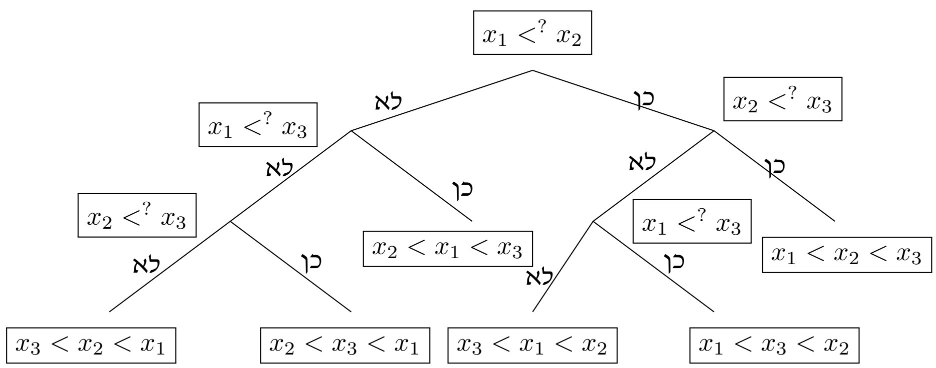
אלגוריתמים קומבינטורים

תקצירי הרצאות - רועי משולם

אלגוריתמים לבעיות סדר

נסמן $[n]=\{1,\ldots,n\}$ ויהא S_n אוסף התמורות על $[n]$.
בעיית המיון: בהנתן סדרת מספרים ממשיים שונים $a=(a_1,\ldots,a_n)$ מצא את התמורה היחידה $\pi\in S_n$ עבורה $a_{\pi(1)}<\ldots<a_{\pi(n)}$. π זו תיקרא התמורה הממיינת של a.
אנו נתרכז באלגוריתמים המשתמשים רק בהשוואות ולא - למשל - בפעולות אלגבריות המנצלות תכונות של הממשיים מעבר ליחס הסדר ביניהם. חישוב במודל זה מתואר על ידי עץ השוואות.
דוגמא:



האלגוריתם מופעל באופן הבא: קלט $a=(a_1,a_2,a_3)$ מגדיר מסלול מהשורש לעלה באופן הבא: כאשר בקודקוד פנימי המסומן ב- $x_i <^? x_j$ משווים בין a_i לבין a_j. אם $a_i<a_j$ ממשיכים ימינה בעץ ואם $a_j<a_i$ ממשיכים שמאלה בעץ. התמורה המופיעה על העלה שבקצה המסלול היא התמורה הממיינת של a.

הערה: נשים לב שבאלגוריתם זה מספר ההשוואות המקסימלי שביצענו על קלט הוא 3. האם יש אלגוריתם למיון שלושה מספרים המבצע לכל היותר 2 השוואות על כל קלט? נענה על שאלה זו בהמשך.

מודל עץ ההשוואות

עץ בינארי T הוא גרף מכוון עם שורש s כך שדרגת היציאה של כל קודקוד ≤ 2. בדרך כלל לא נסמן חץ על צלע אלא נבין שכיוון הצלע הוא מלמעלה למטה. עלים הם קודקודים עם דרגת יציאה 0. הבנים הימני והשמאלי של קודקוד v מסומנים $left(v), right(v)$ בהתאמה (אם הם קיימים). גובה העץ $h(T)$ הוא מספר הצלעות המירבי במסלול מכוון בין שורש לעלה.
יהא T עץ בינארי שבו כל קודקוד פנימי v מתוייג על ידי השוואה $q(v)=x_i <^? x_j$ כאשר $1\le i,j\le n$, וכל עלה v מתוייג על ידי תמורה $\pi(v)\in S_n$.

לכל וקטור $a=(a_1,\dots,a_n)$ של ממשיים שונים נגדיר מסלול

$$Path(a)=(s=v_0,\dots,v_m)$$

מהשורש s לאחד העלים באופן הבא: נניח שהגדרנו את $s=v_0,\dots,v_k$ עד $0\le k$ כלשהו. אם v_k עלה, נגדיר $m=k$ ונסיים. אחרת v_k קדקד פנימי ויהא $q(v_k)=x_i <^? x_j$. נגדיר עתה

$$v_{k+1}=\begin{cases} right(v_k) & a_i<a_j \\ left(v_k) & a_j<a_i \end{cases}$$

העץ המתוייג T ייקרא <u>עץ השוואות למיון n איברים</u> אם לכל $a=(a_1,\dots,a_n)$ כנ"ל מתקיים: $Path(a)=(s=v_0,\dots,v_m)$ גורר ש $\pi(v_m)$ היא התמורה הממיינת של a.
כל אלגוריתם השוואות למיון ניתן לייצוג על ידי עץ השוואות מתוייג T.
<u>סיבוכיות האלגוריתם</u> הינה מספר ההשוואות המירבי שיבצע האלגוריתם T על קלט באורך n, ותסומן $c_T(n)$. סיבוכיות האלגוריתם שווה לגובה עץ ההשוואות T, כלומר $c_T(n)=h(T)$.
בפועל, נוח יותר לתאר אלגוריתמי השוואות על ידי "תוכנית מחשב" המאפשרת בין השאר שמוש בלולאות וקריאות רקורסיביות.

<u>מספר אלגוריתמי מיון</u>

להלן נתאר מספר אלגוריתמי מיון ונעריך את סיבוכיותם.
<u>Insertion Sort</u>
יהא $A=(A_1,\dots,A_n)$ וקטור של ממשיים שונים. המיון מתבצע ב־ m שלבים, כאשר בסוף השלב ה־ i הסדרה החלקית $A(1),\dots,A(i)$ ממויינת. בשלב ה־ $(i+1)$ משווים את $A(i+1)$ בזה אחר זה ל־ $\dots,A(i-1),A(i)$ עד שמוצאים את מקומו ביניהם.
<u>דוגמא:</u>

i	הסדרה בסוף שלב i
1	7 4 5 3 6
2	4 7 5 3 6
3	4 5 7 3 6
4	3 4 5 7 6
5	3 4 5 6 7

תיאור על ידי התוכנית:

```
IS(A,n)
For i = 2 to n
k ← A(i)
j ← i − 1
while (k < A(j) & j ≥ 1)
                    A(j+1) ← A(j)
                    j ← j − 1
A(j+1) ← k
```

<u>טענה:</u>

$$c_{IS}(n)=\binom{n}{2}$$

הוכחה: מספר ההשוואות המבוצעות בשלב i הוא לכל היותר $i-1$. לכן

$$c_{IS}(n) \leq \sum_{i=1}^{n} (i-1) = \left(\begin{array}{c} n \\ 2 \end{array} \right).$$

מאידך על הקלט $A=(n,n-1,\ldots,2,1)$ יבוצעו בדיוק $i-1$ השוואות בשלב i ולכן

$$c_{IS}(n) \geq \sum_{i=1}^{n} (i-1) = \left(\begin{array}{c} n \\ 2 \end{array} \right).$$

$\square$

בעיית המיזוג: נתונים שני וקטורים ממויינים זרים $a=(a_1<\ldots<a_k)$ ו־ $b=(b_1<\ldots<b_l)$ עלינו למיין את הסידרה $c=\{a_i\}_{i=1}^{k}\cup\{b_j\}_{j=1}^{l}$ כך ש: $c=(c_1<\ldots<c_{k+l})$.
להלן אלגוריתם השוואת רקורסיבי הממזג את $a\cup b$ לתוך c.

$merge(a,k,l,b,c)$
If $k=l=0$ stop.
If $k=0$ do $c(j)\leftarrow b(j),\ j=1,\ldots,l$ and stop.
If $l=0$ do $c(i)\leftarrow b(i),\ j=1,\ldots,k$ and stop.
If $a(k)<b(l)$
    $c(k+l)\leftarrow b(l)$
    $merge(a,k,b,l-1,c)$
If $a(k)>b(l)$
    $c(k+l)\leftarrow a(k)$
    $merge(a,k-1,b,l,c)$

נסמן ב־ $c_M(k,l)$ את הסיבוכיות של $merge$ על קלטים (a,b) באורכים (k,l).

טענה 1 אם $(k,l)\neq(0,0)$ אזי $c_M(k,l)\leq k+l-1$.

הוכחה 1 אינדוקציה על $k+l$. המקרים $k=0$ ו־ $l=0$ ברורים. נניח אפוא $k,l\geq 1$. מהתיאור הרקורסיבי של האלגוריתם ומהנחת האינדוקציה נובע כי

$$c_M(k,l) \leq 1+\max\{c_M(k-1,l), c_M(k,l-1)\}$$

$$\leq 1+\max\{(k-1)+l-1, k+(l-1)-1\} = k+l-1.\square$$

אלגוריתם מיון־מיזוג שיתואר להלן הוא דוגמא לשימוש בטכניקה אלגוריתמית הנקראת "הפרד ומשול" (divide and conquer) המבוססת על פיצול הבעיה למספר תת־בעיות קטנות יותר, פתרון כל אחת מהן, ולאחר מכן סינתזה של הפתרונות החלקיים לפתרון מלא.

Merge Sort

$$\boxed{\begin{array}{l} MS(A,n) \\ \text{If } n=1 \text{ stop.} \\ B \leftarrow (A(1),\ldots,A(\lfloor \frac{n}{2} \rfloor)) \\ C \leftarrow (A(\lfloor \frac{n}{2} \rfloor+1),\ldots,A(n)) \\ MS(B,\lfloor \frac{n}{2} \rfloor) \\ MS(C,\lceil \frac{n}{2} \rceil) \\ merge(B,\lfloor \frac{n}{2} \rfloor,C,\lceil \frac{n}{2} \rceil,A) \end{array}}$$

נסמן ב־ $c_{MS}(n)$ את הסיבוכיות של MS על קלט באורך n. מהתיאור הרקורסיבי של האלגוריתם נובע כי אם $n \geq 2$ אזי

$$c_{MS}(n) \leq c_{MS}(\lfloor \frac{n}{2} \rfloor) + c_{MS}(\lceil \frac{n}{2} \rceil) + c_M(\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil)$$

$$\leq c_{MS}(\lfloor \frac{n}{2} \rfloor) + c_{MS}(\lceil \frac{n}{2} \rceil) + n - 1 \tag{1}$$

<u>מסקנה:</u>

$$c_{MS}(2^k) \leq k \cdot 2^k$$

<u>הוכחה:</u> אינדוקציה על k. המקרה $k=0$ ברור. נניח $k \geq 1$ ואזי לפי הנחת האינדוקציה ו־ 1 נקבל

$$c_{MS}(2^k) \leq 2c_{MS}(2^{k-1}) + c_M(2^{k-1}, 2^{k-1}) \leq$$

$$2(k-1) \cdot 2^{k-1} + 2^k - 1 = k \cdot 2^k - 1 < k \cdot 2^k$$

□

<u>מסקנה:</u> לכל $n \geq 1$ מתקיים

$$c_{MS}(n) \leq 2n \log_2 n + 2n.$$

<u>הוכחה:</u> יהא k כך ש־ $2^{k-1} < n \leq 2^k$. אזי $2^k < 2n$ ולכן

$$c_{MS}(n) < c_{MS}(2^k) = k2^k < 2n \log_2 n = 2n \log_2 n + 2n.$$

□

תרגיל: הוכח באינדוקציה על n ובעזרת (1) כי

$$c_{MS}(n) \le n\lceil \log_2 n \rceil \le n\log_2 n + n.$$

סיבוכיות בעיית המיון

נסמן ב־$C_{sort}(n)$ את $\min C_A(n)$ כאשר A עובר על כל אלגוריתמי הסדר למיון n איברים.
מהתרגיל נובע כי

$$C_{sort}(n) \le C_{MS}(n) \le n\log_2 n + n$$

נראה כי סיבוכיות זו אופטימלית עד כדי הקבוע הכפלי של n. יהא $L(T)$ מספר העלים בעץ בינארי T.

טענה: $L(T) \le 2^{h(T)}$.

