטעים מחוברים לפי זמן הסיום שלהם, כלומר $b_1 \leq b_2 \leq \dots \leq b_n$.

שימו לב, אם אנחנו מרשים פיתרון שלא חוצה מחדר ל- b_j , אז זה פיתרון עבור הקטעים $I_1, I_2, \dots, I_j$.

$$S_j = \text{שיבוץ של קטעים } I_1, \dots, I_j \text{ שמקלה מקסימלית}$$

המטרה שלנו היא למצוא את S_n .

זה ניתן למטלת בעזרת מסתת הקורסיה הבאה:

$$j_i = \operatorname{argmax} \{b_j : b_j \leq a_i\}$$

$$S_1 = \{I_1\}$$

$$S_i = \begin{cases} S_{i-1} \\ S_{j_i} \cup \{I_i\} \end{cases}$$

$$w(S_{i-1}) \geq w(S_{j_i}) + w_i \quad \text{אם}$$

אלת

סיקוביות? -

$O(n \log n)$ זמן (צורך למיין לפי b לפי a)

$O(n)$ מקום (צורך למחוק את היש-מה הממוינת
לפי b ואת הסימן הנ לרא i)

קז"ת סכום חלקי (subset sum)

נתונה סדרה של מספרים שלמים (מספר יכול להיות
שלילי) $a_1, a_2, \dots, a_n$
צריך לקרר אם יש תת-סדרה לא ריקה של
המספרים שסכומה 0.

פיתרון: נניח שהמספרים ממוינים מהקטן
לגדול. N סכום השליליים, P סכום החיוביים.

$$T(i, \sigma) = \begin{cases} \text{True} & \text{אם יש תת סדרה של } a_1, \dots, a_i \text{ שסכומה } \sigma \\ \text{False} & \text{אחרת} \end{cases}$$

קירור כי $1 \leq i \leq n$

אם קירור כי $N \leq \sigma \leq P$ קטריכים עבור
(כי כל יתר התוצרים הם בקירור False)

$$T(1, \sigma) = \begin{cases} \text{True} & \sigma = a_1 \\ \text{False} & \text{אחרת} \end{cases} \quad \text{עבור } i > 1$$

$$T(i, \sigma) = \begin{cases} \text{True} & T(i-1, \sigma) \vee T(i-1, \sigma - a_i) \\ \text{False} & \text{אחרת} \end{cases}$$

היתשלה נמצאת בראש $T(n, s)$

כמה תאים יש? - $n \times P + |N| + 1$

אפשר למלא את הטבלה לפי סדר
מילוי תא דורש $O(1)$ פעולות אריתמטיות

זה אלגוריתם פסאודו-פולינומי, כי P ו- $|N|$

אינם פולינומים במספר הקטעים הדורש

ל"זאת את הקלט.

אבל אם הקלט מוצג ביצוג אולי, זה אולי
פולינומי.

בעיית התעלה

$v_1, v_2, \dots, v_n$
 $w_1, w_2, \dots, w_n$

n חפצים עם גודל:
 ומשקל:

V תרומת שקיהולת

צריך למצוא

$$\begin{aligned} \arg \max_{P \subseteq \{1, \dots, n\}} \quad & \sum_{i \in P} w_i \\ \text{s.t.} \quad & \sum_{i \in P} v_i \leq V \end{aligned}$$

כאלו:

1. האריזה לפי משקל ערוסה
2. האריזה לפי משקל יחידות גודל ערוסה
3. הטוב מבין 1 ו-2 משהם לפחות $\frac{1}{2}$ מהמקסימום

פיתרון רקורסיבי: החפץ האחרון (n) נמצא בפיתרון או אינו נמצא בפיתרון.

מקרה א' - הוא נמצא בפיתרון. במקרה זה צריך למצוא את שאר החפצים בתעלה שקיהולת $V - v_n$.

מקרה ב' - הוא לא נמצא בפיתרון. במקרה זה צריך למצוא את שאר החפצים בתעלה שקיהולת V .

אם כן, נסמן ב- $P(i, V)$ את האריזה האופטימלית של החפצים $1, \dots, i$ בתרומת שקיהולת V .

$$P(n, V) = \max \{ P(n-1, V), P(n-1, V-v_n) + w_n \}$$

↑
 זה מה שאנחנו רוצים לחשב

מימנו בסוף של נוסחת הדינמיקה מקבלים את המכניזם
 עם סיבוכיות זמן אקספוננציאלית - כל אפילו אפשר
 עקרו את האלגוריתם, כלומר 2^n אפשרויות.

אולם, אם נתבונן ב- $P(i, \cdot)$ אין קהברה 2^i
 אפשרויות שצריך לבדוק. הערכים הדינמיים של
 הנבח הם מספרים שלמים בין 0 ל- n $\sum_{i=1}^n$.

הביטוי של $P(i, \cdot)$ ערכי $P(i-1, \cdot)$ ניתן לחשב את כל
 ערכי $P(i, \cdot)$ בזמן $O(n)$.

עבור איברי P נסמן ב- $w(P)$ את משקלה.

האינדוקציה:

אם $v, v' \in V$ ϕ, s
 אחרת w, w'
 $\forall v' \in \{0, 1, \dots, v\}$:
 $P(i, v'), w(P(i, v')) \leftarrow$

עיצוב! נניח שחישבנו את כל $v' \in \{0, 1, \dots, v\}$ את
 $P(i-1, v')$ ואת $w(P(i-1, v'))$

$\forall v' \in \{0, 1, \dots, v\}$
 $P(i, v'), w(P(i, v')) \leftarrow$
 $\begin{cases} P(i-1, v'), w(P(i-1, v')) \\ P(i-1, v'-v_i), w(P(i-1, v'-v_i)) + w_i \end{cases}$
 (כאן w_i הוא המשקל של v_i)

טענה: בסיום היציג האלגוריתם $P(n, V)$ הוא פיתרון אופטימלי.

הוכחה: מוכיחים באינדוקציה על i שכל $V, \dots, V'$ $P(i, V')$ הוא פיתרון אופטימלי של אריזת החפצים $V', \dots, V$ בתמורה בעמ V' .

סיכומים:

זמן: אימתור + n איטרציות על i
כל צעד כזה יש לולאה על $1-V$ זרמים של נבח
לכל צעד כזה מקבלים $O(1)$ פעולות אריתמטיות
סה"כ $O(nV)$ פעולות אריתמטיות

מקום: ציג לטמור זרמים עקב $1-i$ ופגור i .
סה"כ $O(V)$ תאי ציפון מעבר לקלט.
כל תאי שומרים את האריזה ולא מעקלה
סה"כ $O(nV)$ תאים שמחזיקים ערך מספרי
או מצביז.

זה פולינמי האורך הקלט 2 - תלוי מה הייצוג
של V . אם V מיוצג בייצוג אולטארי, אז כן.
אם V מיוצג בייצוג בינארי - לאו דווקא ("תכן
ע- V אקספוננציאלי בערך הקלט, זה תלוי ב- n).

3/13/2002

procedure dyn_knapsack(v, w, V):

for $j = 0, \dots, V$:

if $j < v_1$ then $P(1, j) \leftarrow \emptyset$
else $P(1, j) \leftarrow \{1\}$

for $i = 2, \dots, n$:

for $j = 0, \dots, V$:

if $v_i > j$ then $P(i, j) \leftarrow P(i-1, j)$

else if $P(i-1, j) > P(i-1, j-v_i) + w_i$

then $P(i, j) \leftarrow P(i-1, j)$

else $P(i, j) \leftarrow P(i-1, j-v_i) \cup \{i\}$

return $P(n, V)$

end procedure

סיבוכיות פולינומית בעלות הקלט, אם הוא ניתן
 ב"צט"א אלקרי, נקראת פסאודו-פולינומית.

וסיבוכיות של האלגוריתם עולה הן פסאודו-פולינומית ביחס
 לביטוי V .

במובן, ייתכן ש- V מאלף בעד היחס ϵ -ח. במקרים רבים ברורה
 זאת הפיגורציה שהמשקלים של המפצים קטנים, לא הרבה.

אז נסה לבנות אלגוריתם פסאודו-פולינומי ביחס למעקף.
 המפצים $w_1, \dots, w_n$ במקום היחס ϵ - V .

$$W_{max} = \max_i \{w_i : v_i \leq V\}$$

המשקל המרבי של איפה פגשתי הן W_{max} ח.

אם כן, נגדיר $Q(i, w) =$

איפה של מפצים n - $\{1, \dots, n\}$ שמסירה הן של
 בדיוק w ובעיה מינמליזציה. (אם אין איפה שמסירה הן בדיוק w נסמן
 ב"י זרז מילוד $none$)

זכור, אפשר להפחית נוסטר הקורסיה בקלמן:

$$\begin{array}{ll} \forall i=1, \dots, n & Q(i, 0) \leftarrow \phi \\ \forall w=1, \dots, W_{max} & Q(1, w) \leftarrow \begin{cases} none & w \neq w_1 \\ \{1\} & \text{אחר} \end{cases} \end{array}$$

$\forall i=2, \dots, n$
 $\forall W=1, \dots, nW_{max}$

if $Q(i-1, W) = \text{none} \wedge (W - w_i < 0 \vee Q(i-1, W - w_i) = \text{none})$:

$Q(i, W) \leftarrow \text{none}$

else if $v(Q(i-1, W)) < v(Q(i-1, W - w_i)) + v_i$:

$Q(i, W) \leftarrow Q(i-1, W)$

else

$Q(i, W) \leftarrow Q(i-1, W - w_i) \cup \{i\}$

היכן התוצאה? - בתא $Q(n, W)$ עבור W המקסימלי.
 עבורו בתא זה לא ישום none .

מה הסבירות? - כל אי-תחל/זיכרון גורם $O(n)$ פזולות.
 יש סה"כ $O(n^2 W_{max})$ צעדים כאלו. ניתן לקרוא את
 התוצאה תוך כדי חישוב זיכר $Q(n, \cdot)$.

זה אלגוריתם פולינומי אם $W_{max} = \text{poly}(n)$.

אבל הימנעו עוד דבר מה:

יהי K פרימטור טיפוסיהמטק. אם נעזר את המטקלים (כלם).
 משהי) מכפולות של K , נקבל $1 + \frac{W_{max}}{K} \geq$ זרימים שאינם:

$$w_i' = \left\lfloor \frac{w_i}{K} \right\rfloor \in \{0, 1, 2, \dots, \left\lfloor \frac{w_{\max}}{K} \right\rfloor\} \quad \text{נשפיר}$$

הסיבוכיות של הרצת האלגוריתם עם הקלט (V, w', V) הוא $O(n^2 \frac{w_{\max}}{K})$.

ומה נשפיר? - נניח שהפיתרון שלט הוא $P \subseteq \{1, \dots, n\}$ והפיתרון האופטימלי לבדיקה המקורית הוא $OPT \subseteq \{1, \dots, n\}$

$$\sum_{i \in P} w_i \geq K \sum_{i \in P} \left\lfloor \frac{w_i}{K} \right\rfloor \geq K \sum_{i \in OPT} \left\lfloor \frac{w_i}{K} \right\rfloor \geq \sum_{i \in OPT} w_i - nK$$

המבצאה תלויה בחירה מוצמדת של K

$$K = \frac{\epsilon w_{\max}}{\eta} \quad \text{נשפיר עבור } \epsilon > 0$$

$$O\left(\frac{n^3}{\epsilon}\right) \quad \text{נקבל - סיבוכיות זמן הריצה:}$$

$$\sum_{i \in P} w_i \geq \sum_{i \in OPT} w_i - \epsilon w_{\max} \geq$$

$$\geq (1 - \epsilon) \sum_{i \in OPT} w_i$$



כלומר, יש לנו אלגוריתם, מקבלת V, w, V, ϵ כ"כ $w_{\max} \geq OPT$

מחזיק ביתרון שזריכו לפחות $(1 - \epsilon) OPT$ בזמן פולינומי ב- n וב- $\frac{1}{\epsilon}$. (זה נקרא סכימת קירוב פולינומית עתה ואין)

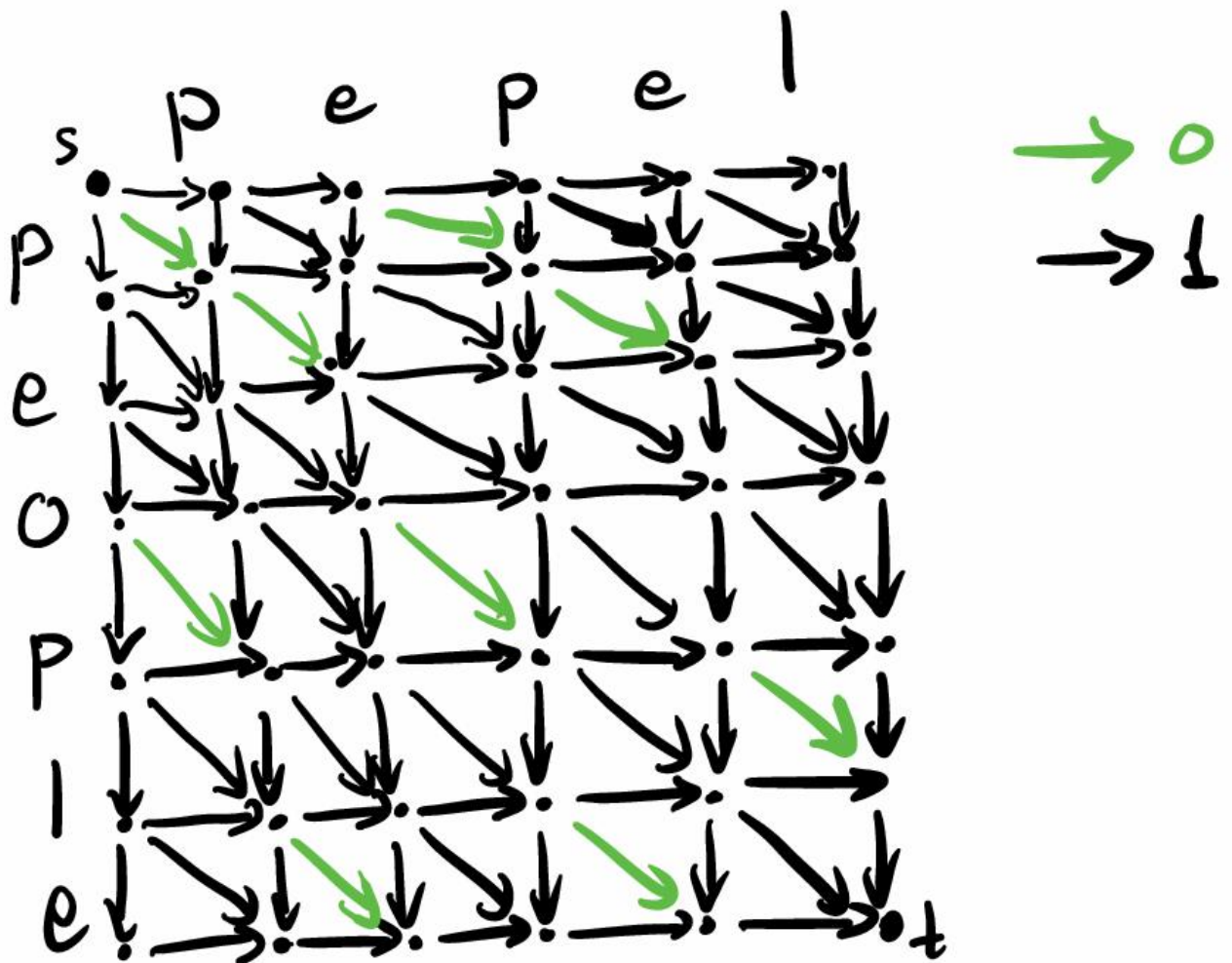
מרחק עיבה

נתונות שתי מחרוזות x, y
 צריך לחשב מהו המספר המינימלי של פעולות
 עיבה שמסד את x ל- y .

פעולות עיבה: מחיקה, הוספת אות, החלפת
 אות באות (לפעמים מוסיפים אלה פעולות מקומיות
 בלבד - זה לא משנה מהונית את הפיתרון).

צאמה: חישוב המרחק בין DNA של אדם
 ל-DNA של סימפנזה.
שאלה: תיזון שגיאות כתיב

היכן הגדול?



נסמן ב- L_x את האורך של x וב- L_y את האורך של y .
 מס' הזמנים: $O(L_x L_y)$
 מס' הקטעים: $O(L_x L_y)$
 האלמנטים של דייוקסטרלה: $O(L_x L_y (\log L_x L_y))$

למספר את הממוצות 0 - N ב- L_x ואת
 הממוצות 0 - M ב- L_y .

מסמל i באתר (i, j) מייצג את
 מרחק המינימלי בין $x[i+1:]$ ל- $y[j+1:]$
 וזה נוסחה רקורסיבית:

$$\text{ed}(x[i+1:], y[j+1:]) = \begin{cases} j & i=0 \\ i & j=0 \\ \min \{ \text{ed}(x[:i], y[j+1:]) + 1, \\ \text{ed}(x[i+1:], y[:j]) + 1, \\ \text{ed}(x[:i], y[:j]) + \chi_{x_i \neq y_j} \} & i \neq 0 \wedge j \neq 0 \end{cases}$$

זו טבלה בעמוד $(L_y + 1)(L_x + 1)$

אני מניח למלאה בזמן $O(L_x L_y)$ כלומר

הזמן באיבר (L_x, L_y) הוא הפיתרון המקסימלי.

סיבוכיות זמן: $O(L_x L_y)$ ביצועים אריתמטיים
(ריבועית בעמוד הקודם)

סיבוכיות מקום: כדי למלא את הטבלה הזו
צריך בטבלה הקודמת. לכן למלא את הטבלה
בסדר עולה של z . למלא, אפשר למלא לפי
עמודות. אז: $O(\min\{L_x, L_y\})$.

(לכן אריתמטי בעמוד הקודם)

הערה: ניתן לחשב את המסלול, כלומר
סדרת פתרונות העריכה, בסיבוכיות זמן
ריבועית או סיבוכיות מקום ליניארית.

אוק?

לסמן ב- $rev(x)$ את המחרוזת ההפוכה- x .

נתון את y עשן חלקים של y_1, y_2 (גודל כמעט שני).

נחשב את $ed(x, y)$ ואת

$$ed(rev(x), rev(y))$$

וגם את השורה האחרונה קטן בחישובים.