הוכחה: אינדוקציה על $h = h(T)$. המקרה $h = 0$ ברור. נניח $h > 0$ ויהיו T_1, T_2 העצים הנטועים בבנים של השורש. אזי $h(T_i) \le h(T) - 1$ ולכן לפי הנחת האינדוקציה

$$L(T) = L(T_1) + L(T_2) \le 2^{h(T_1)} + 2^{h(T_2)} \le 2^{h(T)-1} + 2^{h(T)-1} = 2^{h(T)}.$$

$\square$

מסקנה: $C_{sort}(n) \ge \log_2 n!$

הוכחה: יהא T עץ השוואות לסדרות באורך n כך ש־ $C_{sort}(n) = h(T)$.
מכיוון שכל תמורה $\pi \in S_n$ היא תמורה ממיינת של סדרה מסויימת הרי ש־ $L(T) \ge n!$ ולכן

$$C_{sort}(n) = h(T) \ge \log_2 L(T) \ge \log_2 n!$$

$\square$

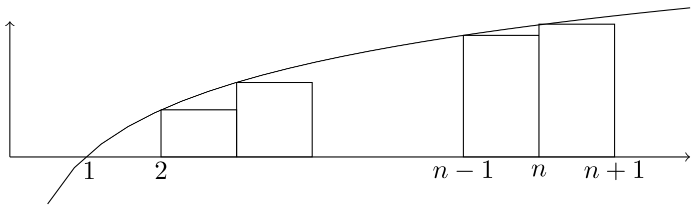
הערכה אסימפטוטית ל־ $\log_2 n!$

הפונקציה $\ln x$ היא מונוטונית עולה וחיובית באינטרוול $[1, \infty)$. לכן

$$\sum_{j=1}^{n} \ln j \le \int_2^{n+1} \ln x dx = [x\ln x - x]|_2^{n+1} =$$

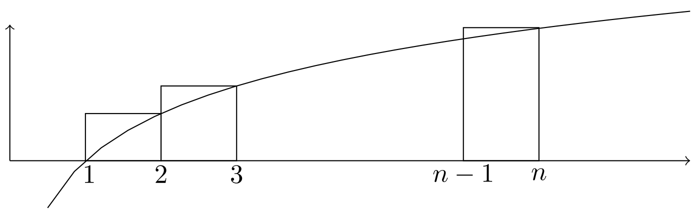
$$(n+1)\ln(n+1) - (n+1) - (2\ln 2 - 2)$$

$$\le (n+1)\ln(n+1) - (n+1).$$



וגם

$$\sum_{j=1}^{n}\ln j \geq \int_1^n \ln x dx$$
$$= [x\ln x - x]|_1^n = n\ln n - n + 1.$$



מסקנה: $n\log_2 n - O(n) \leq \log_2 n! \leq n\log_2 n + O(n)$

מסקנה: $C_{sort}(n) \geq \log_2 n! \geq n\log_2 n - O(n)$

עוד על בעיית המיזוג

נחזור לבעיית המיזוג: בהינתן שני וקטורים ממויינים זרים

$$a = (a_1 < \ldots < a_k)\ ,\ b = (b_1 < \ldots < b_l)$$

עלינו למיין את $a\cup b$. נסמן ב־ $C_{merge}(k,l)$ את סיבוכיות הבעיה. ראינו אלגוריתם פשוט למיזוג שסיבוכיותו מקיימת $c_M(k,l) \leq k+l-1$ לכן $C_{merge}(k,l) \leq k+l-1$.

טענה:

$$C_{merge}(k,l) \geq \left\lceil \log_2 \begin{pmatrix} k+l \\ k \end{pmatrix} \right\rceil$$

הוכחה: נעיין בעץ השוואות T לבעיית המיזוג של הוקטור $x = (x_1 < \ldots < x_k)$ עם $y = (y_1 < \ldots < y_l)$. כל קודקוד פנימי בעץ מתוייג ע"י $x_i \overset{?}{<} y_j$ וכל עלה מתוייג על ידי תמורה על $\{x_i\}_{i=1}^k \cup \{y_j\}_{j=1}^l$ שבה $x_1 < \ldots < x_k$ וגם $y_1 < \ldots < y_l$. כמו כן כל תמורה המקיימת אילוצים אלה מופיעה על אחד מהעלים. מספר התמורות על $\{x_i\}_{i=1}^k \cup \{y_j\}_{j=1}^l$ שעבורן מתקיים $x_1 < \ldots < x_k$ וגם $y_1 < \ldots < y_l$ הוא $\begin{pmatrix} k+l \\ k \end{pmatrix}$.

לכן $2^{h(T)} \geq \begin{pmatrix} k+l \\ k \end{pmatrix}$ ולכן $h(T) \geq \left\lceil \log_2 \begin{pmatrix} k+l \\ k \end{pmatrix} \right\rceil$.

$\square$

<u>מסקנה:</u> $\left\lceil \log_2 \begin{pmatrix} k+l \\ k \end{pmatrix} \right\rceil \leq C_{merge}(k,l) \leq k+l-1$

להלן נדון בשני המקרים הקיצוניים $k=l$ ו־ $k=1$.
<u>המקרה $l=1$:</u>
בהינתן $A=(a_1<\ldots<a_k)$ ו־ b עלינו למצוא $0 \leq i \leq k$ עבורו $a_i < b < a_{i+1}$ (כאשר מגדירים $a_0=-\infty$ ו־ $a_{k+1}=\infty$).
דרך יעילה לבצע זאת היא על ידי חיפוש בינארי:

```
BS(A, k, b, i)
    If k = 1 & A(1) < b then i = 1, stop.
    If k = 1 & A(1) > b then i = 0, stop.
If b > A(⌈k/2⌉)
            A' = (A(⌈k/2⌉ + 1), ..., A(k))
            BS(A', ⌊k/2⌋, b, i)
            i ← i + ⌈k/2⌉
If b < A(⌈k/2⌉)
            A'' = (A(1), ..., ⌈k/2⌉ − 1))
            BS(A'', ⌈k/2⌉ − 1, b, i)
```

נסמן ב־ $c_{BS}(k)$ את הסיבוכיות של חיפוש בינארי כאשר A באורך k.

<u>טענה:</u>

$$c_{BS}(k) \leq \lceil \log_2 (k+1) \rceil$$

<u>הוכחה:</u> מתיאור האלגוריתם נובע כי $c_{BS}(1)=1$ וכי לכל $k>1$ מתקיים

$$c_{BS}(k) \leq 1+\max\{c_{BS}(\lfloor \frac{k}{2} \rfloor), c_{BS}(\lceil \frac{k}{2} \rceil -1)\} \leq 1+c_{BS}(\lfloor \frac{k}{2} \rfloor)$$

נניח $2^{t-1} \leq k \leq 2^t-1$ אזי

$$c_{BS}(k) \leq 1+c_{BS}(\lfloor \frac{k}{2} \rfloor) \leq 1+\left\lceil \log_2 \left(\lfloor \frac{k}{2} \rfloor +1 \right) \right\rceil \leq 1+\lceil \log_2 2^{t-1} \rceil = t = \lceil \log_2 (k+1) \rceil$$

$\square$

<u>מסקנה:</u>

$$C_{merge}(k,1) = \lceil \log_2 (k+1) \rceil$$

<u>שימוש של חיפוש בינארי למיון</u>
אם נחליף ב־ Insertion sort את החיפוש הסדרתי בחיפוש בינארי נקבל אלגוריתם מיון יעיל המתואר להלן:

$BIS(A,n)$ For $i=2$ to n Binary insert $A(i)$ into $A(1)<\ldots<A(i-1)$

נסמן ב־ $c_{BIS}(n)$ את סיבוכיות $BIS(A,n)$. אזי $c_{BIS}(1)=0$ ולכל $n\geq 1$ מתקיים

$$c_{BIS}(n)\leq c_{BIS}(n-1)+c_{merge}(n-1,1)=c_{BIS}(n-1)+\lceil\log_2 n\rceil$$

<u>מסקנה:</u>

$$c_{BIS}(n)\leq\sum_{i=1}^{n}\lceil\log_2 n\rceil\leq n\lceil\log_2 n\rceil$$

$\square$

<u>המקרה $k=l$:</u>
במקרה זה

$$2k-\log_2(2k+1)=\log_2\frac{2^{2k}}{2k+1}\leq\log_2\left(\begin{array}{c}2k\\k\end{array}\right)\leq C_{merge}(k,k)\leq 2k-1$$

<u>טענה:</u>

$$C_{merge}(k,k)=2k-1.$$

<u>הוכחה:</u> נגדיר שתי סדרות באורך k: $a=(a_1,\ldots,a_k)$, $b=(b_1,\ldots,b_k)$ כאשר

$$a_i=2i-1,\quad b_i=2i.$$

יהי T עץ ההשוואות של אלגוריתם למיזוג שתי סדרות באורך k, ויהא P המסלול שעובר הזוג (a,b) על T. העלה שבקצה המסלול מתוייג על ידי התמורה

$$x_1<y_1<x_2<y_2<\cdots<x_k<y_k$$

נראה כי כל ההשוואות מהצורות

$$x_t<y_t,\quad 1\leq t\leq k$$

ו־

$$y_t<x_{t+1},\quad 1\leq t\leq k-1$$

מופיעות על קודקוד פנימי כלשהוא במסלול P.

(א) נניח בשלילה כי $x_t <^? y_t$ לא מופיע ב־ P. נגדיר $a^{'} = \{a_i^{'}\}_{i=1}^{k}$ ו־ $b^{'} = \{b_j^{'}\}_{j=1}^{l}$ על ידי

$$a_i^{'} = \begin{cases} a_i & i \neq t \\ b_t & i = t \end{cases}$$

ו־

$$b_i^{'} = \begin{cases} b_i & i \neq t \\ a_t & i = t \end{cases}$$

נשים לב כי אם $i \neq j$ או $i = j \neq t$ אזי $a_i^{'} < b_j^{'} \leftrightarrow a_i < b_j$, ולכן מכיוון שההשוואה $x_t < y_t$ אינה מופיעה ב־ P הרי שהזוג $(a^{'}, b^{'})$ יתקדם באותו מסלול כמו הזוג (a, b), ולפיכך יסיים בתמורה $x_1 < y_1 < \ldots, x_k < y_k$ בסתירה לכך ש־ $a_t^{'} \not< b_t^{'}$.

(ב) נניח בשלילה כי $y_t <^? x_{t+1}$ לא מופיע ב־ P. נגדיר $a^{''} = \{a_i^{''}\}_{i=1}^{k}$ ו־ $b^{''} = \{b_j^{'}\}_{j=1}^{l}$ על ידי

$$a_i^{''} = \begin{cases} a_i & i \neq t+1 \\ b_t & i = t+1 \end{cases}$$

ו־

$$b_i^{''} = \begin{cases} b_i & i \neq t \\ a_{t+1} & i = t \end{cases}$$

שוב $a_i^{''} < b_j^{''} \leftrightarrow a_i < b_j$ אלא אם $(i, j) = (t+1, t)$. ולכן אם ההשוואה $y_t < x_{t+1}$ אינה מופיעה ב־ P הרי ש־ $(a^{''}, b^{''})$ יעבור אותו מסלול כמו (a, b) ולפיכך יסיים בתמורה $x_1 < y_1 < \ldots, x_k < y_k$ בסתירה לכך ש־ $b_t^{''} < a_{t+1}^{''}$.

מ־(א) ו־(ב) נובע כי המסלול P הינו באורך לפחות $2k+1$ ולכן $C_{merge}(k, k) \geq 2k - 1$.

$\square$

ערימות

נסמן $\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}$ ונגדיר ל־ $i \in \mathbb{N}$

$$left(i) = 2i, \quad right(i) = 2i + 1.$$

העץ הבינארי האינסופי הוא הגרף המכוון על קבוצת הקודקודים $\mathbb{N}$ שצלעותיו הן $(i, left(i)), (i, right(i))$ לכל $i \geq 1$. עץ בינארי T על n קודקודים ייקרא מאוזן אם הוא איזומורפי לתת הגרף של העץ הבינארי האינסופי המושרה על קבוצת הקודקודים $[n] = \{1, \ldots, n\}$.