טבלה:

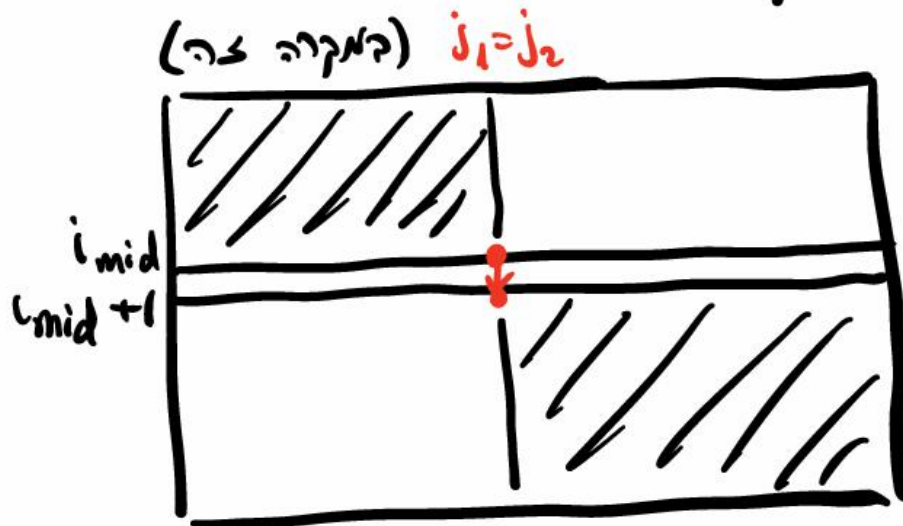
$$ed(x, y) = \min \{ T_{i_{mid}, j_1} + T_{i_{mid}+1, j_2} +$$

$$+ W(i_{mid}, j_1; i_{mid}+1, j_2) :$$

$$\{ (i_{mid}, j_1; i_{mid}+1, j_2) \text{ היא קטנה} \}$$

קטנה $j_1 \leq j_2 \leq j_1+1$

אחרי שמצאנו את j_1 ו- j_2 , מצאנו
 בעזרת עריכה אחת של האלמנטים,
 ואפשר עתה את הקט"ה לשניים:



שימו לב! השטח של הטבלה שבה j_1 לא
 עכשיו הוא $\geq$ חצי משטח הטבלה המקורית.
 הסיבוכיות:

$$c \cdot L_x L_y + c \cdot \frac{1}{2} L_x L_y + \\ + c \cdot \frac{1}{4} L_x L_y + \dots = O(L_x L_y)$$

סיבוכיות המקום מסומה $O(L_x)$
 אם משקים ממלאים במקום שורה $O(L_y)$

מחזור א' ח' א' ח' א'

procedure Bellman ($G = (\{s\}, L_1, \dots, L_{\max}, A), w$):

$d(s) \leftarrow 0$

for $i = 1, 2, \dots, \max$:

for $v \in L_i$:

$d(v) \leftarrow \min_{a=(u,v) \in A} d(u) + w(a)$

$p(v) \leftarrow \arg \min_{a=(u,v) \in A} d(u) + w(a)$

end for

end for

return $d(t), s \rightarrow p(p(\dots(t)) \dots) \rightarrow \dots \rightarrow p(t) \rightarrow t$

היכרות נכונות: באינדוקציה על העברה.

סיבוכיות: $O(|V| + |E|)$ בעזרת אריתמטיקה.

$O(|V|)$ מאי סיבוכיות בלנסוף הקדמ.

אם הקדמ לא כולם רשומים קשתות נכונות
עם צומת, אפשר בקי:

$d(s) \leftarrow 0$; $\forall v \in V \setminus \{s\}, d(v) \leftarrow \infty$

for $i = 0, 1, \dots, \max - 1$:

for $u \in L_i$:

for $a = (u, v) \in A$:

if $d(u) + w(a) < d(v)$:

$d(v) \leftarrow d(u) + w(a)$

הטור דijkstra

$S \leftarrow \emptyset$ קי' S - מחרוזת של נקודות

$\forall x \in S$ קי' $d(x) \leftarrow 0$
 $\forall x \in V \setminus S, d(x) \leftarrow \infty$
 $\forall x \in V, p(x) \leftarrow \text{null}$

כאשר $x \notin S$ ו- $d(x) < \infty$ אז x הוא הנקודה הבאה שיש להוסיף ל- S .

נבדוק: $d(x) + w(x, y) < d(y)$, $(x, y) \in A$, $y \notin S$
 $d(y) \leftarrow d(x) + w(x, y)$
 $p(y) \leftarrow x$

$S \leftarrow S \cup \{x\}$

```

procedure Dijkstra( $G, w$ ):
   $S \leftarrow \emptyset$ ;  $d(s) \leftarrow 0$ ;  $\forall v \in V \setminus \{s\}, d(v) \leftarrow \infty$ ;
   $\forall v \in V, p(v) \leftarrow \text{null}$ 
  while  $\exists v \in V \setminus S$  s.t.  $d(v) < \infty$ :
     $u \leftarrow \underset{x \in V \setminus S}{\text{argmin}} d(x)$ 
    for  $a = (u, v) \in A$  s.t.  $v \notin S$ :
      if  $d(u) + w(a) < d(v)$ :
         $d(v) \leftarrow d(u) + w(a)$ 
         $p(v) \leftarrow u$ 
      end if
    end for
     $S \leftarrow S \cup \{u\}$ 
  end while
  return  $d(t), s \rightarrow \underbrace{p(p(\dots(t)\dots)) \rightarrow \dots \rightarrow p(t)}_{\text{(or null if } d(t) = \infty)}$ 
end procedure

```

אורך $s-t$: קבוצה של קשתות BEA שהיו
 4000 הקשתות היוצאות מ- S חברה $s \in S$
 ו- $t \notin S$.

אירוע של חתום: קבוצה $\{B_1, B_2, \dots, B_k\}$ של
 אירועי $s-t$ שיש להם משקל חיובי $c_1, c_2, \dots, c_k$
 עבורם $e \in A$ $\sum_{i: e \in B_i} c_i \leq w(e)$

דוגמה: עבור G אירוע של חתום $s-t$,
 ו- t הוא מסלול מ- s ל- t .

$$\sum_i c_i \leq \sum_{e \in P} w(e)$$

$$\sum_{e \in P} w(e) \geq \sum_{e \in P} \sum_{i: e \in B_i} c_i =$$

היפוך:

$$= \sum_i |B_i \cap P| \cdot c_i \geq \sum_i c_i$$

$\uparrow$
 כי $|B_i \cap P| \geq 1$

הוכחת נכונות האלגוריתם:

א. $d(s) = 0$ ו- $p(s) = \text{null}$.

ב. נניח $x \neq s$, אם $d(x) < \infty$ אז $p(x) \neq \text{null}$.
 $0 \leq d(p(x)) < d(x)$

ג. נסתכל: $d(t) < \infty$ מסלול מ- s ל- t ש- s ו- t :

$$s = x_0 \rightarrow x_{i_1} \rightarrow x_{i_2} \rightarrow \dots \rightarrow x_{i_k} = t$$

כאשר $i_j = p(x_{i_{j+1}})$ ו- $j = 0, \dots, k-1$

$$\sum_{j=0}^{k-1} w(x_{i_j}, x_{i_{j+1}}) = d(t)$$

קרי: כי

ד. אם יש מסלול מ- s ל- x ש- $d(x) < \infty$ אז $x \in S$.
 הוכחה באינדוקציה על אורך המסלול (מס' הקטנות):
 בסיס האינדוקציה: קצת הראשון מנמיים את s
 ו- $d(s) = 0$.

צעד האינדוקציה: אם יש מסלול מ- s ל- x קאורך $k > 0$, אז ע"י הנחת האינדוקציה הבה y הקודם ל- x במסלול מקיים $d(y) < \infty$ ו- $y \in S$.
 אז, כאשר מנמיים את y ל- x , אז x נכר ב- S (ועל כן $d(x) < \infty$).
 אז ש- $d(x)$ מעודכן כך שהוא קטן מ- ∞ , אז קסלול של דבר x ובלם S .

ה. $s = x_0, x_1, \dots, x_\ell = t$
 סדרת הקודקודים לפי סדר ההכנסה ל- S .

לצורך חתכים עם הקוביות:

$$S_1 = \{x_0\}$$

$$S_i = S_{i-1} \cup \{x_{i-1}\}$$

$$B_i = S_i - S_{i-1}$$

משקיף B_i יהיה $c_i = d(x_i) - d(x_{i-1})$

כל הירידות והעלייה הכוללת

$$\sum c_i = d(t) - d(s) = d(t)$$

כדי להוכיח שכל הירידות חתכים, נחזקן

קלט כלשהי $y \rightarrow x_i$. אם $y = x_j$

עזאי $j < i$, הקשר מהמשתנה האחר.

אם $y = x_j$ עבור $j > i$, אז הקלט

משתנה בחתכים $B_{i+1}, \dots, B_j$

משקיפים הכוללים $d(x_j) - d(x_i)$.

אבל, עם כלל הזדקן מתקיים

$$d(x_j) \leq d(x_i) + w(x_i, x_j)$$

ולכן זה בסדר.

אם $y \notin S$ בסיום היצר העליון, אז

(x_i, y) משתנה בחתכים $B_{i+1}, \dots, B_\ell$

משקיפים הכוללים $d(t) - d(x_i)$

אבל, $d(x_i) + w(x_i, y) \geq d(y) \geq d(t)$ ולכן זה בסדר.

קצרת זרימת פיקוצ' (Fibonacci heap)
 (או זרימת Brodal או rank pairing):
 insert ו-decrease key זולים
 (1) $O(1)$ amortized עם פיקוצ', worst case,
 עם המקנים האחרים)

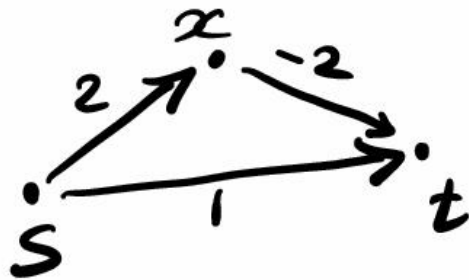
מקבלים $O(m + n \log n)$ בזמנים אריתמטית
 זה זמן ההיציבה הלא קבוע שיצא
 עבור אלה כלים עם קשתות מחושקות
 חיוביות!

סיבוכיות מקום: היארימה דורשת $O(n)$ מספרים
משקלים שליליים

אם יש מספרים $n - t$ שמגיעים למחצה
 שמעקלם הכלל שלילי, אין פיתרון סופי.
 לדעיה (כ) אפשר להסתלק קצת
 כמה שרוצים).

אז נניח שאין מחצה שלילי. קבל.

ד"ר, האלמנטים של דיסטנציה שלם
משל:



ד"ר, אם לכל $x \in V$ מתקיים ש- $d(x)$
הוא עכשיו משקל מסלול קצר ביותר מ- s ל- x
ל- x , אז צעד העדכון הזה:

if $d(x) + w(x, y) < d(y)$:
 $d(y) \leftarrow d(x) + w(x, y)$
 $p(y) \leftarrow x$

משמר את התכונה הזאת.

מה יקרה אם נעביר על כל הקשתות
ונבצע את העדכון הזה? (כמובן, אם
 $d(s) = 0$)

טענה: אם שמסלול קצר ביותר מ- s ל- x שמשתמש
בקשת אחת, אחרי איטרציה אחת ככל $d(x)$
יחזיק את המרחק של x מ- s (משקל המסלול
הזה).

הוכחה: באיטרציה נעביר על הקשת (s, x)

טענה 1: יהי G גרף לא ממונן, $V \in V$, $S \subseteq V$, $d(v)$ הוא רצף היתר.

הוכחה: נוכיח זאת באינדוקציה על מספר התיצובות של d על צמתים.

בסיס האינדוקציה: בהתחלה $d(s) = 0$ וכל $v \neq s$ $d(v) = \infty$ ולכן הטענה בולטת (אפילו ללא צמתים v שונים מאלו). $S = \{s\}$ וכל $v \neq s$ $d(v) = \infty$.

צעד האינדוקציה: נניח שזה נכון לכל S קודם.

נבנה, ונכסיו מודבנים $d(v) \leftarrow d(u) + w(u, v)$.

ע"י השוואת האלמנטים, $d(u) < \infty$ ע"י הנחה.

האינדוקציה, יש מסלול P מ- s ל- u שמקורו

הכלל $w(P) \leq d(u)$ מקיים.

אם נשרה ל- P בסופו את הקטע (u, v)

נקבל מסלול מ- s ל- v שמקורו הכולל

$w(P) + w(u, v) \leq d(u) + w(u, v) = d(v)$ וזה כן סוגר

האינדוקציה ממשיכה להתקיים אם אנו הציגנו. (הן $d(v)$ שונה, מאחר שהכיוון נותר כשהוא).

טעם 2: אם יש מסלול $S-N$ δ - V אזי בסוף
היציג האלגוריתם, $d(v) < \infty$.

הוכחה: האינדוקציה על מספר הקשתות $n(v)$
במסלול קצר ביותר (= מספר קשתות מינימלי).
 $S-N$ δ - V .

בסיס האינדוקציה: עבור $n(v)=0$ חייב להיות
 $V=S$, ולכן $d(s)=0 < \infty$ בסוף היציג האלג.

צעד האינדוקציה: נניח נבנתו עבר u וזהו

$1-i = n(u)$ ונבנה עבר צומת v עבורו $n(v)=i$.

נבחר במסלול P $S-N$ δ - v שאורכו $n(v)$.

$i > 0$ ולכן יש צומת u שקודם δ - v במסלול
זה, כלומר, הקשת האחרונה ב- P היא (u,v) .

$1-i = n(u)$ ולכן ע"י הנחת האינדוקציה $d(u) < \infty$
בסוף היציג האלגוריתם, כפי ש- u מוכרם

תקדמו S באיזשהי איטרציה של פולסות

ה- $while$, והזמן זה $d(u) < \infty$. אם

$d(v) = \infty$ האלי הזמן, אז $v \notin S$ ולכן

מחברים P $d(v) \leftarrow d(u) + w(u,v)$ ולכן החל מחדש

זה $d(v) < \infty$.

לעמוד 3: עקב כל צומת $v \in V$ הסיום היציג
האלץ $d(v)$ הוא משקל מסלול קל ביותר מ- s - v
ע- v , ו/או $v \neq s$ יש מסלול כזה שמסתיים
בקשת $(p(v), v)$. (עבור $p(s) = null, v = s$)

הוכחה: נבדוק במצב הסיום היציג האלץ.
אם $d(v) = \infty$ אז יפני לעמוד 2 אין מסלול
מ- s ע- v וזה כן לעמוד 3 מתקיימת לפי v .
אחרת, יפני לעמוד 1 יש מסלול מ- s ע- v
שמעקבו יפני האלץ $d(v)$.

כדי להוכיח את הטענה זקוק $d(v) < \infty$,
נשים לב שהסיום היציג האלץ (האחרון)

$$S = \{v \in V : d(v) < \infty\}$$

הסימון הבא: $S = \{v_1, v_2, \dots, v_k\}$

באשר סדר האינדקסים הוא סדר ההכלמה

$$S_i = \{v_1, \dots, v_i\}, \quad (v_1 = s)$$

$d_i(v)$ הוא הערך של $d(v)$ כאשר מכניסים
אלו v_i ע- S , ו- $p_i(v)$ הוא הערך של $p(v)$
האלץ שמו.

נוכיח האינדוקציה על i את הטענה

המרחקת הבאה: (א) לכל $v \in S_i$ מתקיים

כי $d_i(v)$ הוא משקל מסלול קל

היות $S-M$ $\delta-v$, 1 - $(p(v), v)$ היא
 קשת אחרונה במסלול כזה. $(p(v), v) \notin S_i$
 מתקיים כי $d_i(v)$ הוא מסלול מסוג
 קף היות $S-M$ $\delta-v$ שואר רק
 דרך צמתים S_i - 1 - $(p(v), v)$
 היא קשת אחרונה במסלול כזה.

בסיום האינדוקציה: $i=1$. הטענה נכונה עבור
 האינדוקציה של i כי $d \equiv d_1$ - 1 - $p \equiv p_1$
 והעקבה $S_1 = \{S\}$.

צעד האינדוקציה: נניח לבואר עבור $i-1$
 ונוכיח עבור i .

אם v_i הנתת האינדוקציה, $d_i(v_i) = d_{i-1}(v_i)$
 הוא מסלול מסוג קף היות $S-M$ $\delta-v_i$
 שואר רק דרך צמתים S_{i-1} - 1 - S .
 אם כן אז $d_i(v_i) = d_{i-1}(v_i)$ קף היות $S-M$ $\delta-v_i$
 הוא מסלול מסוג קף היות $S-M$ $\delta-v_i$
 צמתים מחוץ ל- S_{i-1} , שאינם v_i . יהי
 v צומת ראשון כזה שלא היה במסלול.
 אם $d_i(v) \geq d_{i-1}(v)$, v_i בחירת
 קף במסלול $S-M$ $\delta-v$ הוא מסלול
 קף היות $S-M$ $\delta-v$, והוא שואר רק

ואם כן $d_i(v) = d_{i-1}(v)$ / נשמרת למצמ
 האינדוקציה המקרה זה. אם כל מסלול
 קם ביותר מ- s - δ v שזוהי רק דרך
 צמתים מ- S_i חייב לעבור דרך v_i ,
 הקשת האחרונה במסלול כזה חייבת
 להיות (v, v_i) . אחרת, קשת אחרונה
 במסלול כזה היא (v, v_j) עבור
 $i < j$, אבל מסלול קם ביותר מ- s - δ v_j
 לא עובר דרך v_i אלא רק דרך צמתים
 ב- S_{j-1} , ואם כן יש מסלול קם
 ביותר מ- s - δ v שזוהי רק דרך
 צמתים מ- S_i ואינו עובר דרך v_i .
 במקרה זה, אם v_i הנחת האינדוקציה
 לאי. $d_{i-1}(v)$ מתקיים כי
 $d_{i-1}(v_i) + w(v_i, v) < d_{i-1}(v)$
 כן מתקיים עדיין שמשמר את
 למצמ האינדוקציה.

נתון גרף $G = (U, V, E)$.

עבור קבוצת צמתים $U' \subseteq U$, נסמן $N(U')$ את קבוצת הצמתים $(V - U)$ השכנים ל- U'

שידוך הוא קבוצה של קשתות $M \subseteq E$ כך שכל צומת של G טעון לכל היותר קשת אחת מ- M .

שידוך F הוא מנטלם אם $|M| = |U|$.

משפט Hall: יש ב- G שידוך מנטלם אם ורק אם $|N(U')| \geq |U'|$, $U' \subseteq U$.

הוכחה: הכיוון $\Leftarrow$ טריוויאלי.

נבחר את הכיוון $\Rightarrow$: יהי M שידוך מקסימאלי. נניח בעזרה שאין מנטלם. בפרט, יש $x \in U$ שאינו משויך.

נדדיר: מסלול פשוט שבו הקשתות הן עסייובין M ו- $E \setminus M$ ו- M זקרא מסלול מתחלף.

ניתבונ קאוסל המסלולים המתחלפים

x - הוא קצה אחד שלהם.
 נסמן ב- U' את צמת u (כולל x)
 שמתקיים במסלולים הללו וק- V' את
 צמת V שמתקיים במסלולים הללו.
 ע"פ הנחת המקסימליות של M , לא
 ייתכן מסלול מתחיל שאי אפשר להאריך
 שקצהו השני ק- V' , כי אז יש
 בו יותר קשתות לא ק- M מאשר
 ב- M ואפשר להגדיל את השידוק
 ע"י החרפה:

$x \cdot \text{---} \cdot \text{---} \cdot y \in V'$
 (נזכור את הקשתות הכתולות מ- M
 ונכניס את הקשתות האדומות)
 מסקנה: כל צמת V' מחזיקים עצמות
 ב- U' .
 כל צמת זגל U' מחזיקים
 עצמת V' .