יהא T עץ בינארי מאוזן על קבוצת הקודקודים V, $|V| = n$ ויהא $A = (A(v))_{v \in V}$ מערך המאונדקס על ידי V. A ייקרא ערימה אם לכל $v \in V$ מתקיים

$$A(v) \geq \max\{A(left(v)), A(right(v))\}.$$

(כמובן, נתייחס ל־ $left(v), right(v)$ רק אם הם מוגדרים.)

לקודקוד $u \in V$ נסמן ב־ T_u את תת העץ הנטוע ב־ u.

בניית ערימה

דרך אחת להפוך מערך $(A(v))_{v \in V}$ לערימה היא על ידי מיון הדורש $O(n \log n)$ השוואות: אנו נתאר אלגוריתם יעיל יותר הדורש רק $O(n)$ השוואות. האלגוריתם ישתמש בשגרת עזר הפותרת את הבעייה הבאה: נניח כי $v \in V$ וכי צמצום A ל־ $T_{left(v)}$ הוא ערימה וכן צמצום A ל־ $T_{right(v)}$ הוא ערימה.

$Heapify(A, n, v)$ המתוארת להלן הופכת את A המצומצם ל־ T_v לערימה:

```
Heapify(A, n, v)
if A(v) ≥ max{A(left(v)), A(right(v))} stop.
else if A(left(v)) > A(v)

        exchange  A(left(v)) & A(v)
        Heapify(A, n, left(v))

else

        exchange  A(right(v)) & A(v)
        Heapify(A, n, right(v))
```

נסמן ב־ $height(v)$ את גובה העץ T_v, אזי הסיבוכיות של $Heapify(A, n, v)$ הינה $O(height(v))$.

בניית ערימה מתבצעת על ידי האלגוריתם הבא:

```
makeheap(A,n)
  For i = n down to 1
  Heapify(A, n, i)
```

יהא $2^m \leq n \leq 2^{m+1} - 1$ אזי הסיבוכיות של $makeheap$ הינה

$$O\left(\sum_{i=1}^{n} height_T(i)\right) = O\left(\sum_{i=1}^{2^{m+1}-1} height_T(i)\right) =$$

$$O(\sum_{j=0}^{m}(m-j)2^j) = O(\sum_{j=0}^{m} j2^{m-j})$$
$$\leq O(2^m)\sum_{j=0}^{\infty} j2^{-j}.$$

עתה

$$\sum_{j=0}^{\infty} jx^j = x(\sum_{j=1}^{\infty} jx^{j-1}) = x(\sum_{j=0}^{\infty} x^j)'$$
$$= x\cdot(\frac{1}{1-x})' = \frac{x}{(1-x)^2}.$$

ולכן $\sum_{j=1}^{\infty} j2^{-j} = 2$. לכן הסיבוכיות של $makeheap(A,n)$ היא $O(2^m) = O(n)$.

מיון ערימה

```
Heapsort(A, n)

makeheap(A, n)
  For i = n down to 2
  exchange A(1) ↔ A(i)
  Heapify({A(1), ..., A(i − 1)}, 1)
```

הסיבוכיות של Heapsort חסומה על ידי

$$C_{Heapsort}(n) \leq C_{Makeheap}(n) + (n-1)O(\log n) \leq O(n\log n)$$

בחירה

תהא $A = (a_1, \ldots, a_n)$ סדרה עם תמורה ממיינת $\pi \in S_n$, $a_{\pi(1)} < \ldots < a_{\pi(n)}$.
נגדיר

$$sel(A,k) = a_{\pi(k)}.$$

למשל $sel(A,n) = \max A, \quad sel(A,1) = \min A$.

נסמן ב־ $C(n,k)$ את הסיבוכיות של חשוב $sel_k(A)$ עבור $|A| = n$. מיון מלא נותן כמובן את $sel(A,k)$ לכל $1 \leq k \leq n$, ולכן $C_{sel}(n,k) \leq O(n\log n)$. בהמשך נראה כי קיים קבוע מוחלט $\widetilde{c}$ כך שלכל k מתקיים $C_{sel}(n,k) \leq \widetilde{c}n$.

טענה:

- $C_{sel}(n,1) = n-1$
- $C_{sel}(n,2) = n + \lceil\log_2 n\rceil - 2$

נתאר עתה אלגוריתם רקורסיבי $Sel(A,n,k)$ המוצא את $sel(A,k)$ של סדרה A באורך n.

<u>$Sel(A,n,k)$</u>

(א) נחלק את A לחמישיות $F_1,\dots,F_{\frac{n}{5}}$ ונמצא את החציון של כל חמישייה:

$$b_i \leftarrow Sel(F_i,5,3)$$

יהא $B=(b_1,\dots,b_{\frac{n}{5}})$ וקטור החציונים.

(ב) יהא $x \leftarrow Sel(B,\frac{n}{5},\frac{n}{10})$ החציון של B.

(ג) נחשב:

$$C=\{a_i \in A : a_i < x\}$$

$$D=\{a_i \in A : a_i > x\}$$

(ד)

$$Sel(A,n,k) \leftarrow \begin{cases} Sel(C,|C|,k) & |C| \geq k \\ x & |C| = k-1 \\ Sel(D,|D|,k-|C|-1) & |C| \leq k-2 \end{cases}$$

נסמן ב־ $c_{Sel}(n,k)$ את הסיבוכיות של האלגוריתם $Sel(A,n,k)$ ונסמן $\widetilde{S}(n)=\max_{1\leq k\leq n} c_{Sel}(n,k)$. הערכת $S(n,k)$ מבוססת על העובדה הבאה:

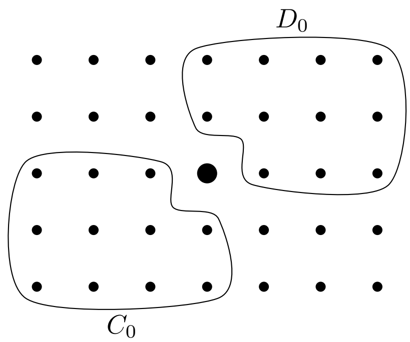
<u>טענה</u>: C,D המתקבלות בצעד 3 באלגוריתם מקיימות

$$|C|,|D| \leq \frac{7n}{10}$$

הוכחה: יהיו

$$C_0 = \bigcup_{\{i:b_i<x\}} \{y \in F_i : y \le b_i\} \subset C$$

$$D_0 = \bigcup_{\{i:b_i>x\}} \{y \in F_i : y \ge b_i\} \subset D$$



אזי

$$|C| \ge |C_0| \ge \frac{3n}{10}$$

$$|D| \ge |D_0| \ge \frac{3n}{10}$$

ולכן

$$|C| \le n - |D| \le \frac{7n}{10}$$

$$|D| \le n - |C| \le \frac{7n}{10}$$

$\square$

הערכת סיבוכיות $Sel(A,n,k)$
נעריך את מספר ההשוואות בכל אחד מהשלבים באלגוריתם:

(א) $2n = \frac{n}{5}\cdot\binom{5}{2} \ge \frac{n}{5}\cdot c_{Sel}(5,3)$ השוואות למציאת ה־ b_i-ים.

(ב) $c_{Sel}(\frac{n}{5},\frac{n}{10})$ השוואות למציאת x.

(ג) n השוואות לקביעת C,D.

(ד) $\max_\alpha c_{Sel}(\frac{7n}{10},\alpha)$ השוואות למציאת $sel(C,k)$ ו־ $sel(D,|C|-k-1)$.

לכן

$$c_{Sel}(n,k) \le 2n + c_{Sel}\left(\frac{n}{5},\frac{n}{10}\right) + n + \max_\alpha c_{Sel}\left(\frac{7n}{10},\alpha\right) \le 3n + \widetilde{S}(\frac{n}{5}) + \widetilde{S}(\frac{7n}{10})$$

ולכן

$$\widetilde{S}(n) \le 3n + \widetilde{S}(\frac{n}{5}) + \widetilde{S}(\frac{7n}{10})$$

למה:
אם $g(n) \le \sum_{i=1}^m g(\theta_i n) + cn$ כאשר $\sum_{i=1}^m \theta_i < 1$, אזי

$$g(n) \le \frac{Cn}{1-\sum_{i=1}^m \theta_i}.$$

$\square$

<u>מסקנה:</u>

$$c_{Sel}(n,k) \le \widetilde{S}(n) \le \frac{3n}{1-\frac{1}{5}-\frac{7}{10}} = 30n$$

קידוד חסר רעש (noiseless) coding

הבעייה: נתון קובץ הכתוב באלף בית סופי $x_1,\dots,x_n$. ברצוננו לקודד אותו בתווים בינאריים כך שיתקיים:

(א) אפשר יהיה לשחזר את הקובץ המקורי מהקובץ המקודד.

(ב) הקובץ המקודד יהיה באורך מינימלי.

<u>דוגמא:</u> האלף בית הוא $\{A,B,C,D\}$. בקובץ N אותיות עם טבלת השכיחויות הבאה:

אות	A	B	C	D
שכיחות	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$

<u>פתרון א:</u>

אות	A	B	C	D
קוד	00	01	10	11

הקובץ המקודד הוא באורך

$\frac{N}{2}\cdot 2+\frac{N}{4}\cdot 2+\frac{N}{8}\cdot 2+\frac{N}{8}\cdot 2 = 2N$ ביטים

<u>פתרון ב:</u>

אות	A	B	C	D
קוד	0	10	110	111

הקובץ המקודד הוא באורך

$\frac{N}{2}\cdot 1+\frac{N}{4}\cdot 2+\frac{N}{8}\cdot 3+\frac{N}{8}\cdot 3 = 1.75N$ ביטים

אנו רואים כי בחירה מושכלת של הקוד יכולה לשפר משמעותית את אורך הקובץ המקודד.

<u>הגדרה:</u> <u>צופן רישא</u> הוא אוסף מילים בינאריות $w_1,\dots,w_M \in \{0,1\}^N$ כך שלכל $i \neq j$ המילה w_i איננה רישא של w_j.

<u>טענה:</u> צופן רישא ניתן לפענוח יחיד. כלומר, אם

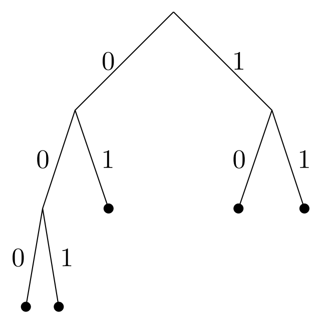
$$w_{i_0}\dots w_{i_s} = w_{j_0}\dots w_{j_t}$$

אזי $s=t$ ומתקיים $i_l = j_l$ לכל $1 \le l \le t$.

<u>טענה:</u> יש התאמה חח"ע בין עצים בינאריים עם M עלים לבין צופני רישא עם M מילים.

<u>הוכחה</u>: נסמן את צלעות העץ הפונות שמאלה ב־ 0 ואת אלה הפונות ימינה ב־ 1. לכל עלה j מתאים את המילה הבינארית המתארת את המסלול מהשורש לעלה. אוסף M המילים המתקבל באופן זה מעץ עם M עלים הוא צופן רישא, וכל צופן רישא מתקבל באופן יחיד.
$\square$

<u>דוגמא</u>:



$$\longleftrightarrow \qquad \{000, 001, 01, 10, 11\}$$

<u>טענה</u>: קיים צופן רישא $\{w_i\}_{i=1}^{M}$ עם אורכים $|w_i| = l_i$ אם ורק אם

$$\sum_{i=1}^{M} 2^{-l_i} \leq 1$$

לפי השקילות בין עצים בינאריים לבין צופני רישא הטענה שקולה ל:

<u>טענה</u>:
קיים עץ בינארי T עם עלים $v_1, \ldots, v_M$ כך ש $h_T(v_i) = l_i$ אם ורק אם

$$\sum_{i=1}^{M} 2^{-l_i} \leq 1$$

(כאן $h_T(v)$ הוא גובה העלה v בעץ T, כלומר המרחק בין השורש לעלה v).

<u>הוכחה</u>:
כיוון $\Leftarrow$: יהא $L = \max_{1 \leq i \leq M} l_i$. יהא T_∞ העץ הבינארי השלם האינסופי. לכל $1 \leq i \leq n$ נסמן

$$A_i = \{v \in T_\infty \ : \ h_{T_\infty}(v) = L, \ v_i \text{ צאצא של } v\}.$$

אזי $|A_i| = 2^{L-l_i}$ ו־ $A_i \cap A_j = \emptyset$ לכל $1 \leq i < j \leq n$ ולכן

$$2^L \geq |\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{M} 2^{L-l_i} \Rightarrow \sum_{i=1}^{M} 2^{-l_i} \leq 1.$$

כיוון $\Rightarrow$: בלי הגבלת הכלליות נניח כי $l_M = \max_{1 \leq i \leq M} l_i$. לפי הנחת האינדוקציה קיים עץ $T^{'}$ עם עלים $v_1, \ldots, v_{M-1}$ כך ש־ $h_{T'}(v_i) = l_i$ לכל $1 \leq i \leq M-1$. יהיו

$$A_i = \{v \in T_\infty \ : \ h_{T_\infty}(v) = l_M, \ v_i \text{ צאצא של } v\}.$$

הקבוצות A_i זרות בזוגות ומקיימות $|A_i| = 2^{l_M - l_i}$.

$$|\bigcup_{i=1}^{M-1} A_i| = \sum_{i=1}^{M-1} |A_i| = \sum_{i=1}^{M-1} 2^{l_M - l_i} \leq 2^{l_M}\left(1 - 2^{-l_M}\right) = 2^{l_M} - 1.$$

לכן קיים קודקוד v_M בגובה l_M שאינו שייך ל־ $\bigcup_{i=1}^{M-1} A_i$ ולכן $\{v_m$ וכל אבותיו$\} T = T^{'} \cup$ הוא העץ הדרוש. $\square$.

נסמן ב־$|w|$ את האורך של מילה בינארית w.

<u>בעיית הקידוד חסר הרעש (noiseless coding):</u>

בהינתן וקטור הסתברויות $p = (p_1, \ldots, p_M)$, $p_i \geq 0$, $\sum_{i=1}^{M} p_i = 1$ מצא צופן רישא $w_1, \ldots, w_M$ כך ש־ $\sum_{i=1}^{M} p_i |w_i|$ הוא מינימלי.

ניסוח שקול: מצא עץ עם עלים $v_1, \ldots, v_M$ כך ש־ $c(T,p) = \sum_{i=1}^{M} p_i h_T(v_i)$ מינימלי.

נסמן $f(p) = \min_T c(T,p)$.

תהא $H(p) = H(p_1, \ldots, p_M) = \sum_{i=1}^{M} p_i \log_2 \frac{1}{p_i}$ פונקציית <u>האנטרופיה</u> המוגדרת על $\{(p_1, \ldots, p_M) \ : \ p_i \geq 0, \ \sum_{i=1}^{n} p_i = 1\}$.

<u>משפט Shannon</u>

$$H(p) \leq f(p) < H(p) + 1$$

<u>הוכחה</u>: בהינתן $p = (p_1, \ldots, p_M)$ נגדיר $l_i = \lceil \log_2 \frac{1}{p_i} \rceil$. אזי

$$\sum_{i=1}^{M} 2^{-l_i} \leq \sum_{i=1}^{M} 2^{-log_2 \frac{1}{p_i}} = \sum_{i=1}^{M} p_i = 1$$

ולכן קיים עץ בינארי T עם עלים $v_1, \ldots, v_M$ כך ש־ $h_T(v_i) = l_i$ ולכן

$$f(p) \leq \sum_{i=1}^{M} p_i l_i = \sum_{i=1}^{M} p_i \lceil \log_2 \frac{1}{p_i} \rceil < \sum_{i=1}^{M} p_i (\log_2 \frac{1}{p_i} + 1) = H(p) + 1$$

הפונקציה $g(y) = \log_2(y)$ קמורה ולכן לכל $y_1, \ldots, y_M$ ו־ $p = (p_1, \ldots, p_M)$ כך ש־ $\sum_{i=1}^{M} p_i = 1$, $p_i \geq 0$ מתקיים

$$g\left(\sum_{i=1}^{n} p_i y_i\right) \geq \sum_{i=1}^{n} p_i g(y_i)$$

יהא $w_1,\dots,w_M$ צופן רישא עם אורכים $l_1,\dots,l_M$. אזי $\sum_{i=1}^M 2^{-l_i} \le 1$ ולכן

$$0 \ge \log_2 \sum_{i=1}^M 2^{-l_i} = \log_2 (\sum_{i=1}^M p_i \frac{2^{-l_i}}{p_i})$$

$$\ge \sum_{i=1}^M p_i \log_2 \frac{2^{-l_i}}{p_i} = \sum_{i=1}^M p_i \log_2 \frac{1}{p_i} + \sum_{i=1}^M p_i \log_2 2^{-l_i} = H(p) - \sum_{i=1}^M p_i l_i$$

$\square$

<u>דוגמא:</u> $p = (\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8})$. ראינו כי $f(p) \le 1.75$. מצד שני, לפי משפט שנון:

$$f(p) \ge H(p) = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{8}\log_2 8 + \frac{1}{8}\log_2 8 = 1.75.$$

לכן הצופן שתיארנו הוא אופטימלי.

<u>אלגוריתם Huffman למציאת $f(p_1,\dots,p_M)$</u>

<u>משפט:</u> יהיו $p_1 \ge \dots p_{M-1} \ge p_M$, $\sum_{i=1}^M p_i = 1$, $p_i \ge 0$. אזי

$$f(p_1,\dots,p_M) = f(p_1,\dots,p_{M-2},p_{M-1}+p_M) + p_{M-1} + p_M$$

<u>הוכחה:</u> כוון אחד: יהא $T^{'}$ עץ אופטימלי עבור הוקטור $p^{'} = (p_1,\dots,p_{M-2},p_{M-1}+p_M)$ עם עלים $v_1,\dots,v_{M-2},v^{'}_{M-1}$. ניצור מ־ $T^{'}$ עץ חדש T על ידי פיצול $v^{'}_{M-1}$ לשני בניו v_{M-1},v_M. אזי

$$c(T^{'},p^{'}) = \sum_{i=1}^{M-2} p_i h_{T'}(v_i) + (p_{M-1}+p_M) h_{T'}(v^{'}_{M-1})$$

לכן:

$$c(T,p) = \sum_{i=1}^{M-2} p_i h_T(v_i) + p_{M-1} h_T(v_{M-1}) + p_M h_T(v_M)$$

$$= \sum_{i=1}^{M-2} p_i h_{T'}(v_i) + p_{M-1}(h_{T'}(v^{'}_{M-1})+1) + p_{M-2}(h_{T'}(v^{'}_{M-1})+1)$$

$$= c(T^{'},p^{'}) + p_{M-1} + p_M$$

ולכן

$$f(p_1,\dots,p_M) \le c(T,p) = c(T^{'},p^{'}) + p_{M-1} + p_M$$

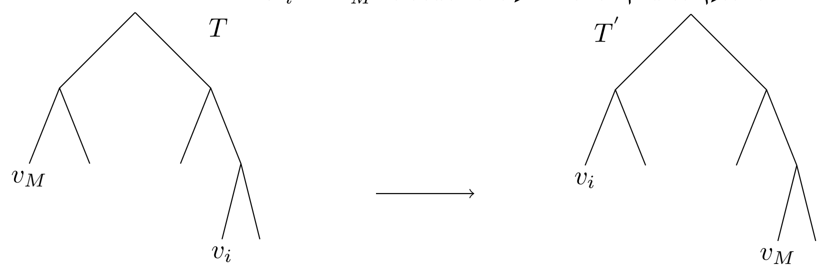
$$= f(p_1,\dots,p_{M-2},p_{M-1}+p_M) + p_{M-1} + p_M$$

כוון שני: יהא T עץ אופטימלי ל־ $p = (p_1,\dots,p_M)$, $p_1 \ge \dots \ge p_M$. אם העלים של T הם $v_1,\dots,v_M$ אזי מתקיים $f(p) = \sum_{i=1}^M p_i h_T(v_i)$.

יהא $1 \le i \le M$ כך ש־

$$h_T(v_i) = \max\{h_T(v_j) : 1 \le j \le M\}$$

נסמן ב־ $T^{'}$ את העץ המתקבל מ־ T על ידי החלפת v_M ב־ v_i.



טענה: $T^{'}$ עץ אופטימלי ל־ P.

הוכחה:

$$c(T^{'},p) - c(T,p) = [h_{T'}(v_i)p_i + h_{T'}(v_M)p_M] - [h_T(v_i)p_i + h_T(v_M)p_M]$$

$$= [h_T(v_M)p_i + h_T(v_i)p_M] - [h_T(v_i)p_i + h_T(v_M)p_M]$$

$$= (h_T(v_M) - h_T(v_i))(p_i - p_M) \le 0$$

לכן $c(T^{'},p) \le c(T,p)$. $\square$

מהטענה נובע כי קיים T אופטימלי כך ש־ $h_T(v_M) = \max_{1\le i\le M} h_T(v_i)$. מאופטימליות T נובע כי v_M אינו בן יחיד שהרי אז אפשר היה להחליפו באביו ולהקטין את $c(T,p)$. לכן לאביו של v_M יש צאצא נוסף v_i. ממקסימליות $h_T(v_M)$ נובע כי v_i הוא אחיו של v_M.

יהא v_j כך ש־ $h_T(v_j) = \max\{h_T(v_k) : k \neq M\}$ ויהא $T^{'}$ העץ המתקבל מהחלפת v_j ו־ v_{M-1}.

טענה: $T^{'}$ עץ אופטימלי ל־ p.

הוכחה:

$$c(T^{'},p) - c(T,p) = [h_{T'}(v_j)p_j + h_{T'}(v_{M-1})p_{M-1}] - [h_T(v_j)p_j + h_T(v_{M-1})p_{M-1}]$$

$$= [h_T(v_{M-1})p_j + h_T(v_j)p_{M-1}] - [h_T(v_j)p_j + h_T(v_{M-1})p_{M-1}]$$

$$= (h_T(v_{M-1}) - h_T(v_j))\,(p_j - p_{M-1}) \le 0$$

ולכן $c(T^{'},p) = c(T,p)$. $\square$

מהטענות נובע כי קיים T אופטימלי שבו v_{M-1}, v_M אחים. נגדיר את S להיות עץ עם עלים $u_1, \ldots, u_{M-1}$ על ידי:

$$u_i = \begin{cases} v_i & 1 \leq i \leq M-2 \\ \text{parent}(v_{M-1}) = \text{parent}(v_M) & i = M-1 \end{cases}$$

ויהא $q = (q_1, \ldots, q_{M-1}) = (p_1, \ldots, p_{M-2}, p_{M-1} + p_M)$. אזי

$$c(S,q) = \sum_{i=1}^{M-1} q_i h_S(u_i) = \sum_{i=1}^{M-2} p_i h_T(v_i) + (p_{M-1} + p_M) h_S(u_{M-1})$$

$$= \sum_{i=1}^{M-2} p_i h_T(v_i) + (p_{M-1} + p_M)(h_T(v_{M-1}) - 1)$$

$$= \sum_{i=1}^{M} p_i h_T(v_i) - (p_{M-1} + p_M) = c(T,p) - (p_{M-1} + p_M)$$

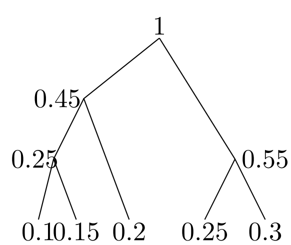
לפיכך

$$f(p_1, \ldots, p_{M-2}, p_{M-1} + p_M) = f(q) \leq f(p) - (p_{M-1} + p_M)$$

$\square$

<u>אלגוריתם הופמן למציאת קוד רישא אופטימלי ל־ $p = (p_1, \ldots, p_M)$:</u> מצא את שני האיברים המינימליים ב־ p. בלי הגבלת הכלליות $p_1, \ldots, p_{M-2} \geq p_{M-1}, p_M$. מצא ברקורסיה קוד רישא אופטימלי ל־ $q = (p_1, \ldots, p_{M-2}, p_{M-1} + p_M)$ ופצל את הקודקוד המתאים ל־ $p_{M+1} + p_M$ לשני בניו.