לכן $|V'| = |\{u, v\}| = 2$ או $|V'| > |U'|$

אבל, אם קיים $u \in U'$ ו- $v \notin V'$

עבור $\{u, v\} \in E$, אז ניתן לקחת

מסלול מתחיל ב- u ונראה כי אולי

קיימת הקשת $\{u, v\}$ וזו סתירה לבנייה

של U' ו- V' . כנראה, $N(U') \subseteq V'$.

כבר, הקבוצה $U' \subseteq U$ מכילה את

התנאי של משפט Hall, משום

ג- $|U'| > |V'| \geq |N(U')|$

הערה: ניתן להפוך את ההוכחה של משפט

Hall לאמצעי יחס שמוצא ש'דוק' מושגם

או קב' U' מכילה את התנאי של המשפט.



נתחיל משידוק M בין אלגוריתם אלו באיטרציות.
בכל איטרציה:

נחיל פרוצדורה MIN BFS החל $x-N$, שהוא
הצומת היחיד בענף 0. משכבה x גלית M ונת
להתקדם בין דרך קשתות לא M ובענף
אי גלית ממנו להתקדם בין דרך קשתות M -
(כבר), הקשתות בין ענף $u-z$ בענף z
מבנות x -שידוק של M , ונת השידוקים
האלו עברו z -ים שאינם הם z (חיים).

שימו לב ש- G הוא צבאי ולכן על יבולה להיות
קשת בין שני צמתים האותה שכבה.

אם מסיים פרוצדורה y בענף x גלית
שממנו אין דרך להמשיך בענף התאה, אז
כל מסלול $x-N$ y קצר והענף של y
הפרוצדורה הוא מסלול מתחיל ממתחיל ומסתיים
זה קשת לא M , ולכן מאפשר להעביר את
 $|M|$ באתר (x) תחלופת הקשתות לא בין התחיל.

א/חית, הצמתים בשכבות האי-זוגיות
 מהווים את קבוצת כל השכבות של
 הצמתים בשכבות האי-זוגיות. כיוון שלכל
 צומת בשכבה אי-זוגית, קומט x , מצויים
 צ'ק קטת השידוק M , מספר הצמתים
 בשכבות האי-זוגיות (כולם x) גדול $k-L$
 ממספר הצמתים בשכבות האי-זוגיות, ולכן
 הצמתים בשכבות האי-זוגיות הם קבוצה
 U שמכילה את תת-ה $Hall$.

סיבוכיות זמן: לכל היות $|U|$ אי-זוגית,
 כל פרוצדורה זמנית BFS , סה"כ:
 $O(m + n^2)$ פעולות אריתמטיות

סיבוכיות מקום: $O(m + n)$ (אולי הקטן)
 סימונים על הצמתים והקשתות מספרים

procedure Hall ($G=(U,V,E)$):
mark x as unmatched $\forall x \in U \times V$
 $M \leftarrow \emptyset$

while $\exists$ unmatched $x \in U$:

$y, P \leftarrow \text{alt_BFS}(x, M, G)$

if $y = \text{null}$:

return failure, M

else:

$M \leftarrow (P \setminus M) \cup (M \setminus P)$

mark x, y as matched

end if

end while

return success, M

end procedure

```

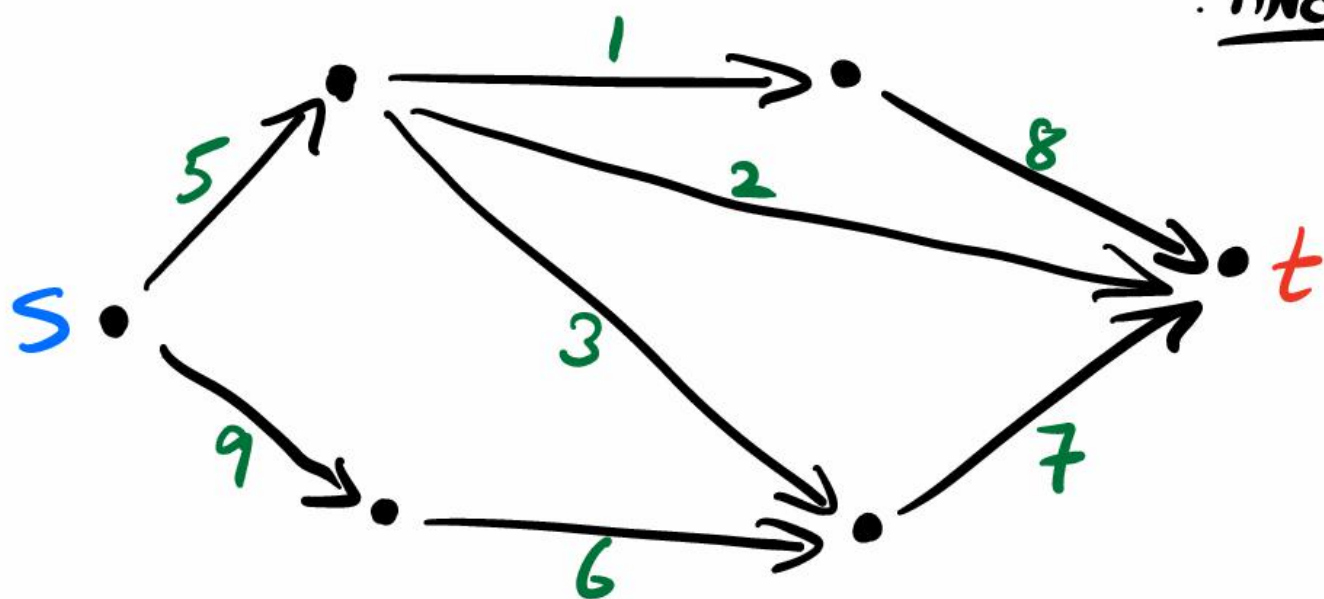
procedure alt-BFS( $x, M, G$ ):
  mark  $u$  as unvisited  $\forall u \in U(G) \cup V(G)$ 
  queue  $\leftarrow x$ 
  level( $x$ )  $\leftarrow$  even
   $p(x) \leftarrow$  null
  while queue  $\neq$  empty:
     $u \leftarrow$  dequeue(queue)
    if level( $u$ ) = even:
      for  $v \in N_E(G) \setminus M^{(u)}$ :
        if  $v$  is unvisited:
          level( $v$ )  $\leftarrow$  odd
           $p(v) \leftarrow u$ 
          enqueue( $v$ , queue)
        end if
      end for
    else if  $\exists$  unvisited  $v$  st.  $\{u, v\} \in M$ :
      level( $v$ )  $\leftarrow$  even
       $p(v) \leftarrow u$ 
      enqueue( $v$ , queue)
    else
      return  $u, \underbrace{\{x, \dots, \{p(u), u\}\}}_P$ 
    end if
  end while
  return null,  $\emptyset$ 
end procedure

```

צרימה קרשת

רשת צרימה היא רביעית (G, c, s, t)
 ובה: G גרף סופי מכ"ן, $c: E(G) \rightarrow \mathbb{N}$,
 פונקצית קיבול חלופית, $s, t \in V(G)$, ונקודות
 מקור (s) ונקודת יעד (t) .

דוגמה:



צרימה קרשת (G, c, s, t) היא פונקציה

$$f: E(G) \rightarrow \mathbb{R}$$

שמקיימת:

(1) (שימור הצרימה) לכל $x \in V(G) \setminus \{s, t\}$,

$$\sum_{e=(y,x) \in E(G)} f(e) = \sum_{e=(x,y) \in E(G)} f(e)$$

הצרימה הנכנסת ל- x
 שווה ל- x הצרימה היוצאת
 מ- x

(2) (אזעוז קיבול) לכל $e \in E(G)$, $0 \leq f(e) \leq c(e)$

בהינתן זרימה f , הזרם שמה $|f|$ הוא:

$$|f| = \sum_{e=(s,x) \in E(G)} f(e) - \sum_{e=(x,s) \in E(G)} f(e)$$

כל הזרימה היוצאת מ- s פחות הזרימה הנכנסת ל- s .

תכונות של זרימה

טענה: יהי $A \subseteq E(G)$ חתך s - t שלמה. $t \notin A$.
 קבוצה $S \subset V(G)$ שקורה $s \in S$ ו- $t \notin S$. יהי
 B קבוצת הקשתות הנכנסות ל- S מ- S^c ו- $V(G)$.

$$|f| = \sum_{e \in A} f(e) - \sum_{e \in B} f(e)$$

הזרימה נטו של אדי החתך

$$|f| = \sum_{e=(x,t) \in E(G)} f(e) - \sum_{e=(t,x) \in E(G)} f(e)$$

מסקנה:

(הזרימה שיוצאת מהמקור מסיימת לנקודה)

$$\sum_{e \in A} f(e) - \sum_{e \in B} f(e) = \quad \text{ה/כחיה:}$$

$$= \sum_{u \in S} \sum_{e=(u,v) \in E(G)} f(e) - \sum_{v \in S} \sum_{e=(u,v) \in E(G)} f(e)$$

השילוב מתייחס כי קצת מ'ן כולל ים
 י'ן קטע פ' קצת א'ו' פ' ח'ו' ק-2
 ק' $e \in A$ נ'ל' $e \in B$
 ק' ע' ס' מ' ח'ו' . ק' $e \in B$
 נ'ל' ק' ע' ס' מ' ח'ו' . ק' $e \in B$
 ע' ק' ח'ו' ק-2 מ' ח'ו' ע' ח'ו' $e \in B$
 ע' ע' ח'ו' מ' ח'ו' $e \in B$ $e \in B$ $e \in B$

$$\sum_{u \in S} \sum_{e=(u,v) \in E(G)} f(e) - \sum_{v \in S} \sum_{e=(u,v) \in E(G)} f(e) =$$

$$= \sum_{e=(s,v) \in E(G)} f(e) - \sum_{e=(v,s) \in E(G)} f(e) +$$

$$+ \sum_{\substack{x \neq s \\ x \in S}} \left(\sum_{e=(x,v) \in E(G)} f(e) - \sum_{e=(v,x) \in E(G)} f(e) \right)$$

$= 0$

כל צומת שיש לו יציאה ויציאה
הצומת הזה

$$= \sum_{e=(s,v) \in E(G)} f(e) - \sum_{e=(v,s) \in E(G)} f(e) = |f|$$

למשפט: נתון בחינה של צומת v
החלקה
 $V \setminus \{t\}, \{t\}$

A = קב' הקטמת סוכנוסות t

B = קב' הקטמת סוכנוסות t

$$|f| = \sum_{e=(x,t) \in E(G)} f(e) - \sum_{e=(t,x) \in E(G)} f(e)$$

דבר קבוצה $A \subseteq E(G)$, ω :

$$c(A) = \sum_{e \in A} c(e)$$

טענה: לכל חתך $s-t$ $A \subseteq E(G)$ וכל זרימה חוקית f ב- G , $|f| \leq c(A)$

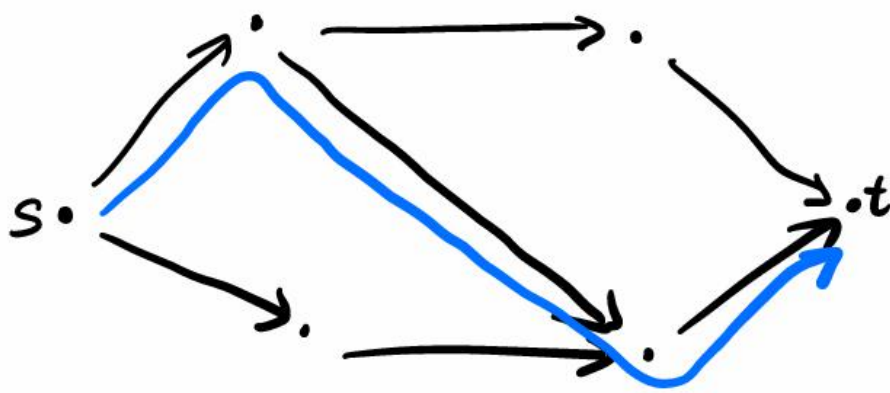
הוכחה: ע"י הטענה הקודמת, $|f| \leq \sum_{e \in A} f(e)$.
מצד שני, ע"י איכות הקיבול, לכל $e \in A$, $f(e) \leq c(e)$.

רשת פירוק

נתונה רשת זרימה $N = (G, c, s, t)$ וזרימה חוקית f .
הרשת $N_f = (G_f, c_f, s, t)$ היא רשת פירוק של N ו- f .
שאיפת את הקיבול הנותר ב- N אחרי העברת הזרימה f .

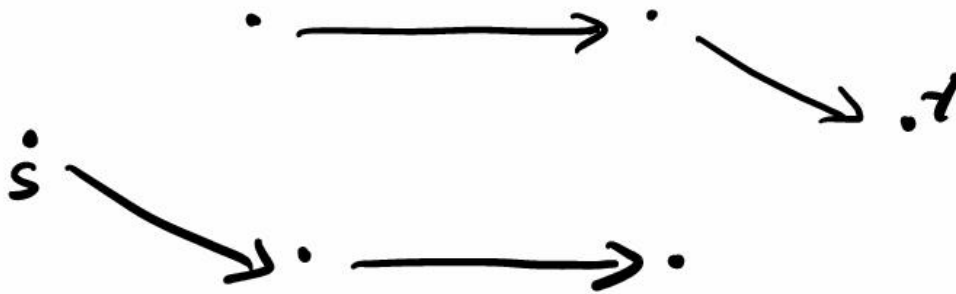
$$c_f(e) = c(e) - f(e), \quad G_f = G$$

ניסיון ראשון:



צפייה: $\forall e, c(e) = 1$

→ צפייה $c(e) = 1$

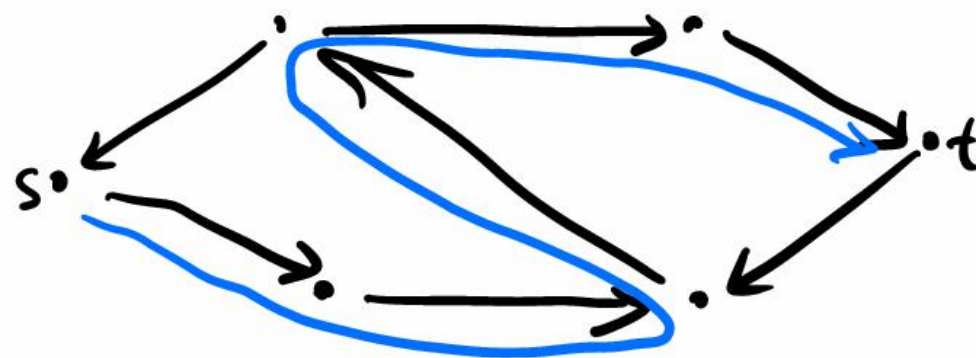


כדי להעביר כאן חץ ציפה צריך למצוא מסלול
הציפה הקיימת. זה דומה "לשלב חזרה" ציפה
שהוא חזרה

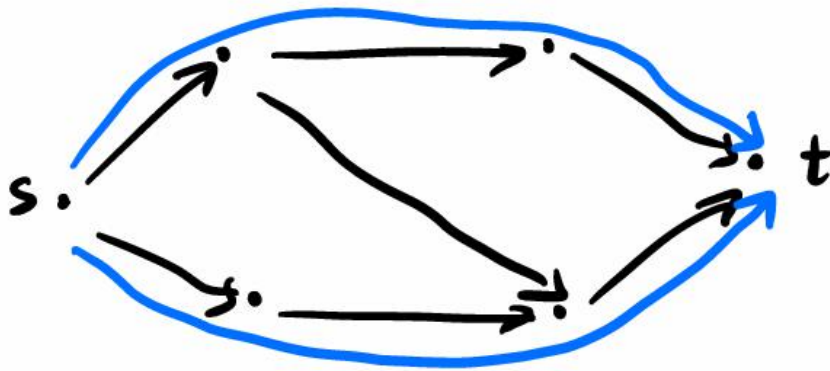
הישתתפות!

G_f

→ צפייה $c(e) = 1$



הצורה הכללית נראית כך:



לשם פשטות:

- א. נתיב קטנות עם קיבול 0
- ב. אם $(u, v) \in E(G)$ אזי $(v, u) \in E(G)$
- ג. אם $c(u, v) > 0$ אז $c(v, u) = 0$

ניתן להתייחס רשת זרימה כרשת שמתחברת
אלהם הן כללית לא שוללת את הערך של זרימה מקסימום

השדרה: הרשת השלולה $N_f = (G_f, c_f, s, t)$
מקיימת:

$$G_f = G \text{ וכל } (u, v) \in E(G)$$

$$\text{אם } f(u, v) > 0$$

$$c_f(u, v) = \begin{cases} c(u, v) - f(u, v) \\ f(v, u) \\ c(u, v) \end{cases}$$

$$\text{אם } f(v, u) > 0$$

אלוהי

משפט: תהי f פונקציה חלקית ב- N ו- f' פונקציה חלקית ב- N_f (עבורה אם $f'(u,v) > 0$ אם $f'(v,u) = 0$).
 אזי $f + f' : E(G) \rightarrow \mathbb{N}$ מוגדרת כן:

$$(f + f')(u,v) = \begin{cases} f(u,v) + f'(u,v) - f'(v,u) & \text{אם } f(u,v) > 0 \\ 0 & \text{אם } f(v,u) > 0 \\ f'(u,v) & \text{אחרת} \end{cases}$$

אזי $f + f'$ היא פונקציה חלקית ב- N וזהו
 האיבר $|f + f'| = |f| + |f'|$

הוכחה: איננו בקושי -
 תהי $(u,v) \in E(G)$ קשת.
 אם $f(u,v) > 0$ אז $c_f(u,v) = c(u,v) - f(u,v)$

$$f'(u,v) \leq c(u,v) + f(u,v) \quad , \rho \delta$$

$$(f+f')(u,v) = f(u,v) + f'(u,v) - f'(v,u) \leq \quad , \rho \delta$$

$$\leq f(u,v) + c(u,v) - f(u,v) = c(u,v)$$

$$(f+f')(u,v) = 0 \leq c(u,v) \quad \text{since } f(v,u) > 0 \quad \text{and}$$

$$c_f(u,v) = c(u,v) \quad , \text{otherwise}$$

$$(f+f')(u,v) = f'(u,v) \leq c_f(u,v) = c(u,v) \quad , \rho \delta$$

סיכום הוכחה:

$$u \in V(G) \setminus \{s, t\}$$

$$\sum_{v: (u,v) \in E(G)} (f+f')(u,v) - \sum_{v: (v,u) \in E(G)} (f+f')(v,u) =$$

$$= \sum_{v: f(u,v) > 0} (f(u,v) + f'(u,v) - f'(v,u)) + \sum_{v: f(u,v) = f(v,u) = 0} f'(u,v) -$$

$$- \sum_{v: f(v,u) > 0} (f(v,u) + f'(v,u) - f'(u,v)) - \sum_{v: f(v,u) = f(u,v) = 0} f'(v,u) =$$

$$= \boxed{\sum_{v: (u,v) \in E(G)} f(u,v) - \sum_{v: (v,u) \in E(G)} f(v,u)} +$$

$$+ \boxed{\sum_{v: (u,v) \in E(G)} f'(u,v) - \sum_{v: (v,u) \in E(G)} f'(v,u)}$$