דוגמא:



$\longrightarrow \{000, 001, 01, 10, 11\}$

עצים ויערות

גרף $G=(V,E)$ ייקרא קשיר אם יש בו מסלול בין כל שני קודקודים.
G ייקרא אציקלי או יער אם אינו מכיל מעגלים.
G הוא עץ אם G קשיר ואציקלי.
עץ פורש של G הוא תת גרף $T=(V,E')$, $E'\subset E$ כך ש־ T עץ.
נסמן ב־ $c(G)$ את מספר רכיבי הקשירות של גרף G.

טענה:

(א) כל עץ מכיל עלה.

(ב) אם $T=(V,E)$ עץ אזי $|E|=|V|-1$. באופן כללי: אם $G=(V,E)$ יער אזי $|E|=|V|-c(G)$.

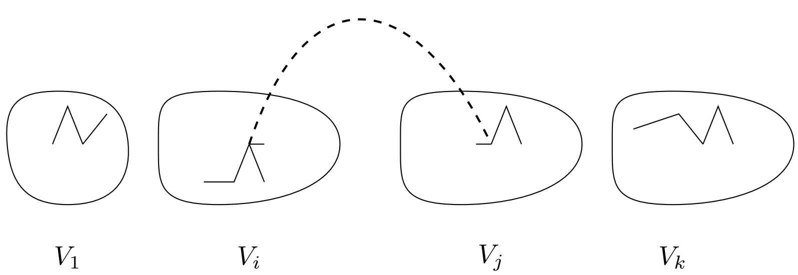
(ג) יהא $G=(V,E)$ גרף קשיר ויהא $F=(V,E')$ יער כאשר $E'\subset E$, אזי קיים עץ פורש $T=(V,E'')$ כך ש ־ $E'\subset E''\subseteq E$.

בפרט: כל גרף קשיר מכיל עץ פורש.

טענה (תכונת החילוף ליערות): יהיו $F_1=(V,E_1)$, $F_2=(V,E_2)$ שני יערות על אותה קבוצת קודקודים V. אם $|E_2|>|E_1|$ אזי קיימת צלע $e\in E_2-E_1$ כך ש־ $(V,E_1\cup\{e\})$ יער.

הוכחה: יהא $k=c(F_1)$ ויהיו $V_1,\ldots,V_k$ קבוצות הקודקודים של רכיבי הקשירות השונים של F_1. נשים לב כי לכל $1\le i\le k$ הגרף $(V_i,\binom{V_i}{2}\cap E_2)$ הוא יער (כי אינו מכיל מעגל) ולכן $|\binom{V_i}{2}\cap E_2|\le|V_i|-1$.

עתה: אם קיימים $1\le i<j\le k$ וצלע $e=\{u,v\}\in E_2$ כך ש־ $u\in V_i, v\in V_j$ אזי $E_1\cup\{e\}$ יער כדרוש.



אחרת $E_2=\bigcup_{i=1}^{k}(E_2\cap\binom{V_i}{2})$ ואזי

$$|E_2|=\sum_{i=1}^{k}|E_2\cap\binom{V_i}{2}|\le\sum_{i=1}^{k}(|V_i|-1)=|V|-k=|E_1|$$

בסתירה להנחה $|E_2| > |E_1|$. $\square$

יהא $G = (V, E)$ גרף קשיר עם פונקציית משקל $w : E \to \mathbb{R}$. ברצוננו למצוא עץ פורש מינימלי (עפ"מ) ב־ G, כלומר עץ $T = (V, E^{'})$ כך ש־ $w(T) = \sum_{e \in E'} w(e)$ מינימלי.
הערה: לפונקציית משקל w יתכנו מספר עצים פורשים מינימליים.

<u>אלגוריתם קרוסקל (Kruskal) למציאת עפ"מ</u>
<u>אתחול:</u> תהא $e_1 \in E$ כך ש־ $w(e_1) = \min\{w(e) : e \in E\}$.
<u>איטרציה:</u> נניח שבחרנו את $e_1, \ldots, e_k$, $1 \leq k \leq n-2$. נבחר צלע e_{k+1} בעלת משקל מינימלי כך שהגוף $(v, \{e_1, \ldots, e_k, e_{k+1}\})$ אציקלי.
נסמן $E' = \{e_1, \ldots, e_{n-1}\}$.

<u>טענה:</u> $(V, E^{'})$ עפ"מ של הגרף הממושקל G.

נוכיח עובדה יותר חזקה.

<u>טענה:</u> יהא $T^{'} = (V, F)$ עץ פורש כלשהוא ב־ G, $F = \{f_1, \ldots, f_{n-1}\}$, כך ש־

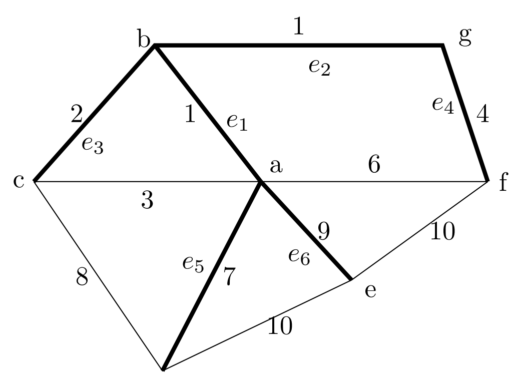
$$w(f_1) \leq \cdots \leq w(f_{n-1}).$$

אזי לכל $1 \leq k \leq n-1$ מתקיים

$$w(e_k) \leq w(f_k)$$

<u>הוכחה:</u> נסמן $F_k = \{f_1, \ldots, f_k\}, E_{k-1} = \{e_1, \ldots, e_{k-1}\}$. (V, E_{k-1}) ו־ (V, F_k) הם יערות ולכן לפי למת החילוף קיימת צלע $f_i \in F_k$ כך ש־ $E_{k-1} \cup \{f_i\}$ יער. לכן לפי בחירת e_k נובע כי $w(f_i) \geq w(e_k)$. מאחר ו־ $w(f_k) \geq w(f_i)$ הרי שגם $w(f_k) \geq w(e_k)$. $\square$

דוגמא:



תיאור מפורט של אלגוריתם קרוסקל: נסמן בכל שלב את רכיב הקשירות של הקודקוד v בעץ המתהווה F על ידי $A(v)$.
<u>אתחול:</u> $F \leftarrow \emptyset$, $A(u) = \{u\}$ לכל $u \in V$.

מיין את צלעות G $w(f_1) \leq \ldots \leq w(f_m)$.
לכל $1 \leq k \leq m$ בצע: תהי $f_k = \{u, v\}$. אם $A(u) \neq A(v)$ אזי $F \leftarrow F \cup \{f_k\}$ ולכל $x \in A(u) \cup A(v)$, $A(x) \leftarrow A(u) \cup A(v)$.

צלעות	רכיבי קשירות	F
ab	ab,c,d,e,f,g	ab
bg	abg,c,d,e,f	ab,bg
bc	abcg,d,e,f	ab,bg,bc
~~ac~~		
gf	abcgf,d,e	ab,bg,bc,gf
~~af~~		
ad	abcdgf,e	ab,bg,bc,gf,ad
~~cd~~		
ae	abcdegf	ab,bg,bc,gf,ad,ad
~~ef~~		
~~ed~~		

<u>ניתוח סיבוכיות אלגוריתם קרוסקל</u>

בכל שלב של האלגוריתם נחזיק אוסף רכיבי קשירות שחלקם ריקים $A_1, \ldots, A_n$. בתחילת האלגוריתם $|A_i| = 1$ לכל $1 \leq i \leq n$. נסמן $\ell_i = |A_i|$ ולכל $v \in V$ יהא $i(v)$ כך ש־ $v \in A_{i(v)}$. בשלב ה־ k בודקים את הצלע ה־ k הקטנה ביותר $f_k = \{u, v\}$.

(I) אם $i(u) = i(v)$ עוברים לצלע הבאה.

(II) אחרת $i(u) \neq i(v)$. אם $\ell_{i(u)} > \ell_{i(v)}$ מאחדים את $A_{i(v)}$ לתוך $A_{i(u)}$ ומעדכנים את $A(*)$ ואת $i(*)$.

ספירת פעולות: $O(|E| \log |E|)$ למיון הצלעות. בדיקת $i(u) = i(v)$ לכל צלע $\{u, v\}$ ובסה"כ $O(|E|)$ השוואות. עבור $|V| - 1$ צלעות מתבצע (II).

<u>טענה</u>: כל קודקוד מוזז/מעודכן $O(log(|V|)$ פעמים.

<u>הוכחה</u>: נשים לב כי אם הקודקוד $v \in A_{i(v)}$ הוזז ל־ $A_{i(u)}$ אזי הקבוצה החדשה של v גדולה לפחות פי שניים מ־ $A_{i(v)}$. לכן מספר ההזזות של קודקוד קטן שווה מ־ $\log |V|$. $\square$

לכן סה"כ פעולות ב־ (II) הוא $O(|V| \log |V|)$ וסה"כ סיבוכיות האלגוריתם היא $O(|E| \log |E|)$.

<u>אלגוריתם פרים PRIM</u>

יהא v_1 קודקוד שרירותי ב־ V. נגדיר באינדוקציה סדרת עצים $T_k = (V_k, E_k)$ כך ש־ $|V_k| = k$, $V_k = \{v_1, \ldots, v_k\} \subset V$, $E_k = \{e_1, \ldots, e_{k-1}\} \subset E$, באופן הבא:
$V_1 = \{v_1\}\ ,\ E_1 = \emptyset$.
נניח שהגדרנו את $T_k = (V_k, E_k)$ עבור $1 \leq k < n - 1$, ונגדיר את T_{k+1}. תהא $e = \{u, v\} \in E(V_k, V - V_k)$ צלע בעלת משקל מינימלי כך ש־ $u \in V_k, v \in V - V_k$. נגדיר $e_k = e\ ,\ v_{k+1} = v$, $V_{k+1} = V_k \cup \{v_{k+1}\}$, $E_{k+1} = E \cup \{e_k\}$ ו־ $T_{k+1} = (V_{k+1}, E_{k+1})$.

<u>טענה</u>: T_n עפ"מ.

<u>הוכחה</u>: נוכיח באינדוקציה על k כי T_k מוכל בעפ"מ. טענה זו ברורה ל $k = 1$.

נניח שהוכחנו זאת ל־ k ויהא $T_k \subset T = (V, F)$ עפ"מ. אם $e_k \in F$ אזי $T_{k+1} \subset T$.
אחרת $e_k \notin F$.
יהא C מעגל ב־ $F \cup \{e_k\}$ ותהא $f \in C - \{e_k\}$ כך ש־ $f \in E(V_k, V - V_k)$. מבחירת e_k נובע כי $w(f) \geq w(e_k)$.
יהא $T^{'} = (V, F - \{f\} \cup \{e_k\})$. אזי $T^{'}$ ע"פ המקיים

$$w(T^{'}) = w(T) - w(f) + w(e_{k+1}) \leq w(T)$$

ולכן $T^{'}$ עפ"מ המכיל את T_{k+1}. $\Box$

<u>ממוש של אלגוריתם PRIM ע"י ערימות</u>

להלן, ערימה תהיה עץ בינארי מאוזן עם משקלות $w(x)$ על הקדקדים x, כך ש

$$w(x) \leq \min\{w(left(x)), w(right(x))\}$$

<u>אלגוריתם PRIM</u>

בכל שלב של האלגוריתם $1 \leq k \leq n$, נחזיק עץ $T_k = (V_k, E_k)$
כאשר $V_k = \{v_1, \ldots, v_k\}$, $E_k = \{e_1, \ldots, e_{k-1}\}$, וכן, ערימה H_k שקדקדיה הם צלעות החתך $(V_k, V - V_k)$ המסודרת לפי המשקלות של הצלעות בגרף המקורי.

אתחול: $E_1 = \emptyset$, $V_1 = \{v_1\}$, H_1־ ערימה על החתך $(v_1, V - v_1)$.

אטרציה: נתונים $T_k = (V_k, E_k)$ ו־ H_k כנ"ל. נבחר את הצלע $e = (u, v)$, $u \in V_k$, $v \in V - V_k$ הנמצאת בשורש H_k.

נגדיר $v_{k+1} = v$, $e_k = e$, $E_{k+1} = E_k \cup \{e_k\}$, $V_{k+1} = V_k \cup \{v_{k+1}\}$.
נעדכן את H_k ל־ H_{k+1}.
בסוף התהליך T_n, עפ"מ.

<u>סבוכיות:</u>
נחשב את סיבוכיות עדכון הערימה H_k לערימה H_{k+1}.
בעדכון זה משמיטים מ־ H_k את כל הצלעות מהצורה xv_{k+1} כאשר $x \in V_k$ ומוסיפים את כל הצלעות מהצורה vy כאשר $y \in V - V_k$.
כל פעולה כזו ניתן לבצע ע"י Heapify ולכן עלותה $O(\log n)$ השוואות.
מאחר שבצענו $degv_{k+1}$ השמטות / הוספות במעבר מ־H_k ל־H_{k+1}, הרי סיבוכיות הכוללת היא:

$$O(\log V \cdot \sum_{v \in V} degv) = O(|E| \log |V|)$$

חיפוש רוחב (BFS)

נתון: גרף מכוון $G=(V,E)$ על $|V|=n$ קדקדים, וקודקוד קבוע $u \in V$.
מטרה: לסרוק את כל קודקודי V החל מ־ u.
אלגוריתם חיפוש רוחב מייצר סידור של הקודקודים $u=v_1,\dots,v_n$ באופן הבא: בכל שלב באלגוריתם יש שתי סדרות של קודקודים S,R.
$S=$ סדרת קודקודים שכבר טופלו. $R=$ סדרת קודקודים שעדיין בטיפול.
נסמן ב־ $\Gamma(v)$ את שכני הקדקד v.
אתחול: $S=\emptyset\ ,\ \ R \leftarrow (u)$.
איטרציה: יהא v הקודקוד השמאלי ב־ R. אם קיים $x \in \Gamma(v)-(S\cup R)$ הוסף את x ל־ R מימין. אם $\Gamma(v) \subset S \cup R$, השמט את v מ־ R והוסף אותו מימין ל־ S. כאשר $R=\emptyset$ סיים וסמן $S=(u=v_1,v_2,\dots,v_n)$.
אלגוריתם BFS מאפשר חישוב פונקציות שונות על G.
דוגמא: חישוב המרחק המינימלי $d(u,x)$ מקדקד קבוע u לקדקד כלשהוא $x \in V$:
נגדיר פונקציות: $d^*: V \to R\ \ ,\ \pi: V \to V \cup \{\emptyset\}$ ע"י
אתחול: $d^*(x) \equiv 0$, $\pi(x)=\emptyset$, לכל $x \in V$. $S=\emptyset$, $R \leftarrow (u=v_1)$.
איטרציה: יהא v הקודקוד השמאלי ב־ R ויהא $x \in \Gamma(v)-(S\cup R)$. נוסיף את x ל־ R מימין, נגדיר $d^*(x)=d^*(x)+1$, $\pi(x)=v$.

טענה: לכל $x \in V$ מתקיים $d^*(x)=d(u,x)$ וגם $x \to \pi(x) \to \pi^2(x) \to \dots$ הוא מסלול באורך מינימלי מ־ u ל־ x.

הטענה תנבע מהעובדות הבאות:

$$0=d^*(v_1) \le d^*(v_2) \le \dots \le d^*(v_n) \quad \text{(I)}$$

הוכחה: נראה כי $d^*(v_j) \le d^*(v_{j+1})$ באינדוקציה על j.
המקרה $j=1$ ברור. יהא $1 < j \le n-1$. נניח כי v_j התגלה כשכן של v_i וכי v_{j+1} התגלה כשכן של $v_{i'}$. אזי $i \le i'$, כי אם $i' < i$ אזי v_{j+1} היה מופיע לפני v_j.
לכן לפי הנחת האינדוקציה $d^*(v_i) \le d^*(v_{i'})$ ולכן

$$d^*(v_j)=d^*(v_i)+1 \le d^*(v_{i'})+1=d^*(v_{j+1}).$$

□

$$\forall 1 \le j \le n \quad d^*(v_j) \ge d(u,v_j) \quad \text{(II)}$$

הוכחה: אינדוקציה על j. המקרה $j=1$ ברור. יהא $1 < j \le n$ ונניח כי v_j התגלה כשכן של v_i. אזי

$$d(u,v_j) \le d(u,v_i)+1 \le d^*(v_i)+1=d^*(v_j)$$

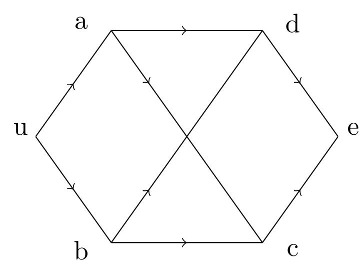
□

הוכחת הטענה: לפי (II) די להראות כי $d^*(v) \le d(u,v)$. נוכיח זאת באינדוקציה על $d(u,v)=\ell$. המקרה $\ell=0$ ברור. נניח עתה כי $\ell \ge 1$ ויהא $v=v_j$ כך ש־ $d(u,v_j)=\ell$. יהא P מסלול קצר ביותר מ־ u ל־ v_j ויהא v_k הקודקוד הקודם ל־ v_j במסלול. נניח כי v_j התגלה כשכן של v_i. אזי $i \le k$, אחרת v_j היה מתגלה כשכן של v_k. לכן $d^*(v_i) \le d^*(v_k)$ ולכן

$$d^*(v_j)=d^*(v_i)+1 \le d^*(v_k)+1=d(u,v_k)+1=d(u,v_j),$$

כאשר $d^*(v_k)+1=d(u,v_k)+1$ נובע מהנחת האינדוקציה. $\square$

דוגמא:

$G=$ 

בכל שלב באלגוריתם נסמן $(d^*(v),\pi(v))$ מתחת לקודקוד v שהתגלה.

S	R	u	a	b	c	d	e
$\emptyset$	u	$(0,\emptyset)$					
$\emptyset$	ua	$''$	$(1,u)$				
$\emptyset$	uab	$''$	$''$	$(1,u)$			
u	ab	$''$	$''$	$''$			
u	abc	$''$	$''$	$''$	$(2,a)$		
u	$abcd$	$''$	$''$	$''$	$''$	$(2,a)$	
ua	bcd	$''$	$''$	$''$	$''$	$''$	
uab	cd	$''$	$''$	$''$	$''$	$''$	
uab	cde	$''$	$''$	$''$	$''$	$''$	$(3,c)$
$uabcde$	$\emptyset$	$(0,\emptyset)$	$(1,u)$	$(1,u)$	$(2,a)$	$(2,a)$	$(3,c)$

סיבוכיות BFS

כל קודקוד בודק את כל שכניו ולכן הסיבוכיות היא

$$O(|V|)+O(\sum_{vinV} deg\ v)=O(|V|+|E|).$$

שימושים נוספים של BFS:

בדיקת דו־צדדיות.

אלגוריתם Dijkstra למרחק המינימלי בגרף ממושקל

יהא $G=(V,E)$ גרף מכוון עם פונקציית משקל $w:E\to\mathbb{R}^+$ על הצלעות. אם הצלע ux אינה בגרף מגדירים $w(u,x)=\infty$. הפונקציה w מגדירה מטריקה הנתונה ע"י:

$$d(u,v)=\min\{\sum_{e\in P}:\ \text{מסלול מכוון ב-}G\text{ מ-}u\text{ ל-}v\ P\}.$$

בהינתן $u\in V$ ברצוננו לחשב את $d(u,v)$ לכל $v\in V$. אלגוריתם Dijkstra הפותר בעייה זו מבוסס על הרעיון הבא: מגדירים סדרה עולה של קבוצות $\{u\}=S_1\subset\ldots\subset S_n=V$ וסדרת $d_1\geq\ldots\geq d_n$ של פונקציות על V כך שלכל $1\leq k\leq n$ ולכל $x\in S_k$ מתקיים $d_k(x)=d(u,x)$.

אלגוריתם Dijkstra

<u>אתחול:</u> ל־ $k=1$ נגדיר $S_1=\{v_1=u\}$, $d_1(x)=w(u,x)$ ו־

$$\pi_1(x)=\begin{cases} u & x\neq u\\ \emptyset & x=u\end{cases}$$

<u>איטרציה:</u> בהינתן $S_k=\{v_1,\ldots,v_k\}$, $d_k:V\to\mathbb{R}^+$, ו־ $\pi_k:V\to V\cup\{\emptyset\}$ $v_{k+1}\in$ $V-S_k$ כך ש:

$$d_k(v_{k+1})=\min\{d_k(x):x\in V-S_k\}$$

נגדיר $S_{k+1}=S_k\cup\{v_{k+1}\}$,

$$d_{k+1}(x)=\begin{cases} d_k(x) & x\in S_{k+1}\\ \min\{d_k(x),d_k(v_{k+1})+w(v_{k+1},x)\} & x\notin S_k\end{cases}$$

$$\pi_{k+1}(x)=\begin{cases} \pi_k(x) & x\in S_{k+1}\\ \pi_k(x) & d_k(x)\leq d_k(v_{k+1})+w(v_{k+1},x), \quad x\notin S_{k+1}\\ v_{k+1}(x) & d_k(x)> d_k(v_{k+1})+w(v_{k+1},x), \quad x\notin S_{k+1}\end{cases}$$

נסמן ב־ $P_k(x)$ את אוסף המסלולים המכוונים מ־ u ל־ x שכל קודקודיהם למעט האחרון ־ דהיינו x ־ נמצאים ב־ S_k. עבור מסלול כלשהו P בגרף נסמן $w(P)=\sum_{e\in P}w(e)$.

<u>משפט Dijkstra</u>

לכל $1\leq k\leq n$ מתקיים

(i) לכל $x\in S_k$: $d_k(x)=d(u,x)$

(ii) לכל $x\in V$: $d_k(x)=\min\{w(P):P\in P_k(x)\}$

<u>הוכחה:</u> אינדוקציה על k. המקרה $k=1$ ברור. נניח ל־ $1\leq k<n$ ונוכיח ל־ $k+1$.

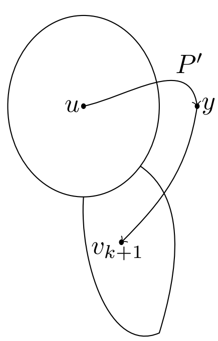
(i) יהא $x\in S_{k+1}$. אם $x\in S_k$ אזי

$$d_{k+1}(x)=d_k(x)=d(u,x)$$

אם $x=v_{k+1}$ אזי

$$d_{k+1}(v_{k+1})=d_k(v_{k+1})=\min\{w(P):P\in P_k(x)\}\geq d(u,v_{k+1})$$

מאידך, יהא P מסלול מכוון מ־ u ל־ v_{k+1} כך ש־ $d(u,v_{k+1})=w(P)$. יהא y הקודקוד הראשון ב־ P שאינו ב־ S_k (ייתכן כי $y=v_{k+1}$).



יהא P' קטע המסלול מ־ u ל־ y. אזי

$$d(u,v_{k+1})=w(P)\geq w(P')\geq\min\{w(Q):Q\in P_k(y)\}$$

$$=d_k(y)\geq d_k(v_{k+1})$$

לכן $d(u,v_{k+1})=d_k(v_{k+1})=d_{k+1}(v_{k+1})$.

(ii) יהא $x \in V$. אם $x \in S_{k+1}$ אזי

$$d_{k+1}(x) \overset{(i)}{=} d(u,x) \le \min\{w(P) : P \in P_{k+1}(x)\}$$

$$\le \min\{w(P) : P \in P_k(x)\} \overset{\text{(I)}}{=} d_k(x) \overset{\text{(II)}}{=} d_{k+1}(x).$$

כאשר שיויון (I) נובע מהנחת האנדוקציה ו־ (II) נובע מהגדרת $d_{k+1}(x)$.

לכן $d_{k+1}(x) = \min\{w(P) : P \in P_{k+1}(x)\}$.