$\square = 0$ f ש"מ. הסימטה f

$\square = 0$ f' ש"מ. הסימטה f'

רק הסימטה :

$$|f+f'| = \sum_{v: (s,v) \in E(G)} (f+f')(s,v) - \sum_{v: (v,s) \in E(G)} (f+f')(v,s) =$$

$$= \sum_{v: f(s,v) > 0} (f(s,v) + f'(s,v) - f'(v,s)) + \sum_{v: f(s,v) = f(v,s) = 0} f'(s,v) -$$

$$- \sum_{v: f(v,s) > 0} (f(v,s) + f'(v,s) - f'(s,v)) - \sum_{v: f(v,s) = f(s,v) = 0} f'(v,s)$$

$$= \sum_{v: (s,v) \in E(G)} f(s,v) - \sum_{v: (v,s) \in E(G)} f(v,s) +$$

$$+ \sum_{v: (s,v) \in E(G)} f'(s,v) - \sum_{v: (v,s) \in E(G)} f'(v,s) =$$

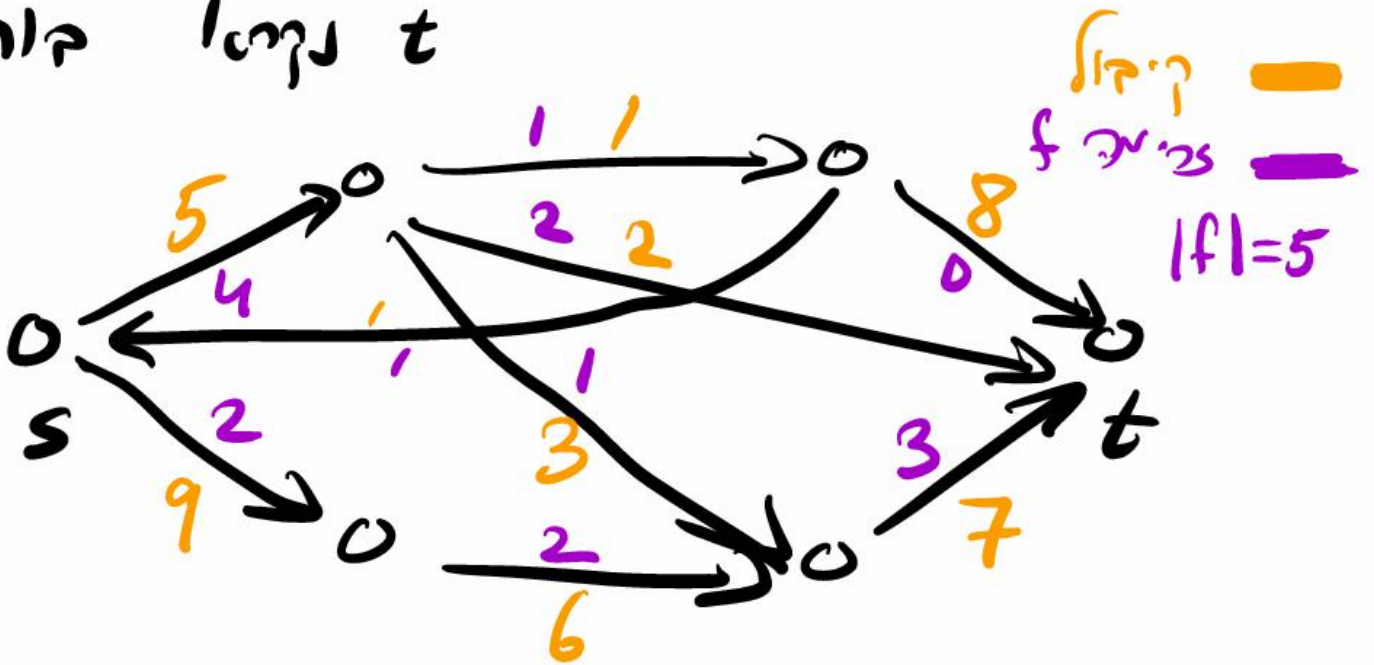
$$= |f| + |f'|$$

צרימה דיסטית

רשת צרימה היא רביעית (G, c, s, t)
 ובה: G גרף סופי מכוון

$c: E(G) \rightarrow \mathbb{N}$ פונקציית קיבול
קוויבית

$s, t \in V(G)$: s נקודת מקור
 t נקודת בור



צרימה דיסטית (G, c, s, t) היא פונקציה
 $f: E(G) \rightarrow \mathbb{R}$ ממקיימת:

(1) $x \in V(G) \setminus \{s, t\}$ (שני צימנים) $\sum_{e=(x,y) \in E(G)} f(e) = \sum_{e=(y,x) \in E(G)} f(e)$

$$\sum_{e=(x,y) \in E(G)} f(e) = \sum_{e=(y,x) \in E(G)} f(e)$$

(2) $e \in E(G)$ (צירוף) $0 \leq f(e) \leq c(e)$

ההינתן f בהסת צימנה (G, c, t) הצורך שיהיה $|f|$ מלאכה "ח" :

$$|f| = \sum_{e=(s,x) \in E(G)} f(e) - \sum_{e=(x,s) \in E(G)} f(e)$$

תכונות של צימנה : $A \subseteq E(G)$ יהי

חלק $s-t$ מלאכה "ח" קבוצה $S \subseteq V(G)$
 גבולה $s \in S$ ו- $t \notin S$. כלומר ,
 $A = E(G) \cap S \times V \setminus S$. יהי $B \subseteq E(G)$ קב'

הקטטה
כח/כח

$V \setminus S \rightarrow S$ שכל מה ש- S לא מכיל

$B = E(G) \cap (V \setminus S) \times S$

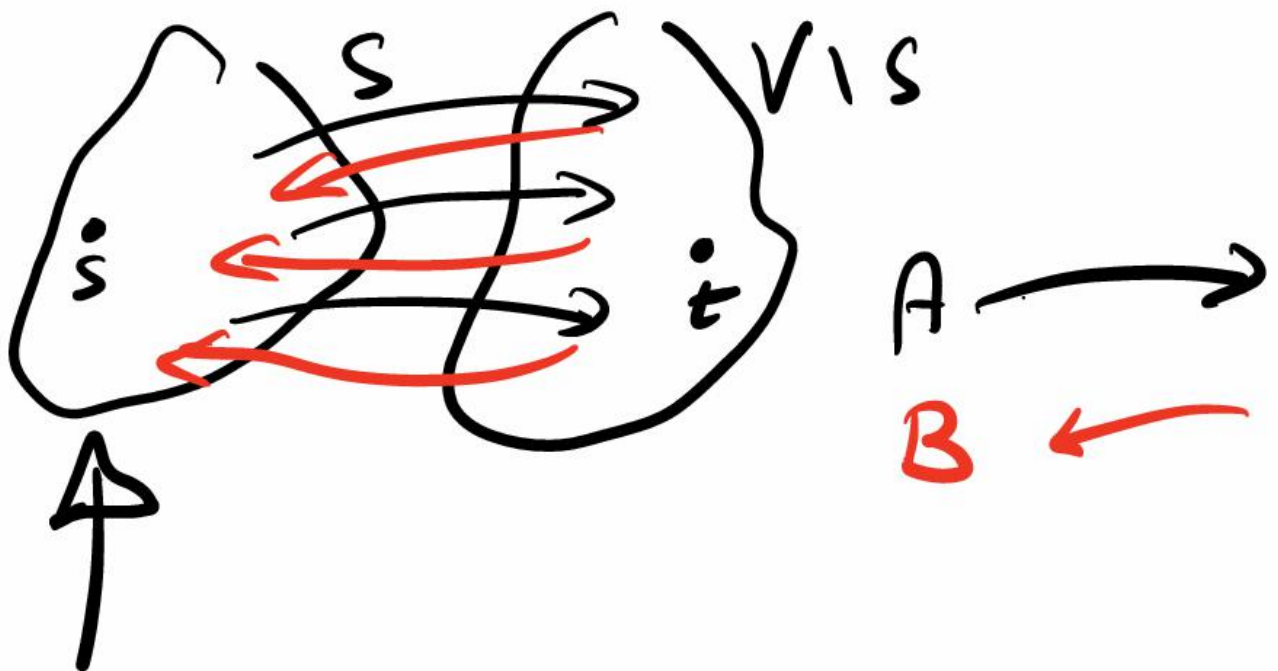
כח/כח

$$|f| = \sum_{e \in A} f(e) - \sum_{e \in B} f(e)$$

הכח/כח של f הוא

כח/כח של f הוא $|f|$ מקיימת שכל s ו- t כח/כח

$V \setminus \{s, t\}$ $S = \{s\}$ t כח/כח



$$\sum_{e \in A} f(e) - \sum_{e \in B} f(e) = \text{ה/כחה:}$$

$$= \sum_{u \in S} \sum_{e=(u,v) \in E(G)} f(e) - \sum_{v \in S} \sum_{e=(u,v) \in E(G)} f(e)$$

השילוב מתקיים כי קצת מן נולד ים
 קי קטע פתח קצת פתח קצת
 קטע $e \in A$ נולד
 קי קטע פתח קצת פתח קצת
 נולד קי קטע פתח קצת פתח קצת
 קטע פתח קצת פתח קצת
 קטע פתח קצת פתח קצת
 קטע פתח קצת פתח קצת

$$\sum_{u \in S} \sum_{e=(u,v) \in E(G)} f(e) - \sum_{v \in S} \sum_{e=(u,v) \in E(G)} f(e) =$$

$$= \sum_{e=(s,v) \in E(G)} f(e) - \sum_{e=(v,s) \in E(G)} f(e) +$$

$$+ \sum_{\substack{x \neq s \\ x \in S}} \left(\sum_{e=(x,v) \in E(G)} f(e) - \sum_{e=(v,x) \in E(G)} f(e) \right)$$

$= 0$

כל צומת שיש לו יציאה ויציאה
הצומת הזה

$$= \sum_{e=(s,v) \in E(G)} f(e) - \sum_{e=(v,s) \in E(G)} f(e) = |f|$$

למשפט: נתבונן בחתך
החתך
 $V \setminus \{t\}, \{t\}$

A קב' הקטמת סוכנוסות

B קב' הקטמת סוכנוסות

$$|f| = \sum_{e=(x,t) \in E(G)} f(e) - \sum_{e=(t,x) \in E(G)} f(e)$$

(הצורה היא סימטרית $s-t$)
 הצורה היא סימטרית $t-s$

הצורה: $A \subseteq E(G)$ וזהו $s-t$ פתרון
 $c(A) = \sum_{e \in A} c(e)$ - ב

למה: אם $s-t$ פתרון $A \subseteq E(G)$
 וזהו $s-t$ פתרון f בקשת (G, c, s, t)
 מתקיים $|f| \leq c(A)$

הוכחה: "אם" הוכחה בקלות,

$$|f| = \sum_{e \in A} f(e) - \sum_{e \in B} f(e) \leq \sum_{e \in A} f(e)$$

אם $f(e) \leq c(e)$, $e \in E(G)$, אז

$$|f| \leq \sum_{e \in A} f(e) \leq \sum_{e \in A} c(e) = c(A), \text{ אכן}$$

שיטת Ford-Fulkerson :

נסמן ב- G_f^+ את הגרף המתקבל מ- G אחרי הסרת כל e עבורם $c_f(e)=0$.
איתחול: f היא זרימה שזרימה 0 על כל קשת

איתחול: נמצא ב- G_f^+ מסלול מכון s ל- t .

$$f'(u,v) = \begin{cases} \min_{e \in P} c_f(e) & (u,v) \in P \\ 0 & \text{אחרת} \end{cases}$$

ק נקרא
מסלול משה

נחשף את f ב- $f+f'$

תגלית: ב- G_f^+ אין מסלול מכון s ל- t

משפט: בסיום, f היא זרימת מקסימום ב- G .

הוכחה: נסמן ב- S את קבוצת הצמתים ש.

ב- G_f^+ מסלול מ- s אל t . קולא $s \in S$ ו

פ. תגלית הסיום $t \notin S$. עכן,

$$A = \{(u,v) : (u,v) \in E(G) \wedge u \in S \wedge v \in V \setminus S\}$$

הוא מת $s-t$.

$$B = \{(v,u) \in E(G) : u \in S \wedge v \in V \setminus S\}$$

$$A \subseteq E(G), \text{ אכן } A \cap E(G_f^+) = \emptyset$$

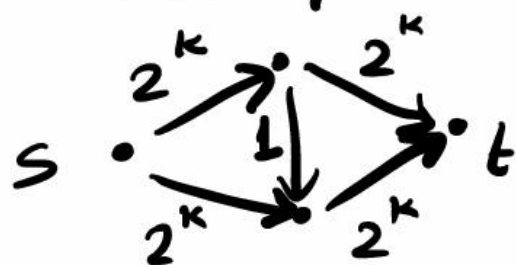
$$\text{כל } (u,v) \in A \text{ ואם } f(u,v) = c(u,v) \text{ אז } f(v,u) = 0$$

$$|f| = \sum_{(u,v) \in A} f(u,v) - \sum_{(v,u) \in B} f(v,u) = c(A) \geq |g| \quad \text{עכ"ל,}$$

עכ"ל זרימה חוקית g .

כמה איטרציות צריך לעצור? - בהנחה שהקבוצות N - שלמים והזרימה f היא בשלמים (כל זיג עם קשת הוא שלם), אם הקבוצות N_f שלמים, למק הזרימה f' היא בשלמים והזיג $f+f'$ הוא בשלמים. $|f+f'| \geq |f| + 1$.

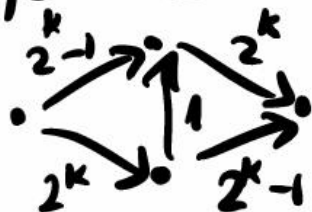
אם f^* זרימת מקסימום, אז מט' האיטרציות הוא לכל היותר $|f^*|$.



דוגמה:

זרימת מקסימום היא 2^{k+1} .

אם נגדיר זרימה דרך הקשת עם קיבול 1, נגדיל את הזרימה ב-1 ונקבל רשת שאינה



אנחנו עושים עמשים להמשיך כך עד שנקבל זרימת מקסימום - $|f^*|$ איטרציות.

אלהם גורם הקלט הוא $(f^* | f | g) O$ אז זה
לא אלקאריטם בולטואל:

מסקנה: אם הקידומים שמים ש ברימור מקסימום בעלות

האלקאריטם של Edmonds - Karp

זה מימוש ספציפי של שיטת פורד-בלקרוסין.
ברשת השילוח נמצא מסלול משפר קצה
ביותר (מס' קשתות מינימלי) - אנשה ליישם
בעזרת BFS בזמן $O(m+n)$ (מספר
הקשתות ברשת השילוח הוא לכל היותר $2m$)

משפט: נדרש $O(mn)$ איטרציות

הוכחה:

עבור ארץ H נסמן d_H את פונקציות
המרחק בין קודקודים H - H (# הקשתות במסלול
קצר ביותר).

תהי f_0 זרימה פוטנציאלית G - G שמועדה במהלך
יציאת האלקאריטם, ותהי $f_1 = f_0 + f'_0$
(כלומר, אחרי השיפור בעזרת N_{f_0})
יהי $v \in V$. נוכיח באינדוקציה על $d_{G_{f_1}}^+(s, v)$
ש - $d_{G_{f_1}}^+(s, v) \leq d_{G_{f_0}}^+(s, v)$:

בסיס האינדוקציה: $d_{G_{f_0}^+}(s, s) = 0 = d_{G_{f_1}^+}(s, s)$

3 האינדוקציה: יהי p מסלול קצה ביותר
 $s - v - \delta - \gamma - k - G_{f_1}^+$ (כלומר, מסלול שאורכו
 $(d_{G_{f_1}^+}(s, v))$ יהי. (u, v) הקטת האחרונה
 במסלול זה. אם $(u, v) \in E(G_{f_0}^+)$ אזי

$$d_{G_{f_0}^+}(s, v) \leq d_{G_{f_0}^+}(s, u) + 1 \leq \underset{\substack{\uparrow \\ \text{נחת האינדוקציה}}}{d_{G_{f_1}^+}(s, u)} + 1 =$$

$$= d_{G_{f_1}^+}(s, v)$$

אחרת, חייב להיות $(v, u) \in E(G_{f_0}^+)$ וכמו
 כן המסלול $\delta - \gamma - u$ מכילים כרימה $k - G_{f_0}^+$
 עולה צינן קטת u . זהו מסלול קצה ביותר,

$$d_{G_{f_0}^+}(s, v) = d_{G_{f_0}^+}(s, u) - 1 \leq \underset{\substack{\uparrow \\ \text{נחת האינדוקציה}}}{d_{G_{f_1}^+}(s, u)} - 1$$

$$\leq d_{G_{f_1}^+}(s, v) - 2 \quad (*)$$

הניתוח הזה מראה אמתם δ ו/או צדד $k - N$:

הכל איטרציה של שיטת פורד-בלקורסון.
 ישנה פסגה קשת אחת e עם זוגי המסלול
 המספר p שנעממת מהקשת השלישית כ.
 $f'(e) = c_f(e)$ (כל קשת e עם קיבול
 מוגבל היא כזו).

נתבונן באינצקה קשת (u, v) שנעממת באיטרציה
 ה- k של Edmonds-Karp, נניח ברשת N_f .
 כדי שהיא תחזיר את v , צריך להיכנס אליה
 יותר מ-1 פעם. הקשת (v, u) , נניח ברשת N_{f_0} .