נניח $x \in V - S_{k+1}$.

$$d_k(x) = \min\{w(P) : P \in P_k(x)\} \ge \min\{w(P) : P \in P_{k+1}(x)\}$$

$$d_k(v_{k+1}) + w(v_{k+1}, x) = \min\{w(P) : P \in P_k(v_{k+1})\} + w(v_{k+1}, x)$$

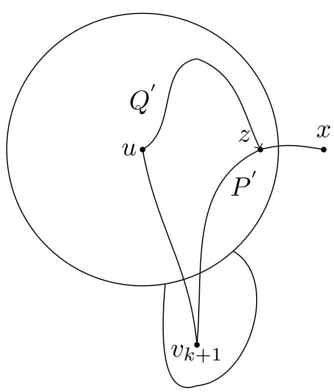
$$\ge \min\{w(P) : P \in P_{k+1}(x)\}$$

ולכן $d_{k+1}(x) \ge \min\{w(P) : P \in P_{k+1}(x)\}$.

כיוון שני: יהא $P \in P_{k+1}(x)$ ויהא z הקודקוד האחרון ב־ P לפני x. אם $z \in S_k$ אזי

$$d(u,z) = d_k(z) = \min\{w(Q^{'} : Q^{'} \in P_k(z)\}$$

ולכן קיים $Q^{'} \in P_k(z)$ כך ש־ $d(u,z) = w(Q^{'})$.



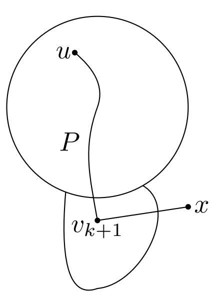
יהא $P^{'} = P - \{zx\}$. אזי

$$w(P^{'}) \ge w(Q^{'})$$

ולכן

$$w(P) = w(P^{'}) + w(zx) \ge w(Q^{'}) + w(zx)$$

$$\ge d_k(x)$$



אם $z = v_{k+1}$ אזי $P^{'} = P - \{v_{k+1}x\} \in P_k(v_{k+1})$ ולכן

$$w(P^{'}) \ge \min\{w(Q^{'}) : Q^{'} \in P_k(v_{k+1})\}$$

$$\overset{\text{הנחת האינדוקציה}}{=} d_k(v_{k+1})$$

ולכן

$$w(P) = w(P^{'}) + w(v_{k+1}, x) \ge d_k(v_{k+1}) + w(v_{k+1}, x)$$

לכן בכל מקרה

$$w(P) \geq \min\{d_k(x), d_k(v_{k+1}) + w(v_{k+1}, x)\} = d_{k+1}(x)$$

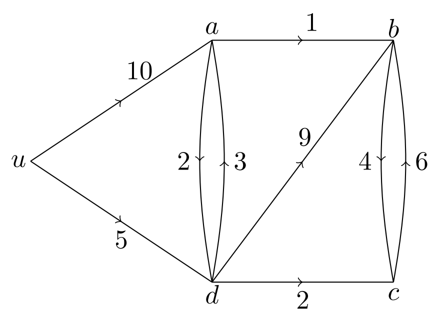
$\square$

<u>מסקנה</u>: לכל $x \in V$

$$d_n(x) = d(u,x)$$

ו־ $x \to \pi_n(x) \to \pi_n^2(x) \to \ldots$ הוא מסלול מינימלי מ־ u ל־ x.

<u>סיבוכיות אלגוריתם Dijkstra</u>
בכל איטרציה של האלגוריתם מעדכנים את d_k ו־ π_k ע"י $O(|V|)$ פעולות, ולכן סה"כ הסיבוכיות היא $O(|V|^2)$.
<u>דוגמא:</u>



d_k

u	a	b	c	d
$\underline{0}$	10	∞	∞	5
$\underline{0}$	8	14	7	$\underline{5}$
$\underline{0}$	8	13	$\underline{7}$	$\underline{5}$
$\underline{0}$	$\underline{8}$	9	$\underline{7}$	$\underline{5}$
$\underline{0}$	$\underline{8}$	$\underline{9}$	$\underline{7}$	$\underline{5}$

π_k

u	a	b	c	d
$\underline{\emptyset}$	u	u	u	u
$\underline{\emptyset}$	d	d	d	$\underline{u}$
$\underline{\emptyset}$	d	c	$\underline{d}$	$\underline{u}$
$\underline{\emptyset}$	$\underline{d}$	a	$\underline{d}$	$\underline{u}$
$\underline{\emptyset}$	$\underline{d}$	$\underline{a}$	$\underline{d}$	$\underline{u}$

למשל, המסלול המינימלי מ־ u ל־ b הוא

$$u = \pi_5(d) \to d = \pi_5(a) \to a = \pi_5(b) \to b$$

<u>אלגוריתם Floyd-Warshall</u>
<u>נתון:</u> גרף מכוון ממושקל על $[n]$. משקל הצלע (i,j) הוא $w(i,j) \in \mathbb{R}$. אם $(i,j) \notin E$ מגדירים $w(i,j) = \infty$. כמו כן $w(i,i) = 0$ לכל i.
<u>מטרה:</u> לחשב את $d(i,j) = \inf\{w(P) : P$ מסלול מכוון מ־i ל־$j\}$
<u>הערות:</u>

- אם לא קיים מסלול מכוון מ־ i ל־ j אזי $d(i,j) = \infty$.

- אם קיים מסלול מכוון מ־ i ל־ j המכיל מעגל שלילי אזי $d(i,j)=-\infty$.

<u>אלגוריתם FW:</u> נגדיר לכל $0 \le k \le n$ מטריצה $(D_k(i,j))_{i,j=1}^n$ באופן הבא.
<u>אתחול:</u> $D_0(i,j)=w(i,j)$.
<u>איטרציה:</u> לכל $1 \le k \le n$ נגדיר

$$D_k(i,j)=\min\{D_{k-1}(i,j), D_{k-1}(i,k)+D_{k-1}(k,j)\}.$$

<u>ניתוח האלגוריתם:</u> נסמן

$$P_k(i,j)=\{P : P-\{i,j\}\subset\{1,\ldots,k\} \text{ מסלול מכוון מ־} i \text{ ל־} j \text{ כך ש־ } P\}$$

$$\widetilde{P}_k(i,j)=\{P\in P_k(i,j) : \text{ לא מכיל מעגלים מכוונים } P\}$$

$$\alpha_k(i,j)=\min\{w(P) : P\in P_k(i,j)\}$$

$$\widetilde{\alpha}_k(i,j)=\min\{w(P) : P\in \widetilde{P}_k(i,j)\}$$

<u>טענה:</u> לכל $1 \le k \le n$

$$(i) \quad \alpha_k(i,j)\le\min\{\alpha_{k-1}(i,j), \alpha_{k-1}(i,k)+\alpha_{k-1}(k,j)\}$$
$$(ii) \quad \widetilde{\alpha}_k(i,j)\ge\min\{\widetilde{\alpha}_{k-1}(i,j), \widetilde{\alpha}_{k-1}(i,k)+\widetilde{\alpha}_{k-1}(k,j)\}$$

<u>הוכחה:</u> (i) יהא $P^{'}\in P_{k-1}(i,j)$ כך ש־ $\alpha_{k-1}(i,j)=w(P^{'})$ ויהיו

$$P^{''}\in P_{k-1}(i,k) \quad P^{'''}\in P_{k-1}(k,j)$$

כך ש־

$$w(P^{''})=\alpha_{k-1}(i,k) \quad w(P^{'''})=\alpha_{k-1}(k,j).$$

אזי $P^{'}, P=P^{''}\cup P^{'''}\in P_k(i,j)$ ולכן

$$\alpha_k(i,j)\le\min\{w(P^{'}),w(P)\}=\min\{\alpha_{k-1}(i,j),\alpha_{k-1}(i,k)+\alpha_{k-1}(k,j)\}.$$

(ii) יהא $P\in\widetilde{P}_k(i,j)$ כך ש־ $w(P)=\widetilde{\alpha}_k(i,j)$. אם $P\in\widetilde{P}_{k-1}(i,j)$ אזי

$$w(P)\ge\widetilde{\alpha}_{k-1}(i,j)$$

אחרת נסמן $P=P^{'}\cup P^{''}$ כאשר $P^{'}\in\widetilde{P}_{k-1}(i,k)$, $P^{''}\in\widetilde{P}_{k-1}(k,j)$. ואזי

$$\widetilde{\alpha}_k(i,j)=w(P)=w(P^{'})+w(P^{''})\ge\widetilde{\alpha}_{k-1}(i,k)+\widetilde{\alpha}_{k-1}(k,j).$$

לכן

$$\widetilde{\alpha}_k(i,j)\ge\min\left\{\widetilde{\alpha}_{k-1}(i,j),\ \widetilde{\alpha}_{k-1}(i,k)+\widetilde{\alpha}_{k-1}(k,j)\right\}$$

$\square$

<u>מסקנה:</u> לכל $0 \le k \le n$ מתקיים

$$\alpha_k(i,j) \le D_k(i,j) \le \widetilde{\alpha}_k(i,j).$$

<u>מסקנה:</u>

(i) אם אין מסלול מ־ i ל־ j הכולל מעגל שלילי אזי $D_k(i,j) = \alpha_k(i,j) = \widetilde{\alpha}_k(i,j)$ לכל $1 \le k \le n$ ובפרט

$$d(i,j) = D_n(i,j)$$

(ii) יש מסלול מ־ i ל־ j הכולל מעגל שלילי $\Leftrightarrow$ קיים $1 \le k \le n$ כך ש־ $D_n(k,k) < 0$ וכך ש־

$$D_n(i,k) + D_n(k,j) < \infty.$$

<u>הוכחה:</u>

(i) אם אין מסלול הכולל מעגל שלילי מ־ i ל־ j אזי המסלול המינימלי מ־ i ל־ j הוא פשוט ולכן $\alpha_n(i,j) = \widetilde{\alpha}_n(i,j)$ ולכן $D_n(i,j)$ שווה לשניהם.

(ii) נניח שיש מסלול P מ־ i ל־ j הכולל מעגל שלילי. אזי P מכיל מעגל שלילי פשוט C. יהא k קודקוד ב־ C. אזי $D_n(k,k) \le \widetilde{\alpha}_n(k,k) < 0$. כמו כן ברור שיש מסלולים פשוטים מ־ i ל־ k ומ־ k ל־ j ולכן $D_n(k,j), D_n(i,k) < \infty$.

להיפך נניח כי $D_n(k,k) < 0$ ו־ $D_n(i,k) + D_n(k,j) < \infty$. אזי יש מסלולים מכוונים $P^{'} \in P_n(i,k)$, $P^{''} \in P_n(k,k)$ עבורן $w(P^{''}) < 0$, ו־ $P^{'''} \in P_n(k,j)$. לכן $P = P^{'} \cup P^{''} \cup P^{'''}$ הוא המסלול הדרוש. $\square$

<u>סיבוכיות:</u> $O(|V|^3)$ כי בכל אחד מ־ n השלבים מעדכנים מטריצה $n \times n$.