נסמן את הרשת השלישית האחרונה בצורה N_{f_1} .

$$d_{G_{f_1}}^+(s, v) \geq d_{G_{f_0}}^+(s, v) + 2 \geq d_{G_f}^+(s, v) + 2 \quad (*)$$

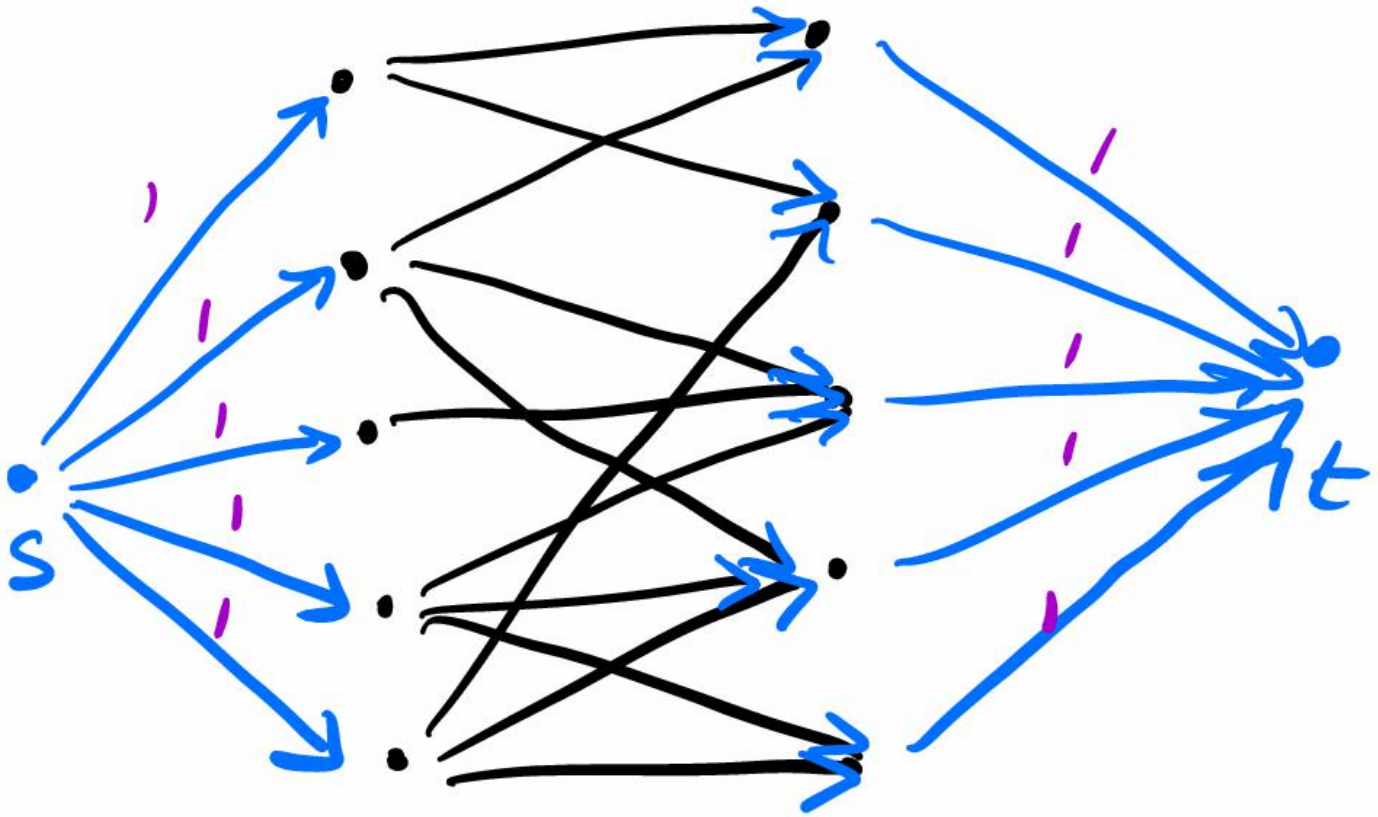
$\uparrow$ (כניסה) $\uparrow$ מוגבלות

בנוסף, כל פסגה שהקשת (u, v) חוצת ומאליה
 ברשת השלישית אחרי שנעממה, מחזיק $N-S$
 v - u בדף 2 לפחות. מחזיק כזה הוא בין
 1 - $n-1$ (אם $v = s$ הקשת (s, u) לא נעממה
 בעצם). כל איטרציה נעממת קשת. עקב זה

האיטרציה הראשונה שבה (u, v) חוצת $N-S$ היא $m \cdot \frac{n-1}{2}$.

סיכומים: האלגוריתם: $O(m^2)$ בעלות אריתמטיות.

שידוך קטן 3-3 ::



כל שידוך מתאים עצומה בשלמים מוכה
 זהה יסודי השידוך וכל צרימה בשלמים
 מתאימה לשידוך שגודלו זהה לערך הצרימה.

מסלול מעבר קרשט השיוויון מתאים
 למסלול מתחיל קטן 3-3.

ביסוי קצמתי:

ניתן להראות לא מכאן $G = (V, E)$ קדושה

$X \subseteq V$ נקראת ביסוי קצמתי

של G אם $e \in E$ לכל $e \in X$ $e \cap X \neq \emptyset$

מסקנה: $V \setminus X$ היא קדושה קטנה

תלוי. מכאן: מצאה של ביסוי מנימי.
עקרונה מצאה של קבוצת מקסימלית.

לניח ש- $G = (V_L, V_R, E)$ הוא

גרף 3-צד. במקרה זה קיים:

האלגוריתם של König

הי' $M \subseteq E$ שיבוק מקסימלי ב- G .

תהי Z קדושת הצמתים ב- V_L שאינם
משוברים, בתוספת כל הצמתים שנית

פרטים אחרים מהצמתים הללו צ"ל
מסלול מתחיל.

$$S = (V_L \setminus Z) \cup (V_R \cap Z)$$

היא כיסוי הצמתים מינימלי.

הוכחה: תהי $\{x, y\} \in E$ כאשר $x \in V_L$
1- $y \in V_R$. אם $x \notin Z$, אז $x \in S$.
אם $x \in Z$ אז אם $y \in Z$ כי אם
 $\{x, y\} \in M$ אז מסלול מתחיל מצומת
זו משלצק ב- V_L מכיוון ש- x צ"ל
קשת בשידוך, ואם $\{x, y\} \notin M$ אז הקשת
היא ממשיכה מסלול מתחיל שהגיע
ל- x , אם לא היינו קודם ב- y .
לכן $y \in S$. כלומר, S הוא אכן כיסוי.
כל כיסוי S חייב לקיים $|S| \geq |M|$, כי
כל קשת ב- M חייבת להיות מכוסה ואין
צומת שמכסה יותר מקשת אחת ב- M .

מצד שני, כל צומת q - V_L היא
 משודבת (כל השדות Z שבתה
 את כל הצמתים הכלואים משודבים q - V_L).
 עבור $x \in V_L$ שמשודבת q - Y , לא ייתכן
 כי $Y \in Z$ (אחרת זה אומר ש- $x \in Z$ כי
 אפסי זה משיק עם מסלול מתחיל
 שמוביל q - Y). אבל אם כל צומת
 q - V_R משודבת, אחרת נקבל מסלול
 מתחיל מקסימלי באורך n בלבד, וזה
 מאפשר להעביר את M , בסתירה
 למקסימליות של M .

אם כן, $|S| \leq |M|$ וזה כן

S כיום מינימלי.

מילים

צריך להטות שיבוק מקסימום M - אנחנו מכירים
 אלגוריתם $O(m+n)$ (יש אלגוריתם יעילים יותר)
 מצד שני Z דומה ל- BFS $O(m+n)$ בעלות
 סיבוכיות המקום הריבועית $O(m+n)$

מה למד? מה בלתי?



בדואמה הוא שידוק מקסימום הוא פאדל 1, אדל
כיסוי מנימום הוא פאדל 2.

אכשו למצוא שידוק מקסימום בלתי - לא
בקורים הזה (נלמד בקורים ההמשך - אלגוריתמים
מקדמ)

לא ידוע לנו אלגוריתם יעיל למציאת כיסוי מנימום.

אכשו בקלות למצוא שידוק טלוי ניתן להעזרה (לא)
בהכרח גורל ביאמה: ניקח קטת, נסיר את כל
הקטתת הנלצות בה, וחוצר חלילה.

בהינתן שידוק כזה, קדוצת כל הקצוות של
הקטתת השידוק היא כיסוי בצמתים (כל
קטת אחרת שכלה של קטת השידוק ולכן
נלצת באחד מקצוותיה).

גורל הכיסוי כפול מלול השידוק (שהוא לכל
הימח גורל שידוק מקסימום) וכל כן זה
קיריז בפקלה 2.

הסיקאלת: $O(m+n)$ פאולאר ומקאם

(הסכומים הם על קטגוריות בשר)
 תוצאת האלגוריתם: כל התצאות i זקוקות

$$W_i = \sum_k y_{ik}$$

סיבוכיות זמן ומקום: $O(m+n)$

לדוגמה:

טענה: אם S היא תוצאת האלגוריתם, אז S הוא ביסוי לתצאות של Q .

הוכחה: בואו נניח שהיא מתקיימת בכל מהלך היציאה האלגוריתם, עבור כל צומת i , ש-

$$W_i \geq \sum_k y_{ik}$$

העידכון של קשת צנוצנו הוא לא שיתקיים שיליון או ב- i או ב- j (או בשניהם). עכשיו $|V| \geq 1$. האלגוריתם עובר על כל הקשתות ועד כן בולן תהיה מכוסות כן בסוף ההיציאה.

טענה: הס'אם הייזע, $\sum_{i \in S} w_i \leq 2 \cdot \sum_{\{i,j\} \in E} y_{ij}$

הוכחה:

$$\sum_{i \in S} w_i = \sum_{i \in S} \sum_{j: \{i,j\} \in E} y_{ij} \leq 2 \sum_{\{i,j\} \in E} y_{ij}$$

כי קסטעלעזען
לספירטירע היילעכעו"ם,
בזמערער זי אדעסערער זי

טענה: $\sum_{\{i,j\} \in E} y_{ij} \leq$ מסקל ביס'אן קצמתי'ם
קלעב'אן

הוכחה: נסמן ק - Z_{OPT} אלס המסקל
סע ביס'אן קצמתי'ם קלעב'אן. אדער עלאפין
אלס כק:

$$Z_{OPT} =$$

$$= \min \left\{ \sum_i w_i x_i : \forall \{i,j\} \in E, x_i + x_j \geq 1 \wedge \forall i \in V, x_i \in [0,1] \right\}$$

(הי - x_i - פ-הם מסקל א'דערערער שטעלע'ס
אלס צמתי'ם נעלעס פ'יירן)

נסמן ס:

$$Z^* = \min \left\{ \sum_i w_i x_i : \forall \{i,j\} \in E, x_i + x_j \geq 1 \wedge \forall i \in V, x_i \geq 0 \right\}$$

$$Z^* \leq Z_{\text{OPT}} \quad \text{כחלק מ: } (M, w, c)$$

עם x רצויים יותר ולכן התנאים חזרו.
מחשבים מינימום עבור (M, w, c) .

טענה: נניח $y: E \rightarrow \mathbb{R}$ מקיימת:

(1) $y_{ij} \geq 0, \{i,j\} \in E$

(2) $\sum_k y_{ik} \leq w_i, i \in V$

$$\sum_k y_{ik} \leq w_i$$

$$\sum_{\{i,j\} \in E} y_{ij} \leq Z^*$$

הוכחה: נניח $x: V \rightarrow \mathbb{R}$ פונקציה המקיימת:

(1) $x_i \geq 0, i \in V$

(2) $x_i + x_j \geq 1, \{i,j\} \in E$

$$\begin{aligned} \sum_{\{i,j\} \in E} y_{ij} &\leq \sum_{\{i,j\} \in E} y_{ij} (x_i + x_j) = \sum_{i \in V} x_i \sum_{j: \{i,j\} \in E} y_{ij} \\ &\leq \sum_{i \in V} w_i x_i \end{aligned}$$

$$U^* = \max \left\{ \sum_{\{i,j\} \in E} y_{ij} : \forall i \in V, \sum_k y_{ik} \leq w_i \wedge \forall \{i,j\} \in E, y_{ij} \geq 0 \right\} \leq$$

$$\leq \min \left\{ \sum_{i \in V} w_i x_i : \forall \{i,j\} \in E, x_i + x_j \geq 1 \wedge \forall i \in V, x_i \geq 0 \right\} = Z^*$$

אלגוריתמים הסתברותיים

הע"ת חתך מינימום:

ניתן להימנע מבלבול
 $G = (V, E)$
הוצים למצוא חתך $C \subseteq E$ קטן ביותר

— אפילו לפתור זאלט"ע: $n-1$ חישובים
של זרימת מינימום.

אלגוריתם פשוט יותר:

כיווץ קטן: יהי $e = \{u, v\} \in E$ אז:

$G/e = (V', E')$ האמור הצמצום הם אלו
צמצום יחסית למחצית u ו- v הצמצום u, v
והקטנת הן אולם קטנת למחצית הסרת e
והחלפת כל קטנת מהצורה $\{x, u\}$ או $\{v, x\}$
בקטנת $\{x, u, v\}$.

(ע"מ לה, יתכן שניצור קטנות מקבילות)

האלגוריתם:

כדי שאר שיהיה G יותר משני צמתים,

- נבחר קשת e שממנה היתכנות אחידה

- נחליף את G ב- G/e .

בסיס - שני הצמתים מייצגים שתי

קבוצות לא חתוכות של צמתים

בצדדים המשותפים, ואוסף הקשתות המקבילות
ביניהן הוא חתך.

האלגוריתם מצביע אם זה חתך מנימל.

לעננה: אם C חתך מנימל בערך G
אז $|E(G)| \geq \frac{|C| \cdot n}{2}$.

הוכחה: $|C|$ הוא לכל היותר הפיפה המנימלית
של צומת ב- G , וסכום הדרגות הוא $2|E(G)|$.

מסקנה: ההסתברות ש- $C \subseteq E(G/e)$ היא לפחות
 $1 - \frac{2}{n}$.

עכשיו נתבונן בסדרה של כיווץ קטנה
 שמסת"מ כאלו מתה להם עם על קווקזים
 למי"ם חתך C' בעלם הקדם.

$$Pr[C' = C] \geq \prod_{k=3}^n \left(1 - \frac{2}{k}\right) \quad \underline{\text{לסל}}$$

הוכחה: באינדוקציה על n . בסיס האינדוקציה הוא
 $n=2$ שכן ההסתברות היא היא 1.
 נניח נבואת $n-1$.

$$\begin{aligned} Pr_G[C' = C] &= \\ Pr_G[C \subseteq E(G_e)] \cdot Pr_{G_e}[C' = C : C \subseteq E(G_e)] &= \\ \left(1 - \frac{2}{n}\right) \cdot \prod_{k=3}^{n-1} \left(1 - \frac{2}{k}\right) \end{aligned}$$

$$Pr[C' = C] \geq \frac{1}{\binom{n}{2}} \quad \underline{\text{לסל}}$$

$$\prod_{k=3}^n \left(1 - \frac{2}{k}\right) = \frac{(n-2)(n-3) \dots 3 \cdot 2 \cdot 1}{n \cdot (n-1)(n-3) \dots 3} = \frac{2}{n(n-1)} \quad \underline{\text{קובחיה}}$$

מסקנה: הסיכוי שהיבטל בחישה C הוא

פזמים, הסיכוי שהיבטל הוא פזל הילתו

$$\left(1 - \frac{1}{n^2}\right)^N \leq e^{-N/n^2}$$

אחרי n^2 ניסיונות מצליחים בהסתברות קבועה.

הסיבוכיות: $O(n^2 m)$

מה לעד. חתך גדול ביותר? - בעיה קשה!

הנה קירוב לעד:

1. נגדיר קטגוריות כלשהן $E = \{x, y\}$ ונשים את

2 ו-1 y בצדדים שאנחנו שם החתך.

2. לכל $\{x, y\} \in V$ נגדיר צדד באופן דו-כיווני

ובהתבטלות אחידה.

משפט: אם C החיץ של G (זה משתנה
מקרי) אז $E[|C|] > \frac{|E|}{2}$

הוכחה: הקטן $|C|$ נחשב כוללית. זהו
כל קטן $|C|$ אחת, ההסתברות שקצותיה קצרים שונים
היא $\frac{1}{2}$. המאורעות של חיץ קטן אינם
בהכרח ב"ת, אבל זה"ע אינדיקטור התואמת
 $E[|C|]$ הוא סכום ההסתברות החיתוך של קטנות.

משקנה: זה קירוב לאלגוריתם בקטלוג 2, כי
החיץ העצום ביותר חוצע לכל הילד את
כל הקשתות.

הערה: אלו חייב מאפשר קירוב 2 להכללה
הבאה: נתון אלס $\mathcal{F}$ משואות אינדיקטור מסוים
 $\mathbb{Z}_2$. דואמה למשלואה נכסות: $x_1 \oplus x_2 \oplus \dots \oplus x_n = 1$.
רוצים למצוא הרכה למשתנים שמקיימת מספר
אדום ביותר של משואות.
פיתרון מקורב: נבחר כל משתנה באופן ב"ת להילד
0 או 1 בהתבססות אחידה.
משואה מתקיימת בהסתברות $\frac{1}{2}$.

דגור בעיית MAX CUT יש אלגוריתם
פארגמיניס"ם שנותנים קירוב 2: אלג' חמור, חיבוב
מקסימלי.
ש קירובים טובים יותר מקטלוג 2.

נתון טקסט T שהוא רצף של אותיות מאלף
 סופי שלמנו Σ . נסמן $n = |T|$, $d = |\Sigma|$
 ונניח בה"ב $\Sigma = \{0, 1, \dots, d-1\}$.

כמו כן נתונה תבנית P , גם היא רצף של אותיות מ- Σ .
 נסמן $m = |P|$. נניח כי $m \ll n$.

רוצים דמיון אחר כל המופעים של P ב- T .

האלמנטים הנאיבי: (עבור $i = 1, 2, \dots, n-m+1$)
 ועבור כל זיג של i נשאלה בין $T[i \dots i+m-1]$ לבין P .

רצף האותיות ב- T החל
 מהמיקום i ורחב המיקום
 ה- $i+m-1$.

סיבוכיות הזמן: $O(n \cdot m)$ פשוטה, קטנה פשוטה היא
 השאלה בין שתי אלויות ב- Σ או גישה לאיבר
 ב- T או ב- P לפי האינדקס שלה.

סיבוכיות המרחב: $O(1)$ תא זיכרון שמחזיקים את נדקס, קלסר
 פקטור ופלט.

האלגוריתם של Karp + Rabin

אופרדה התייחס P ו- $T[i \dots i+m-1]$ כאילו מסתרים
 הישואים בקסים d :

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

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

די פהטור פון t_i פ-ק.

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

פיתויים פארהאטן דער כי המספרים טאטעט עובדים
איתם דורשים $O(m \log d)$ ביטים פיינעס.

זג צו בערער השואה, וועט פאמלע חזשן, ידעו
 $O(m \log d)$ ביט, סה"כ $O(m \log d)$ פאמלע
זו ביטים, קדיקן כמו חז' פאש הא'בי.

אם כן, נשתמש בקבוצה Q של ראשוניים
שמקיימים כמה תכונות:

(1) קבוצה Q , $q_{\max} = \max_{q \in Q} q$, $\log_2 q_{\max}$ קטן (פרימאלה)

פ-מ, m , זומר 2^m , $q_{\max} < 2^m$.

(2) $|Q| \gg m \log d$.

נעריך $q \in Q$ בהתפלגות אחידה. אם $t_i \not\equiv p \pmod{q}$, אז

הסיכוי $t_i \equiv p \pmod{q}$ -

פ- $|t_i - p| < d^m$ יש פכל ה'אר $m \log_2 d$

זורמים ראשוניים (כי כל הזורמים חלקו $2 \leq$ וחרק
הוא מכליתם). פכן, היסתהות היא פכל
ה'אר $\frac{d \log_2 d}{m}$.

סיבוכיות זמן היציבה, הייתה שפזלית על מספרים
 קני $\log_2 q_{\max}$ קי"ם ניתנות לעיצוב בעין $O(1)$,
 הי"א $O\left(m + n + m\left(s + \frac{nm \log_2 d}{1Q}\right)\right)$ בתחלת,
 באשר S מ"ם המופיעים על P ב- T

כדי לבחור את Q אפשר להשתמש בקביעות על
 המספרים הראשוניים:

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

$$\frac{x}{\ln x} \geq m^2 \log_2 d$$

$$x \geq m^2 \log_2 d (\log m + \log \log d)$$

$$\log_2 q_{\max} = O(\log m + \log \log d)$$

פולינומים ממונים

נתון שדה F ופולינום $P \in F[x_1, \dots, x_n]$
הרשום כמעלה של פונקציות עיגוליות
(או באלבן אתר המקשה על פישוט, למשל -
דטרמיננטה של מטריצה פולינומית)
שאלה: האם P היא זהותית 0?

משפט Schwartz-Zippel: תהי A ת

קבוצה סופית של איברי F . כמו כן,
יהי $P \in F[x_1, \dots, x_n]$, $P \neq 0$. נגדיל הצבה

$x_i = a_i$ לכל $i = 1, \dots, n$ כך שה- $a_i \in A$.
כלי תנאים ומתבטאים את P ב- A . אז

$$\Pr[P(a_1, \dots, a_n) = 0] \leq \frac{\deg(P)}{|A|}$$

באשר $\deg(P)$ היא המעלה של P .

הוכחה: באינדוקציה על n . $d = \deg(P)$.

בסיס האינדוקציה: $n=1$. השערה נקראת
מזה שפולינום במשתנה אחד ממעלה d טאט
זהותית 0 יש לכל היותר d ערכים טונים.

נניח נבולת $n-1$.

$$P(x_1, \dots, x_n) = \sum_{i=0}^d x_i P_i(x_2, \dots, x_n) \quad \text{נרשם}$$

$$P \neq 0 \quad \text{ולכן יש } i \text{ שבו } P_i \neq 0$$

נבחר i מקסימלי. ככה המעלה של P_i היא $d-i$, וזהו המעלה הגבוה ביותר של P_i שיש לו.

$$\Pr[P_i(a_2, \dots, a_n) = 0] \leq \frac{d-i}{|S|}$$

אם $P_i(a_2, \dots, a_n) \neq 0$ אז $\sum_{j=0}^d x_j P_j(a_2, \dots, a_n) \neq 0$
 הוא ברובו לא 0 (המשתנה x_0 הוא שכיח ביותר, וזהו המקסימלי שיש לו).

$$\Pr[a_i : P_i(a_2, \dots, a_n) = 0 \mid P_i(a_2, \dots, a_n) \neq 0] \leq \frac{i}{|S|}$$

כעת, נסמן את המאורע E_1 - $P(a_1, \dots, a_n) = 0$
 ואת המאורע E_2 - $P_i(a_2, \dots, a_n) = 0$

$$\begin{aligned} \Pr[E_1] &= \Pr[E_1 \wedge E_2] + \Pr[E_1 \wedge \bar{E}_2] = \\ &= \Pr[E_1 | E_2] \Pr[E_2] + \Pr[E_1 | \bar{E}_2] \Pr[\bar{E}_2] \\ &\leq \Pr[E_2] + \Pr[E_1 | \bar{E}_2] \leq \frac{d-i}{|S|} + \frac{i}{|S|} \end{aligned}$$

מסקנה: קשורה גורלית יש אלגוריתם הספקות
 י.ג.י. חזיר העייה הבאה: בהינתן פולינום
 P מסתנים P ממעלה ידועה d , הנתון
 בייצוג כלשהו של פולינום חישוק יעיל של
 זריכו חזיר כל הצורה נתונה, בדקו אם
 $P \equiv 0$.

הוכחה: ניקח קבוצה S חזרה $|S| = 2d$.
 נגדיל הצורה מקיימת של איברים $M-S$ ומכאן
 אם זה M פתמים. אם נקח 0 קכל
 הפתמים נוצר $P \equiv 0$, אחרת נוצר
 $P \not\equiv 0$. במקרה השני d סופר. במקרה
 הראשון סופר אם $P \not\equiv 0$ זה יהיה
 0 חזיר כל M ההצורה. הסיכוי לזה
 הוא לכל היותר 2^{-d} .

סיכום: נתון גורלית $G = (V_L, V_R, E)$
 המקיים $|V_L| = |V_R|$. נגדיר מאיזה סימוליות
 M באלון הפא: (הטוריות ממספרות לפי איברי
 V_L והצורה לפי איברי V_R)
 $M_{ij} = \begin{cases} x_{ij} & \text{if } (i,j) \in E \\ 0 & \text{אחרת} \end{cases}$ **(המתייחס ל-Edmonds)**
 אזי, הפולינום $|M|$ הוא צהרית 0 אם אין
 ב- G סיבוק מושלם.

הבעיה: נתון גרף $G = (V, E)$, זכורו $|V|$ זוגי.
 נגדיר M כאלפון המא: (השוואה והזמנו)
 ממאספיה (זכור או זכור) (V)

(המאספיה)
 (Tutte fu)

$$M_{ij} = \begin{cases} x_{ij} & j < i \wedge ij \in E \\ -x_{ij} & j > i \wedge ij \in E \\ 0 & \text{אחרת} \end{cases}$$

אז, הפונקציה $|M|$ הוא זהותית 0
 אם אין ה- G שידוק מושלם.

הוכחה: הנוסחת הדטרמיננטה, כל המאספיה
 נאונה מתאבסת היא מומם טמכפיה זוגי- x
 זכור קטנות זוגי. זה איחוד זה של מספיה
 טמכפיה את קובקובי הזכור (כולל מושגים באות 2).
 כל מספיה אפסר עקחת בשני הפונקציה, זו אינה
 זוגי-זוגי של הפונקציה. אם המושג הוא באות אי-זוגי אז
 זוגי-זוגי של זוגי של זוגי ו-זוגי, וזוגי
 בפיון ההפוך הסיון של המושג מתהפך.
 אז המושגים היחידים טמכפיה הם של איחודים
 זוגים של מושגים באות זוגי. כל איחוד כזה
 מראה שיש שידוק מושלם בפניה. אם יש שידוק
 מושלם, אז האיחוד של זוגי: שורה קוואלית.

נבונות מטריצות ריבועיות $n \times n$ שבה F , הממוז $n \times n$.

קצוות:

כפל מטריצות: בהינתן שתי מטריצות $A, B \in F^{n \times n}$, הוצים לחשב
 $C = AB$ $C \in F^{n \times n}$ זכורה

חיסול ההופכי: בהינתן $A \in F^{n \times n}$ לא סינגולרית, הוצים לחשב
 $A^{-1} \in F^{n \times n}$ את

חיסול הדטרמיננטה: בהינתן $A \in F^{n \times n}$, הוצים לחשב את $|A| \in F$.

נסמן את הסיבוכיות ($\#$ הפעולות האריתמטיות) של
 זיגורט אלגוריתם בשדה של כפל מטריצות
 $n \times n$ ב- $M(n)$, של חיבור מטריצה $n \times n$
 ב- $I(n)$, ושל חיסול הדטרמיננטה של מטריצה $n \times n$
 ב- $D(n)$.

שימו לב כי $M(n), I(n), D(n) \in \Omega(n^2)$

נסמן ב- I_n את המטריצה האלכסונית $n \times n$
 שבה כל איברי האלכסון הם 1.

משפט: $M(n) = \Theta(I(n))$, תחת ההנחות:

$$I(3n) = O(I(n)) \quad (א)$$

$$M(n+k) = O(M(n)), k \in \{0, 1, 2, \dots, n\} \quad (ב)$$

הוכחה: מניחים A, B נכונים n -צדדי

$$D = \begin{pmatrix} I_n & A & 0 \\ 0 & I_n & B \\ 0 & 0 & I_n \end{pmatrix}$$

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

אז

ולכן אפשר לחשב את AB על ידי הפלג D .

$$9n^2 + I(3n) + n^2 = O(I(n))$$

עבור AB $\uparrow$ עבור n^2 $\uparrow$ עבור $I(3n)$ $\uparrow$ עבור $9n^2$

כדי להפוך: מה"כ n הוא חזקה של 2

$$\begin{pmatrix} A & 0 \\ 0 & I_k \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & 0 \\ 0 & I_k \end{pmatrix} \quad (כ)$$

כל k , אפשר לבחור $k \in \{0, \dots, n\}$ $(n+k)$ חזקה של 2
עבור

ראשית, נניח כי A היא מטריצה סימטרית

מ/אציות חילוקית. נרשם :

$$A = \begin{pmatrix} B & C^T \\ C & D \end{pmatrix}$$

באשר B, C, D מ/אציות $\frac{n}{2} \times \frac{n}{2}$

נרשם אציות מ/אציות Schur של A כחילוקית B -

$$S \triangleq D - C B^{-1} C^T$$

$$A^{-1} = \begin{pmatrix} B^{-1} + B^{-1} C^T S^{-1} C B^{-1} & -B^{-1} C^T S^{-1} \\ -S^{-1} C B^{-1} & S^{-1} \end{pmatrix}$$

המ/אציות החילוקיות B^{-1} ו- S^{-1} ק"מ/אציות
אל A סימטריות ומ/אציות חילוקיות

נחשב 4 מ/אציות של מ/אציות $\frac{n}{2} \times \frac{n}{2}$:

$$C B^{-1}, (C B^{-1}) C^T, S^{-1} (C B^{-1}), \\ (C B^{-1})^T (S^{-1} C B^{-1})$$

שימו לב כי $B^{-1}C^T = (CB^{-1})^T$ כי

B סימטרית $- B^{-1}C^TS^{-1} = (S^{-1}CB^{-1})^T$
 (כי גם S סימטרית)

חישוב $(C)^T$ וחיבור מרחיבות דורש זמן $O(n^2)$. דבר:

$$I(n) \leq 2I(n/2) + 4M(n/2) + O(n^2)$$

נניח בהינעלות כי $I(n/2) \leq C \cdot M(n/2)$ דבר
 קרא C כלשהו. נשים לב כי $M(n/2) \leq \frac{1}{4}M(n)$ כי $(M(n) = \Omega(n^2))$.

נקבל: $I(n) \leq \frac{C}{2}M(n) + M(n) + O(n^2)$
 $\leq C M(n)$

דבר C גדול ≥ 1 .

מה לעדי מרחיבה A באיננה סימטרית מלאה
 חלופת 2 (אלה הפיכה) -
 $A^{-1} = (A^T A)^{-1} A^T$ כי $A^T A$ סימטרית מלאה חלופת

משפט: $D(n) = O(\mu(n))$.

הוכחה: נשתמש בבל נטה צורה כדי לחשב

את הפירוק $A = LUP$, כאשר P אופרטור פירמוטציה על המאפואת, L נטה צורה משולשית תחתונה ו- U נטה צורה משולשית עליונה.

נקבל:

$$|A| = |L| \cdot |U| \cdot |P|$$

$|P|$ זו הזוגיות של הפירמוטציה (± 1)

$$|L| = \prod_{i=1}^n L_{ii} \quad |U| = \prod_{i=1}^n U_{ii}$$

אז נחשב את הפירוק 2 -

ניסיון ראשון: נסה לחשב $A = LU$ גמר הנחות מסוימות.

$$A = \begin{pmatrix} B & C \\ D & E \end{pmatrix}$$

נישאל

$$\frac{n}{2} \times \frac{n}{2} \quad n \text{ מידות} \quad B, C, D, E$$

אם כן, אנו רוצים לפתור $A = LU$

$$B = L_1 U_1 \quad \text{פירוק}$$

בהנחה ש-B סימטרית (ולכן גם L_1, U_1 סימטריות):

$$A = \begin{pmatrix} L_1 U_1 & P_1 C \\ D & E \end{pmatrix} =$$

$$= \begin{pmatrix} L_1 & 0 \\ D U_1^{-1} & E - D U_1^{-1} L_1^{-1} C \end{pmatrix} \begin{pmatrix} U_1 & L_1^{-1} C \\ 0 & I_{n/2} \end{pmatrix}$$

עכשיו נצא פירוק

$$E - D U_1^{-1} L_1^{-1} C = L_2 U_2$$

בהנחה שיש כזה. נקבל:

$$= \begin{pmatrix} L_1 & 0 \\ DV_1^{-1} & L_2 \end{pmatrix} \begin{pmatrix} U_1 & L_1^{-1}C \\ 0 & U_2 \end{pmatrix} =$$

$$= \underbrace{\begin{pmatrix} L_1 & 0 \\ DU_1^{-1} & L_2 \end{pmatrix}}_L \underbrace{\begin{pmatrix} U_1 & L_1^{-1}C \\ 0 & U_2 \end{pmatrix}}_U$$

צאנזער רמב"ם:

למשך $L(n)$ - אורכי סיבוכיות הפירוק של n מספרים
 $n \times n$, אולי :

$$L(n) = 2L(n/2) + O(M(n)) \leq$$

$$\leq \frac{C}{2} M(n) + C' M(n) \leq C \cdot M(n)$$

רור C בלב מספיק.

כך יחולק, למשל, A' ו- N ויתאחדו לקבוצת

האלגוריתם הבסיסי לפרוק LUP.

הנחה: n חזקה של 2, A מטריצה ריבית

$$A^{(0)} = A \quad \text{נכון}$$

נחשב $P^{(1)}, P^{(2)}, P^{(3)}, \dots, P^{(n-1)}$ ✓

$$A = LUP, \quad P = P^{(1)} P^{(2)} \dots P^{(n-1)}$$

$$L = L^{(1)} L^{(2)} \dots L^{(n-1)} \quad \text{מטריצה מסולסלת}$$

U -1, 0, 1 על האלכסון
מטריצה מסולסלת אינה.

$$|A| = |U| \cdot |P| = \pm \prod_{i=1}^n U_{ii} \quad \text{נקודה:}$$

$$(P^{(i)})^{-1} = P^{(i)} \quad \text{הפרמוטציות הן יוקייטות}$$

$$B_i = \{j: \text{המיקום } j \text{ בהצבה } i \text{ הוא } 1\}$$

(ההצגה הבינארית של i היא, עבור
 $i = \sum_{j=0}^k i_j 2^j$ כאשר k הוא
 המספר j -י

$t = \max\{j : j \in B_i\}$ $2^s \leq i < 2^{t+1}$

$s = \min\{j : j \in B_i\}$

$r = \begin{cases} t & s \neq t \\ t-1 & s = t \end{cases}$

$i = 1, 2, \dots$ עבור $i = 1, 2, \dots$

$$A^{(i-1)} = \begin{pmatrix} A_{11}^{(i-1)} & A_{12}^{(i-1)} \\ \hline O & A_{22}^{(i-1)} \\ A_{21}^{(i-1)} & \end{pmatrix}$$

קטע $A^{(i-1)}$: $A^{(i-1)}$ הוא מטריצה 2×2 -ית

$$A_{11}^{(i-1)} \in F^{(i-1) \times (i-1)}$$
 כאן סימלית N ממשית על-אלה

$$A_{12}^{(i-1)} \in F^{(i-1) \times (n-i+1)}$$

$$O \in F^{(2^{r+1}-i+1) \times (i-1)}$$
 מתה צר אפסים

$$A_{21}^{(i-1)} \in F^{(n-2^{r+1}) \times (i-1)}$$

$$A_{22}^{(i-1)} \in F^{(n-i+1) \times (n-i+1)}$$

נשים לב כי $2^{r+1} - i + 1 > 0$

ולכן בשורה העליונה של $A_{22}^{(i-1)}$ קייב להילת

אבר שונה $D-N$, לאחר $A_{22}^{(i-1)}$ תהיה

סימלית.

אם כן, קיימת פרמטריה $\rho^{(i)}$ של

העמודות שמכילה את האבר הזה

לאחכסין (מיקום) (i, i) .

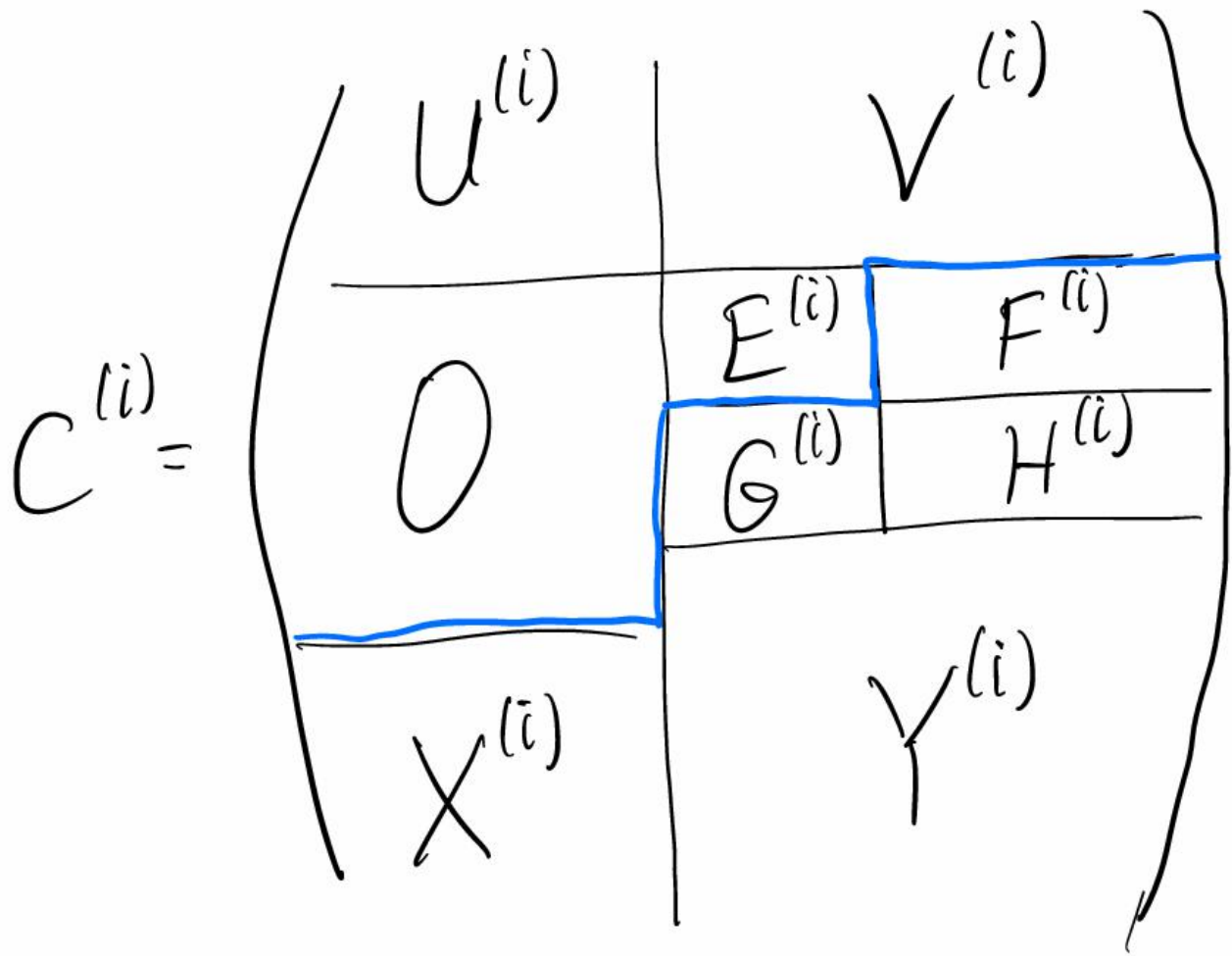
$$C^{(i)} = A^{(i-1)} P^{(i)}$$

7.3.1

$$C_{i,i}^{(i)} \neq 0$$

5/c

: 7.3.2 $C^{(i)}$ מתחילת עמודה i



: 7.3.3

$$L^{(i)} = \begin{pmatrix} I_{i-2^s} & 0 \\ 0 & I_{2^s} & 0 \\ 0 & G^{(i)} (E^{(i)})^{-1} & I_{n-i} \\ 0 & 0 & 0 \end{pmatrix}$$

אזכרנו את $L^{(i)}$ ואת $G^{(i)}$ ואת $E^{(i)}$ ואת I_{n-i}

$$A^{(i)} = (L^{(i)})^{-1} C^{(i)} = \text{pr}$$

$$= (L^{(i)})^{-1} A^{(i-1)} P^{(i)}$$

(היפוך $L^{(i)}$ בשל - כי אלה מהיבט עם סמן
מימין של המוקד מתוך שאם כן)

ש.נ.י. לך כ.

$$A^{(i)} = \left(\begin{array}{c|c} U^{(i)} & V^{(i)} \\ \hline O & \begin{array}{c|c} E^{(i)} & F^{(i)} \\ \hline O & H^{(i)} - G^{(i)}(E^{(i)})^{-1}F^{(i)} \end{array} \\ \hline X^{(i)} & Y^{(i)} \end{array} \right)$$

$$U = A^{(n-1)}$$

אבצדג האחרון

היא מסומשת על-ידי (אם סגולה היא

על-י. הקצויה,

$$U = (L^{(n-1)})^{-1} (L^{(n-2)})^{-1} \dots (L^{(1)})^{-1} A^{(0)} P^{(1)} P^{(2)} \dots P^{(n-1)}$$

לפי

$$A = A^0 = L^{(1)} \dots L^{(n-1)} U (P^{(1)})^{-1} \dots (P^{(n-1)})^{-1}$$

$$= L U P$$

סיקפיות:

חישוק $A^{(i)}$ בהינתן $A^{(i-1)}$ עולה:

מציאת איבר $\neq 0$ בעמודה i של $A_{22}^{(i-1)}$: $n-i$ השוואות

החזית הממוזגת: $n-i+1$ החלפות

חישוב: $E^{(i)} : I(2^s)$

חישוב: $M(2^s) : G^{(i)} (E^{(i)})^{-1}$

חישוב: $\frac{n-i}{2^s} M(2^s) : G^{(i)} (E^{(i)})^{-1} F^{(i)}$

חישוב: $A^{(i)} : 2^s (n-i)$

(שימו לב שכללנו צורך לחשב מפורש את L)

מספר ה- i -ים של חזקים מתקבלים $\leq$ מספרים:
 $\frac{n-1}{2^s}$ של ה- i -ים

סה"כ העלות:

$$\sum_{i=1}^{n-1} (2n-2i+1) + \sum_{s=0}^{\lfloor \log n \rfloor} \left(\frac{n-1}{2^s} (T(2^s) + M(2^s)) + \right. \\ \left. + \sum_{j=1}^{\lfloor \frac{n-1}{2^s} \rfloor} \left(\frac{n-j2^s}{2^s} M(2^s) + 2^s (n-j2^s) \right) \right)$$

$\Rightarrow O(M(n))$ $M(n) = O(n^\omega)$ - כהנחה
 עבור $\omega > 2$.

כפל מatrices

A, B - שתי מatrices $n \times n$ (א'קרים ממשיים)
פאדל

$C = AB$ ה'א מ'א $n \times n$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$$

$$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix}$$

$$c_{ij} = \sum_{t=1}^n a_{it} b_{tj}$$

2-1 מ'א מ'א כפל
מ'א מ'א ח'בור
ס'א $O(n^3)$ מ'א מ'א

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} =$$

= פאדל

$$= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

2-2 מ'א מ'א מ'א מ'א

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

$$B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

$$\frac{n}{2} \times \frac{n}{2}$$

מ'א מ'א מ'א

$$C = AB = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

כל סכום ממוצע

$$C_{11} = A_{11}B_{11} + A_{12}B_{21}$$

$$C_{12} = A_{11}B_{12} + A_{12}B_{22}$$

$$C_{21} = A_{21}B_{11} + A_{22}B_{21}$$

$$C_{22} = A_{21}B_{12} + A_{22}B_{22}$$

נניח ש- n חזקה של 2 ונסמן $T(n)$ את מס' הפעולות הדרושות לחישוב 2 מתייחסת $n \times n$.

שימו לב: סכום של שתי מתייחסת $n \times n$ לפעולות n^2 פעולות חיבור.

$$T(n) = 8T\left(\frac{n}{2}\right) + 4\left(\frac{n}{2}\right)^2 = 8T\left(\frac{n}{2}\right) + n^2$$

פיתרון נוסחת התקדמות היא $\Theta(n^3)$.

האלגוריתם של Strassen

אפשר לחשב את C "ע" 7 הפעולות של $n \times \frac{n}{2}$ מתייחסת $\frac{n}{2} \times \frac{n}{2}$ בלבד $O(n^2)$ פעולות חיבור וחיסור.

$$T(n) = 7T\left(\frac{n}{2}\right) + O(n^2) = \Theta(n^{\log_2 7}) \approx \Theta(n^{2.81})$$

$$\frac{8^4}{16^2} = \frac{4 \cdot 8^2}{2^{3 \log_2 8}}$$

$$n^2 + 8\left(\frac{n}{2}\right)^2 + 8^2\left(\frac{n}{4}\right)^2 + 8^3\left(\frac{n}{8}\right)^2 + \dots + 8^{\log_2 n} n^2 + 2n^2 + 4n^2 + 8n^2 + 16n^2 + \dots + n^3$$

$$A_1 = A_{11} \quad B_1 = B_{12} - B_{22}$$

$$A_2 = A_{11} + A_{12} \quad B_2 = B_{22}$$

$$C_{12} = A_1 B_1 + A_2 B_2 = A_{11} B_{12} - A_{11} B_{22} + A_{11} B_{22} + A_{12} B_{22}$$

$$A_3 = A_{21} + A_{22} \quad B_3 = B_{11}$$

$$A_4 = A_{22} \quad B_4 = B_{21} - B_{11}$$

$$C_{21} = A_3 B_3 + A_4 B_4 = A_{21} B_{11} + A_{22} B_{11} + A_{22} B_{21} - A_{22} B_{11}$$

$$A_5 = A_{11} + A_{22} \quad B_5 = B_{11} + B_{22}$$

$$A_6 = A_{12} - A_{22} \quad B_6 = B_{21} + B_{22}$$

$$\begin{aligned} C_{11} &= A_5 B_5 + A_4 B_4 - A_2 B_2 + A_6 B_6 = \\ &= A_{11} B_{11} + A_{22} B_{11} + A_{11} B_{22} + A_{22} B_{22} + A_{22} B_{21} - A_{22} B_{11} \\ &\quad - A_{11} B_{22} - A_{12} B_{22} + A_{12} B_{21} + A_{12} B_{22} - A_{22} B_{21} - A_{22} B_{22} \end{aligned}$$

$$A_7 = A_{11} - A_{21} \quad B_7 = B_{11} + B_{12}$$

$$\begin{aligned} C_{22} &= A_5 B_5 + A_1 B_1 - A_3 B_3 - A_7 B_7 = A_{11} B_{11} + A_{22} B_{11} + A_{11} B_{22} + A_{22} B_{22} \\ &\quad + A_{11} B_{12} - A_{11} B_{22} - A_{21} B_{11} - A_{22} B_{11} - A_{11} B_{11} - A_{11} B_{12} + A_{21} B_{11} + A_{21} B_{12} \end{aligned}$$

18 פסגות של חיבור/היסוס של $\frac{n}{2} \times \frac{n}{2}$

$$18 \cdot \left(\frac{n}{2}\right)^2 = \frac{9}{2} n^2$$

סה"כ

7 פסגות כפול של חיבור $\frac{n}{2} \times \frac{n}{2}$

$$T(n) = 7T\left(\frac{n}{2}\right) + \frac{9}{2}n^2$$

$$\begin{pmatrix} 1 & 3 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 8 & 4 \\ 6 & 2 \end{pmatrix} = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

ציון:

$$C_{12} = 1 \cdot (4-2) + (1+3) \cdot 2 = 2 + 8 = 10$$

$$C_{21} = (5+7) \cdot 8 + 7 \cdot (6-8) = 96 - 14 = 82$$

$$\begin{aligned} C_{11} &= (1+7) \cdot (8+2) + 7 \cdot (6-8) - (1+3) \cdot 2 + (3-7) \cdot (6+2) = \\ &= 80 - 14 - 8 - 32 = 26 \end{aligned}$$

$$\begin{aligned} C_{22} &= (1+7) \cdot (8+2) + 1 \cdot (4-2) - (5+7) \cdot 8 - (1-5) \cdot (8+4) = \\ &= 80 + 2 - 96 + 48 = 34 \end{aligned}$$

האלג' עובד עקרו מטריות מול כל שדה (א/א חזק)

המציאה האלה ביותר הידועה $O(n^{2.374})$

חסר תועלת $C \cdot n^2$

$$AB = C$$

הדיקה האם

התמרת Fourier הדיסקרטית

מוטיבציה (אחת מיני דעות): נתונים $a, b \in \mathbb{R}^n$

רוצים לחשב קונולוציה שלהם $a * b$
בה $c \in \mathbb{R}^{2n-1}$ המהיר כן:

(נסמן את האינדקסים של c המקבילים
0-n-1 הם המימד בחלל $\mathbb{R}^{2n-1}$)

$$c_i = \sum_{j+k=i} a_j b_k$$

a_{n-1}

$a_i \dots a_0$

$b_0 \dots b_i$

b_{n-1}

המכפלה הפנימית כאן

היא c_i

עמדה? - עמשה, a ו- b הם ווקטורי המקבילים
של שני פולינומים ערוצים עיכבדים. ווקטור
מקבילי פולינום המכפלה הוא c :

$$\left(\sum_{j=0}^{n-1} a_j x^j \right) \left(\sum_{k=0}^{n-1} b_k x^k \right) = \left(\sum_{i=0}^{2n-2} c_i x^i \right)$$

פיתרון נאיבי דורש $O(n^2)$ פעולות חשבון.

דאגים אלקטרוניים יעילים יותר!

• ווקטור a מציגים עם יציג זריכי.

ההסברות שלו עם קבצים אוריתאנלי.

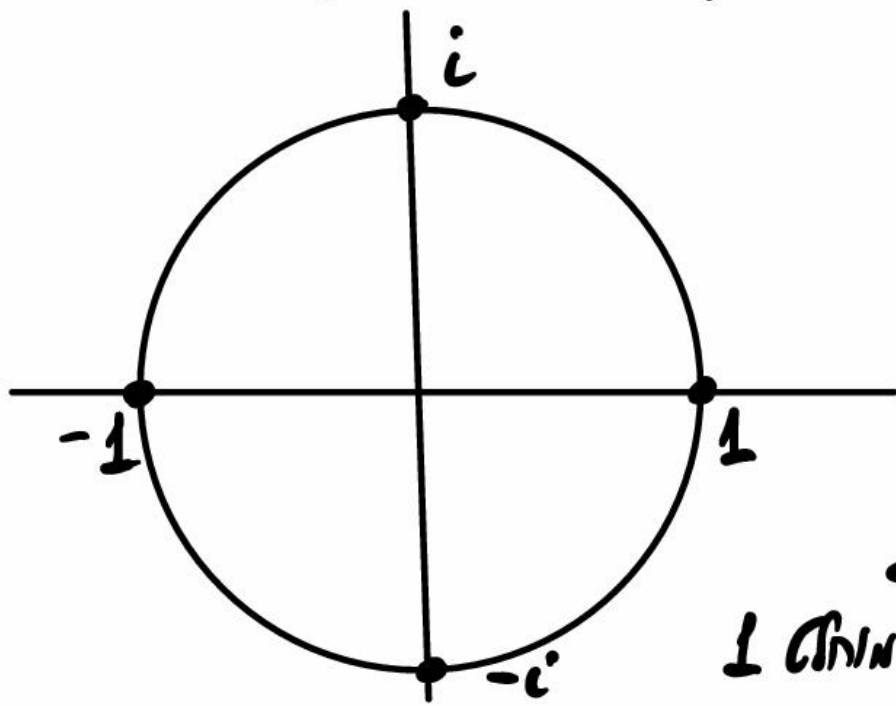
• $\mathbb{R}^n$ מקובל עקרו את הקבצים הסטטי (הזרים).

• עריקה צרכים, כל הקבצים שווים.

• עריכנו, בחירת הקבצים חשובה!

לצדקן עמספרים מרובקים (כלומר, נעקד עם
ווקטורים $\mathbb{C}^n$ במקום $\mathbb{R}^n$)

המישור המרובק



נקודה (α, β)
מייצגת את

$$\alpha + \beta i$$

מחלק היחידה הלא אולי
המס' המרוכבים שזריכ המוחלט 1

$\{-1, 1\}$ הם שורשי היחידה מסדר 2
(המספרים שהיבואם L)

$\{-i, 1, -1, i\}$ הם שורשי היחידה מסדר 4

באופן כללי, שורשי היחידה מסדר n הם

$$\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = e^{i \frac{2\pi k}{n}}$$

זכור $k = 0, 1, 2, \dots, n-1$
 כק שיש n שורשי היחידה מסדר n, שבהם
 n השורשים מתאם למרחבים של הפולינום

נסתכל אולי: $\forall \theta \in \mathbb{R}$

$$e^{i\theta} = \cos \theta + i \sin \theta$$

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!} \quad \sin x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$

$$x^n - 1$$

(מתאם למרחבים, עם פולינום מתאם n ש
 קדיק n שורשים, כולם יחידים)

נקודת אית n ונסמן את n שורשי היחידה
 מסדר n - $1 = \omega_0, \omega_1, \dots, \omega_{n-1}$

$$\omega_k = e^{i \frac{2\pi k}{n}}$$

$$\omega_k^n = 1, \quad k \text{ כל}$$

אם n זוגי אז $\{\omega_k^2 : k=0, \dots, n-1\}$ הם

שונים. הית'זה מסדר $\frac{n}{2}$ $(\omega_k - 1 - \omega_k)$ מתנים אלא דרך כאשר מסלים אותם בה'ק'ל

נניח מכאן ואילך ש- n זוגי ונבדוק ש-2.

נתקן בנקודות $\phi_k = (\omega_k^0, \omega_k^1, \omega_k^2, \dots, \omega_k^{n-1})$
 $k=0, 1, 2, \dots, n-1$

טענה: אם $k \neq l$ אז $\langle \phi_k, \phi_l \rangle = 0$

הוכחה:

$$\langle \phi_k, \phi_l \rangle = \sum_{j=0}^{n-1} \omega_k^j \bar{\omega}_l^j =$$

$$= \sum_{j=0}^{n-1} e^{i \frac{2\pi(k-l)j}{n}}$$

$\bar{\omega}_l$ הוא המספר
 ה-3/4-י של ω_l :
 $e^{-i \frac{2\pi l}{n}}$

זה סכום של n איברים
 שמתחיל ב-1, כלומר, זהו סכום
 חזקות של $e^{i \frac{2\pi(k-l)}{n}}$ (אם הסדר קטן מ- n)
 הסכום הזה, כפי שאנחנו יודעים מתאם,
 שווה לסכום 0.

$$e^{i \frac{2\pi(k-l)j}{n}} = -e^{i \frac{2\pi(k-l)(j+\frac{n}{2})}{n}} \quad 0 \leq j < \frac{n}{2}$$

$$\phi_0, \phi_1, \dots, \phi_{n-1}$$

הקסיס

נקראו קסיס בורייז הפיסקלי

הערה: הנמצא הוא טקסים בורייז הוא האלקטורים
עם האידים הצמודים לאלו שצמדו לעצם. זה
לא משנה את הפיתוח שלהן.

הצגת $a \in \mathbb{R}^n$ בקסיס זה:

$$(\phi_0 a, \phi_1 a, \dots, \phi_{n-1} a)^T = \Phi a$$

(Φ) זו המטריצה טמורטורה $\phi_0, \dots, \phi_{n-1}$

היא התמרת בורייז הפיסקלי

שימוש עבר קוואלוציה

נטכן את וקטורי הקלט a, b ואת $c = a * b$
ב- $\mathbb{R}^{2n}$ עבר n טמורטורה 2 (מ/סינים)
א'בדים עם ערך 0 במידת הצורך

Φ זו התמרת בורייז הפיסקלי ב- $\mathbb{C}^{2n}$.

$$\bar{a}, \bar{b}, \bar{c} = \Phi a, \Phi b, \Phi c$$

משפט הקוואליזציה: $k = 0, 1, \dots, 2n-1$ נכד
 $\bar{c}_k = \bar{a}_k \bar{b}_k$ מתקיים

מסקנה: בקדם פורמלה, חישב קוואליזציה
 מציג $O(n)$ פעולות אריתמטיות.

הוכחת המשפט:

$$\begin{aligned}\bar{a}_k \bar{b}_k &= (\phi_k a) \cdot (\phi_k b) = \\ &= \left(\sum_{l=0}^{n-1} \omega_k^l a_l \right) \left(\sum_{m=0}^{n-1} \omega_k^m b_m \right) = \\ &= \sum_{l=0}^{n-1} \sum_{m=0}^{n-1} \omega_k^{l+m} a_l b_m = \\ &= \sum_{j=0}^{2n-2} \omega_k^j \sum_{l+m=j} a_l b_m = \phi_k c = \bar{c}_k\end{aligned}$$

$c = \phi^{-1}(\phi a \odot \phi b)$ אם כן
 באשר $\odot$ הוא כפל א'קר-א'קר

איננו צריכים אלא אריתמטיקה שבה נתן ווקטור
 a מתעק איתו Φa במהירות, ואם
 אלא אריתמטיקה $a^{-1} \Phi$ במהירות.

האלגוריתם מעתה בזה ש- Φ הינו
 מטריצת Vandermonde, כלומר,
 מהצורה

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{bmatrix}$$

ואם קצה שאם n זוגי - ω מורש יחידה
 מסדר n , אז $\omega^2 = (-\omega)^2$ - מורש יחידה מסדר
 $n-1$.

נשים לב כי עבור

$$k = 0, 1, \dots, \frac{n}{2} - 1$$

$$-\omega_k = \omega_{\frac{n}{2} + k}$$

מה: Φ_k הטור ה- k של Φ נוסח

ק- Φ_k^0 $\sim$ התחילת הרכיב ק- Φ_k

ואם Φ_k^1 $\sim$ התחילת הרכיב האי זוגי

ק- Φ . Φ $\sim$ $N/2$

$$\Phi_k^0 = (1, \omega_k^2, \omega_k^4, \dots, \omega_k^{n-2})$$

$$\Phi_k^1 = (\omega_k, \omega_k^3, \dots, \omega_k^{n-1})$$

$$\Phi_k^1 = \omega_k \Phi_k^0$$

כחול כן, ערכי ω_k^2 עבור $k=0, \dots, \frac{n}{2}-1$ הם שורשי היחידה N מסדר $\frac{n}{2}$.

כחול, המסויבה Φ^0 ששורותיה הן Φ_k^0 עבור $k=0, \dots, \frac{n}{2}-1$ היא התמרת פורייה הזיסטרית מסדר $\frac{n}{2}$.

FFT = fast Fourier transform

Φa מביאה את $FFT_n(a)$

$$\text{FFT}_n(a)$$

א/ס, צי: דחשב את

נהנה את a דאיהרם העצ'ים a^0 ודאיהרם
הל' צאצ'ים a' .

$$\varphi^0 = \text{FFT}_{n/2}(a^0) \quad \text{נחשב רקורסיבית את}$$

$$\varphi' = \text{FFT}_{n/2}(a')$$

$$\phi_k a = \begin{cases} \varphi_k^0 + \omega_k \varphi_k' & 0 \leq k \leq \frac{n}{2} - 1 \\ \varphi_{k - \frac{n}{2}}^0 + \omega_k \varphi_{k - \frac{n}{2}}' & \frac{n}{2} \leq k \leq n - 1 \end{cases} \quad \text{א/ס}$$

בסיס ההקורס'יה: FFT_1 הוא טריוויאלי.

דמיון צי: ההפוכה יש תבנית דא/מלך ולכן

ח'ש/ב ההתמורה ההפוכה $\phi^{-1} a$
מתבצעת באותו האופן.
($\phi^{-1} = \frac{1}{n} \phi^*$)

סיבוכיות: א/ס $T(n)$ הוא מספר הפעולות
האסימטיות של FFT_n , א/ס

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

האלגוריתם של Schönhage & Strassen

תנאי: שני מספרים בינריים בני N ספרות (לוגיים) a, b

פלט: המכפלה שלהם, מודולו $2^N + 1$, $ab \pmod{2^N + 1}$

זמן ביצוע: $O(N \log N \log \log N)$

(ממשית זה מוגדר רק עבור מספרים מעל $2^{10,000}$)

(כיום ידוע אלג' של Harvey & van der Hoeven, שמנפיל בזמן $O(N \log N)$, אבל הקבוצה עצום והאלג' לא שימושי לשם תכלית פקטור)

אנחנו נניח ש- $N = 2^m$

אם כן, ציין לעיל m, N - $N = 2^m$ עבור $ab < 2^N + 1$

נחלק את הציג הבינרי של a ושל b ל- 2^m בלוקים בגודל m כל אחד. נממן את סדרות הבלוקים ב- A ו- B .

נבחר n' עבורו $N' = 2^m n' \geq 2n + m$ ונתייחס לכל בלוק בתור מספר יחיד. מודולו $2^{N'} + 1$.

אלכנר נקח $n' = O\left(\frac{n}{2^m}\right)$

$$2^{N'} + 1 \geq 2^{2n+m} + 1 = 2^m \cdot 2^{2n} + 1$$

לכן, הסכום של המכפלות של כל היתר 2^m בלוק של בלוקים נייב קטן $N - N'$ (אין carry כלשונו מחשבים הקסיים $(2^{N'} + 1)$)

עוד נשים לב כי $g = 2^{2n}$ מקיים $g^{2^m/2} \equiv -1 \pmod{2^{N'} + 1}$

לכן g הוא שורש יחידה פרימיטיבי מסדר 2^m עבור

החוג $\mathbb{Z} / (2^{N'} + 1) \mathbb{Z} = \mathbb{Z}_{2^{N'} + 1}$ כלומר, $g^k \neq 1$ עבור $k < 2^m$

עכשיו, נחשב את התמרת Fourier הקדידה $\hat{A}, \hat{B}$ של A, B

מספרים (כלומר, אריתמטיקה מודולרית $2^N + 1$)

עם q ערכים בתור שונים היתירה מסדר 2^m (שנה אורך האקטורס (A, B) כלומר, q מתחיל את $1, q, q^2, \dots, q^{2^m-1}$ הם כל שורשי היתירה מסדר 2^m .

י"י $\hat{C} = \hat{A} \odot \hat{B}$ $\rightarrow$ כל איבר-איבר C היתירה של היתירה הפוכה של $\hat{C}$.

הסבר קטן (*)

$$ab = \sum_{j=0}^{2^m-1} C_j 2^{nj} \pmod{2^N+1}$$

$$T(N) = \underbrace{O(m 2^m) \cdot O(N')}_{\text{FFT במסדר } 2^m \text{ ו-} N'} + \underbrace{2^m T(c \cdot n)}_{\text{הצטרף הפעם אל היתירה}} + \underbrace{O((n+m) 2^m)}_{\substack{\text{כ-} 2^m \text{ מספרים } C_j \text{ של } C_j \text{ כל } C_j \text{ הוא } 2n+m \text{ ביטים}}}$$

$$= O(N \cdot m) + 2^m T(c \cdot n)$$

נשתמש באופן קטן טורם זה:

$$T(N) = N \log \frac{N}{n_1} + \frac{N}{n_1} c \cdot n_1 \log \frac{c \cdot n_1}{n_2} + \dots$$

$$= N \left(\log \frac{N}{n_1} + c \cdot \log \frac{c \cdot n_1}{n_2} + c^2 \log \frac{c \cdot n_2}{n_3} + \dots \right)$$

נראה $n_i = N^{c^{-i}}$ $\therefore$ מה ש"ן:

$$T(N) = N \left(\log N^{1-c^{-1}} + c \cdot \log c N^{c^{-1}-c^{-2}} + \dots \right)$$

$$= N(1-c^{-1})(1+\frac{c}{c}+\frac{c^2}{c^2}+\dots)\log N + (1+c+c^2+\dots)\log c$$

אפשר למצוא את הקדושים כשער שזלם הלוקי הוא קדוץ, כלומר,
 $i = \Theta(\log \log N)$ או, $c^{-i} = \frac{1}{\log N}$

אז סה"כ נקודות זמן ה"ה של $O(N \log N \log \log N)$.

הסבר ד - (*)

$$a = a_{2^m-1} a_{2^m-2} \dots a_2 a_1 a_0 \quad \text{ניסוח}$$

$$b = b_{2^m-1} b_{2^m-2} \dots b_2 b_1 b_0$$

באשר a_i, b_i הם הקדושים של n קדושים כל אחד.

$$a = \sum_{j=0}^{2^m-1} a_j 2^{n_j} \quad b = \sum_{j=0}^{2^m-1} b_j 2^{n_j} \quad \text{א/כ}$$

באשר a_j, b_j מספרים אחרים מספרים קדושים.

המקדמים 2^{n_j} נבדל מכן שאלה a_j, b_j מספרים קדושים.

$$ab = \sum_{i=0}^{2^{m+1}-2} \sum_{j=0}^i a_j b_{i-j} 2^{n_i} = \sum_{i=0}^{2^{m+1}-2} 2^{n_i} \sum_{j=0}^i a_j b_{i-j}$$

(כי המקדמים של a_j הוא 2^{n_j} והמקדמים של b_{i-j} הוא $2^{n(i-j)}$.)

אנחנו מחשבים את $\sum_{j=0}^i a_j b_j$ לפי i בזכות התמורה
 Fourier המהירה באופן $2^{N'+1}/2$. המודולו
 $2^{N'+1}$ נבחר להיות גדול $N-n$ על מנת שהתוצאה
 תהיה שווה לתוצאה ב- 2 בלי המודולו.

שימו לב כי $c_i = \sum_{j=0}^i a_j b_j$ יכול להיות מספר שלילי יותר
 $N-n$ ביטים לעיתים.

$$ab = \sum_{i=0}^{2^{n+1}-2} c_i 2^{ni}$$

החישוב לעיל מבטיח כי

(רקורסיבית, הכפל מחושב מודולו מס' גדול שמבטיח שזה
 לא משנה את התוצאה)

נתונים שני מספרים טבעיים $m, n \in \mathbb{N}$ (כך ש- $0 \notin \mathbb{N}$)

$$g = \gcd(m, n) = \max\{k \in \mathbb{N} : k|m \wedge k|n\}$$

כלומר, g הוא מכפלה של האחרים המשותפים המשותפים m -ם n -ם.

הצורה: קבוצת הכפולות של g במספר שלם $I = \{ag : a \in \mathbb{Z}\}$
היא אידיאל של החוג $(\mathbb{Z}, +, \cdot)$

→ תת חבורה של $(\mathbb{Z}, +)$ שסגורה לכפל באיבר של $\mathbb{Z}$
(החוג קומוטטיבי אז אין הבדל בחקירה זה בין כפל משמאל לבין כפל מימין ולכן זה גם אידיאל שמאל וימני).

עכשיו $I = \{am + bn : a, b \in \mathbb{Z}\}$ ולכן $g = \min\{k \in I : k > 0\}$

→ בחרו שצד ימין מול צד שמאל
 $g = \min\{am + bn : a, b \in \mathbb{Z} \wedge am + bn > 0\}$ רכיבי משמאל
הוכחה: נטון את המינימום ה- g' אזי

$$m = g \cdot g' + r$$

$$r = m - g \cdot g' =$$

$$= m - g \cdot (\alpha m + \beta n)$$

$$= (1 - g\alpha)m - g\beta n \in \{am + bn : a, b \in \mathbb{Z}\}$$

רכיבי הימנית g' , זה מחייב $r = 0$. באותו אופן, g' מחלק גם את n .

מצד שני, אם g'' מחלק משותף של m, n אז חייב להתקיים $m = \alpha' g''$ ו- $n = \beta' g''$, וזהו $\alpha', \beta' \in \mathbb{N}$.

$$g' = \alpha m + \beta n = \alpha \alpha' g'' + \beta \beta' g''$$

ולכן g'' מחלק את g' ולכן $g'' \leq g'$, ומכאן $g' = g$.

אלגוריתם אוקלידס למציאת מחלק משותף גדול ביותר (גדול לפחות $m \geq n$):

נתון סדרת מספרים $r_{-2}, r_{-1}, r_0, r_1, r_2, \dots, r_\ell = 0$

$$g = \gcd(m, n) = r_{\ell-1}$$

אימות: $r_{-2} = m, r_{-1} = n$

אינדוקציה: r_k הוא הסכימה של פחות מחילוק $\frac{r_{k-2}}{r_{k-1}}$ (חילוק קטלוגי) בפרט $0 \leq r_k < r_{k-1}$ ולכן האלג' קהכרת מתבטא.

משפט: $\gcd(r_{k-2}, r_{k-1}) = \gcd(r_{k-1}, r_k), k = 0, 1, 2, \dots, \ell$

הוכחה: נא $g = \gcd(r_{k-2}, r_{k-1})$

נתון, אם כן, יש q, r אחרים: $r_{k-2} = q \cdot g$

$$r_{k-1} = r \cdot g$$

$$0 \leq r_k = r_{k-2} - r' r_{k-1} = (q - r' r) \cdot g$$

לכן $g \mid r_k$. נניח שיש $g' \mid r_k, r_{k-1}$ אז $g' \mid r_{k-2}$.

אז יש q, r אחרים $r_{k-1} = q g'$

$$r_k = r g'$$

אז $r_{k-2} = r' r_{k-1} + r_k = (r' q + r) g'$ אז $g' \mid r_{k-2}$

כלומר, $g' \mid r_{k-2}, r_{k-1}$ ולכן $g' \leq g$

מסקנה: $r_{\ell-1} = \gcd(m, n)$

הוכחה: האינדוקציה $k = 0, 1, \dots, \ell-1$ נקבל $\gcd(r_{k-1}, r_k) =$

$$= \gcd(m, n) = g$$

אז, מכאן ש- $r_\ell = 0$ מתקיים $\gcd(r_{\ell-2}, r_{\ell-1}) = r_{\ell-1}$

כדי להסיר את זמן ההיבד צריך להעריך את l .

נסמן ϕ את השורש החיובי של המשוואה $x^2 - x - 1 = 0$.

$$\phi - 1 = \frac{1}{\phi} \quad \phi = \frac{1 + \sqrt{5}}{2} \quad (\text{יחס הזהב})$$

$$r_k < r_{k-1} < \frac{r_{k-2}}{\phi} \quad \text{אם} \quad r_{k-2} > \phi \cdot r_{k-1}$$

$$r_k \leq r_{k-2} \cdot r_{k-1} \leq (\phi - 1) \cdot r_{k-1} = \frac{r_{k-1}}{\phi} \quad \text{אחרת} \quad r_{k-2} \leq \phi \cdot r_{k-1}$$

$$r_{k-1} \cdot r_k \leq \frac{r_{k-2} \cdot r_{k-1}}{\phi} \quad \text{בכל מקרה,}$$

אם המכפלה קטנה מ- 1 , אז קווצאול $r_k = 0$, כלומר $k = l$.
זה עוקר לכל היותר

$$1 + \log_{\phi}(m \cdot n) \quad \text{בממוצע}$$

$$O(\log m + \log n), \quad \text{לפי יארי קמס' הביטים לביט}$$

את m, n .

הערה: למעשה, מספר האיטרציות תלוי רק במס' הביטים לביט

את n , כי $r_0 < n$. לכן, תישאר $\gcd(n, r_0)$ לוקח

$O(\log n)$ איטרציות. (מספר Lamé, 1844)

רצף הערה: חילוק (חישוב אחד ושארית) ניתן לבצע באותה סיבוכיות כמו כפל. זה נותן זמן חיבה למחישוב $\gcd$ של $O(N \cdot \text{mult}(M, N))$.
באשר M, N מס' הביטים להצגת m, n ו- $\text{mult}(M, N)$ סיבוכיות כפל מס' בני M, N ביטים.

לא נראה זאת. שיטה פשוטה לבצע חילוק m / n : נחש את התוצאה q בחיפוש בינארי - קובקים אם $r = m - q \cdot n$ מקיים $0 \leq r < n$. זה יבדוק $O(N \cdot \text{mult}(M, N))$ זמן.

הצגה מתקנה: $m, n \in \mathbb{N}$. הוצגים למטה m^n .

י.ה. $p = \max\{k \in \mathbb{N} : 2^k \leq m\}$ (קדם זמשה ההצגה קיטלית)

נחשב עקרה $p, \dots, 2, 1, 0 = k$ את m^{2^k} קוצרת המספר:

$$m^{2^0} = m$$

$$m^{2^k} = m^{2^{k-1}} \cdot m^{2^{k-1}}$$

זה דורש $p \leq N$ כפלים. (N מס' הביטים להצגת m)

נסמן k - את m ערך הביט k -א. (מימין) של ההצגה של m כמס' בינארי, חסר m - $k=0$. אז

$$m = \sum_k n_k 2^k$$

ולכן $k, \dots, 0, 1, \dots, n_k$.

$$m^n = \prod_{k: n_k=1} m^{2^k}$$

זה דורש $\geq N-1$ כפלים.

אם M מס' הביטים של ההצגה של m , אז כל המספרים שמתקבלים בחישוב ניתנים להצגה באורך MN ביטים.

סה"כ, סיבוכיות הזמן $O(N \text{ mult}(MN, MN))$.

משפט השאלה הסיני:

(סונגזי - המאה ה-5 לספירה) מקרה פרטי

אריאקתאה - אלף - המאה ה-6

המאה ה-7 - אלף - המאה ה-7

פיקונאזי - 1202

צ'ין עיוסאו - 1247

סאוס - אלף (חתיק יתק) - 1801

מקרים פרטיים



המקרה הכללי

ניסוח מודרני

יהיו $n_1, n_2, \dots, n_k \in \mathbb{N}$ זרים לזוג $\gcd(n_i, n_j) = 1 \quad i \neq j$.
 יהיו $r_1, r_2, \dots, r_k \in \mathbb{N}$ כאלו $n = \prod_{i=1}^k n_i$.

זרים הם $0 \leq r_i < n_i, i$ אזי, קיים $x \in \mathbb{N}$ יחיד
 עבורו $0 \leq x < n$ וכל i , $x \equiv r_i \pmod{n_i}$.

הוכחה: יחידות נקבעת מכך שאם יש שני פתרונות x, y
 אז לכל i , $x - y \equiv 0 \pmod{n_i}$ ולכן $x - y \equiv 0 \pmod{n}$,
 כלומר $0 \leq x, y < n$ ולכן חייב להיות $x - y = 0$.

כדי להוכיח קיום, נראה אלמנט יחיד. טחטמק את x .
 דעם כך נבדוק האלמנט אוקלידס המופיע:

בהינתן $m, n \in \mathbb{N}$ האלמנט המופיע מחשב את $g = \gcd(m, n)$
 וכל $a, b \in \mathbb{Z}$ עבורם $g = am + bn$.

האלמנט מממש את האינדוקציה הבאה:

זאתים $q_k \in \mathbb{N}$ וזאתו $0 \leq r_k = r_{k-2} - q_k r_{k-1} < r_{k-1}$ (זה האלמנט היחיד)

$$s_k = s_{k-2} - q_k s_{k-1}$$

$$t_k = t_{k-2} - q_k t_{k-1}$$

נחת תנאי ההתקנה:
 (נעזר בהחלפה של האלמנטים)
 $r_{-2} = m, r_{-1} = n$
 $s_{-2} = 1, s_{-1} = 0$
 $t_{-2} = 0, t_{-1} = 1$

כאשר מקבלים $r_\ell = 0$ הטרצואה היא:
 $g = r_{\ell-1}$
 $a = s_{\ell-1}$
 $b = t_{\ell-1}$

נשתמש בזה כך.

ראשית, נניח ש- $k=2$ (במספר השאלה הישן).

$\gcd(n_1, n_2) = 1$ ז"ל פי הנחת המספר ולכן ניתן למצוא

$a_1, a_2 \in \mathbb{Z}$ עבורם $a_1 n_1 + a_2 n_2 = 1$.

הפיתרון המקסימלי הוא

$$x = r_1 a_2 n_2 + r_2 a_1 n_1$$

זה כי:

$$= r_1 (1 - a_1 n_1) + r_2 a_1 n_1$$

$$= r_1 + (r_2 - r_1) a_1 n_1 \equiv r_1 \pmod{n_1}$$

ובאלתר אלפן $x \equiv r_2 \pmod{n_2}$.

כדי לפתור עבור $k > 2$, נמצא פיתרון $r_{1,2}$ עבור שתי המשוואות הראשונות ואז נחליף אתן במשוואה $x \equiv r_{1,2} \pmod{n_1, n_2}$ באינדוקציה, למחרת של ו- k משוואות כאלו יש פיתרון אלגוריתמי.

הסיקאלית: פירופורציות ל- k חישוקי $\gcd$.

שימוש: RSA משמש בין היתר למבטח המסר האלקטרוני באינטרנט

עבור שני ראשוניים גדולים p, q ציג למצוא מבנה פומבי e ז"ל עבורו $\gcd(e, (p-1)(q-1)) = 1$.

המפתח הסודי הוא $d = e^{-1} \pmod{(p-1)(q-1)}$ ואנחנו למעשה קוצרים אלף אלקטרים המורידים כי

$$\gcd(e, (p-1)(q-1)) = 1 = ex + (p-1)(q-1)y \Rightarrow$$

$$\Rightarrow ex \equiv 1 \pmod{(p-1)(q-1)} \Rightarrow x = e^{-1} \pmod{(p-1)(q-1)}$$