<u>חישוב המסלול הקצר ביותר</u>

נגדיר

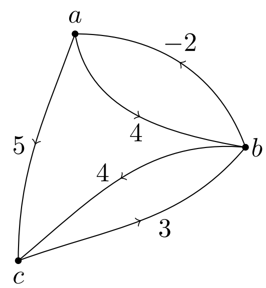
$$\pi_0(i,j) = \begin{cases} \emptyset & i = j \text{ או } w(i,j) = \infty \\ i & \text{אחרת} \end{cases}$$

$$\pi_k(i,j) = \begin{cases} \pi_{k-1}(i,j) & D_k(i,j) = D_{k-1}(i,j) \\ \pi_{k-1}(k,j) & D_k(i,j) = D_{k-1}(i,k) + D_{k-1}(k,j) \end{cases}$$

המסלול הקצר ביותר מ־ i ל־ j נתון ע"י

$$i \to \cdots \to \pi_n(i, \pi_n(i,j)) \to \pi_n(i,j) \to j$$

<u>דוגמא:</u>



$$D_0 = \begin{array}{c|ccc|} & a & b & c \\ \hline a & 0 & 4 & 5 \\ b & -2 & 0 & 4 \\ c & \infty & 3 & 0 \\ \hline \end{array} \qquad \pi_0 = \begin{array}{c|ccc|} & a & b & c \\ \hline a & \emptyset & a & a \\ b & b & \emptyset & b \\ c & \emptyset & c & \emptyset \\ \hline \end{array}$$

$$D_1 = \begin{array}{|ccc|} \hline 0 & 4 & 5 \\ -2 & 0 & 3 \\ \infty & 3 & 0 \\ \hline \end{array} \qquad \pi_1 = \begin{array}{|ccc|} \hline \emptyset & a & a \\ b & \emptyset & a \\ \emptyset & c & \emptyset \\ \hline \end{array}$$

$$D_2 = \begin{array}{|ccc|} \hline 0 & 4 & 5 \\ -2 & 0 & 3 \\ 1 & 3 & 0 \\ \hline \end{array} \qquad \pi_2 = \begin{array}{|ccc|} \hline \emptyset & a & a \\ b & \emptyset & a \\ b & c & \emptyset \\ \hline \end{array}$$

$$D_3 = D_2 \qquad \pi_3 = \pi_2$$

מסלול מינימלי מ־ b ל־ c:

$$b = \pi_3(b,a) \to a = \pi_3(b,c) \to c.$$

חפוש עומק DFS (Depth First Search)

קלט: $G=(V,E)$ גרף מכוון.
פלט: יער מכוון פורש T של G.
משתני האלגוריתם: t- זמן בדיד $t=1,2,\ldots$
$color(v)\in\{W,B,G\}=$ צבע הקדקד v בזמן נתון, כאשר:

$$color(v)=\begin{cases} W & \text{טרם התגלה } v \\ G & \text{בטיפול } v \\ B & \text{הסתיים הטיפול ב} - v \end{cases}$$

$d(v)=$ זמן הגלוי של v.
$f(v)=$ זמן הסגירה של v.
$\pi(v)=$ אב של v ביער ה-DFS T של G.
נסמן $\Gamma^+(u)=\{v\ :\ uv\in E\}$.

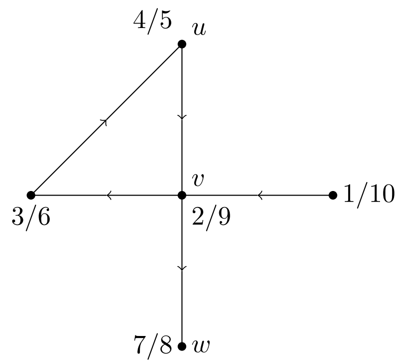
DFS(G)
$t=0$
$\forall u\in V\ \ \pi(u)=\emptyset\ ,\ color(u)=W$
$\forall u\in V$ such that $color(u)=W$ do DFS-visit(u).

DFS-visit(u)
$color(u)\leftarrow G$
$t\leftarrow t+1$
$d(u)\leftarrow t$
$\forall v\in\Gamma^+(u)$: If $color(v)=W$ then ($\pi(v)\leftarrow u$, DFS-visit(v))
$color(u)\leftarrow B$
$t\leftarrow t+1$
$f(u)\leftarrow t$

נסמן $u\rightarrow v$ אם $(u,v)\in E$ ו- $u\rightsquigarrow v$ אם יש מסלול מכוון ב-G מ-u ל-v. נסמן $\overset{T}{\rightsquigarrow}$ אם יש מסלול מכוון מ-u ל-v ביער ה-DFS T.
מתיאור האלגוריתם נובע שהאנטרוולים $[d(u),f(u)]$ מקיימים
תכונת הסוגריים: אם $u\neq v$ אזי האנטרוולים $[d(u),f(u)]$ $[d(v),f(v)]$ הינם זרים או שאחד מוכל באחר.

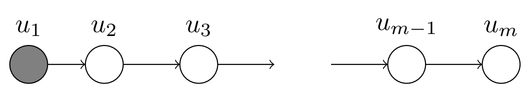
$$d(u)<d(v)<f(v)<f(u)\Leftrightarrow u\overset{T}{\rightsquigarrow}v$$

טענה: אם $u\rightarrow v$ אזי $d(v)<f(u)$.
הוכחה: אם v טרם התגלה הרי שאי אפשר לסגור את u.
הערה: $u\rightarrow v\rightarrow w\ \not\Leftarrow\ d(w)<f(u)$. למשל,



<u>למת המסלול הלבן:</u> אם $u_1 \to u_2 \to \cdots u_m$ ו־$d(u_1) < d(u_2), \ldots, d(u_m)$
אזי $u_1 \overset{T}{\rightsquigarrow} u_m$.

צלום הצבעים בזמן $d(u_1)$:



<u>הוכחה:</u> אנדוקציה על m. אם $m = 2$ אזי

$$d(u_1) \underset{\text{הנחה}}{<} d(u_2) \underset{\text{טענה}}{<} f(u_1)$$

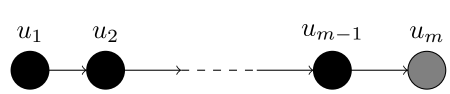
ולכן לפי תכונת הסוגריים $d(u_1) < d(u_2) < f(u_2) < f(u_1)$ ו־$u_1 \overset{T}{\rightsquigarrow} u_2$.
יהא עתה $m > 2$. אזי

$$d(u_1) \underset{\text{הנחה}}{<} d(u_m) \underset{\text{טענה}}{<} f(u_{m-1}) \underset{\text{הנחת האנדוקציה}}{<} f(u_1)$$

לכן לפי תכונת הסוגריים $d(u_1) < d(u_m) < f(u_m) < f(u_1)$ ולכן $u_1 \overset{T}{\rightsquigarrow} u_m$.

<u>למת המסלול השחור:</u> אם $u_1 \to u_2 \to \cdots \to u_m$
ו־$f(u_1), \ldots, f(u_{m-1}) < f(u_m)$ אזי $u_m \overset{T}{\rightsquigarrow} u_1$.

צלום הצבעים בזמן $f(u_m) - 1$:



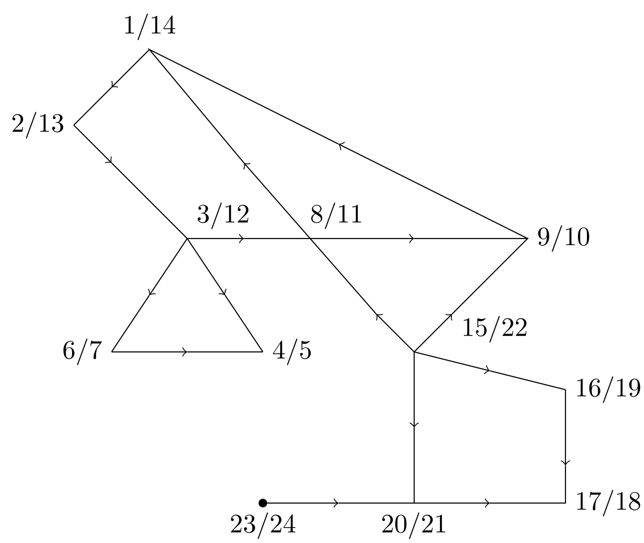
<u>הוכחה</u>: אם $d(u_m) < d(u_1)$ אזי לפי תכונת הסוגריים
$d(u_m) < d(u_1) < f(u_1) < f(u_m)$ ואזי $u_m \overset{T}{\rightsquigarrow} u_1$.
נניח בשלילה כי $d(u_1) < d(u_m)$ ויהא
$m-1 \geq i = \max\{j \ : \ d(u_j) \leq d(u_1)\}$ אזי

$$d(u_i) \leq d(u_1) < d(u_{i+1}), \ldots, d(u_m)$$

ולכן, לפי למת המסלול הלבן $u_m \overset{T}{\rightsquigarrow} u_i$ ולכן $f(u_m) < f(u_i)$, סתירה להנחה.

$\square$

<u>דוגמא להרצת DFS</u>



<u>מיון טופולוגי</u>
יהא $G = (V, E)$ גרף מכוון. <u>מיון טופולוגי</u> של G הוא העתקה חח"ע $\varphi : V \to \mathbb{N}$ כך ש־
$u \to v \Leftarrow \varphi(u) < \varphi(v)$

<u>טענה</u>: קיים מיון טופולוגי ל־G אם"ם G חסר מעגלים מכוונים.

<u>הוכחה</u>: אם $u_1 \to \cdots \to u_m \to u_1$ מעגל ב־G ו־$\varphi : V \to \mathbb{N}$ מיון טופולוגי אזי $\varphi(u_1) < \cdots < \varphi(u_m) < \varphi(u_1)$ סתירה.
להיפך, אם G חסר מעגלים מכוונים אזי יש קדקד u כך ש־
$\{v \ : \ (v,u) \in E\} = \Gamma^+(u) = \emptyset$.
יהא G הגרף המתקבל מ־G ע"י השמטת u.
לפי הנחת האנדוקציה יש $\varphi' : V' = V \setminus \{u\} \to \mathbb{N}$ כך ש φ' מיון טופולוגי של G'.
נגדיר

$$\varphi(v) = \begin{cases} 1 & v = u \\ \varphi'(v) + 1 & v \in V' \end{cases}$$

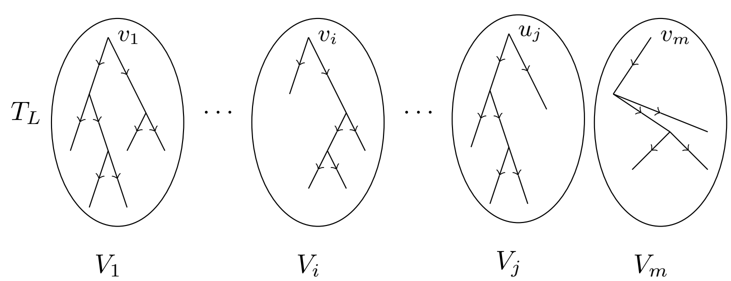
אזי φ מיון טופולוגי של G.
<u>טענה</u>: אם G אציקלי אזי $\varphi(u) = -f(u)$ מיון טופולוגי של G.

<u>הוכחה</u>: נניח $u \to v$. אם $f(u) < f(v)$ אזי $d(v) < f(u) < f(v)$ לפי הטענה ולכן $u \overset{T}{\rightsquigarrow} v$ ולכן G מכיל מעגל מכוון, בסתירה להנחה.
לכן $f(u) > f(v)$ ולכן $\varphi(u) < \varphi(v)$. □

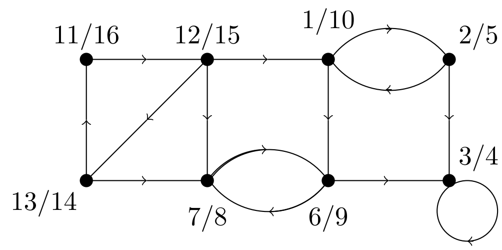
<u>קשירות חזקה</u>
יהא $G = (V, E)$ גרף מכוון. נגדיר $u \sim v$ אם $u \rightsquigarrow v$ ו־$v \rightsquigarrow u$.
$\sim$ הוא יחס שקילות. מחלקות השקילות של יחס זה נקראות רכיבי קשירות חזקה.

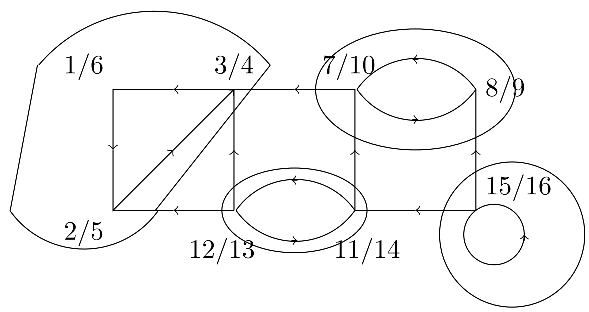
<u>טענה</u>: נפעיל DFS על G ונקבל את סדרת זמני הסגירה של הקדקדים $(f(u))_{u \in V}$.
יהא G^t הגרף המתקבל מ־G ע"י הפוך כוון הצלעות.
נפעיל DFS על G^t כאשר הקדקדים הנבחרים ב־$\mathrm{DFS}(G^t)$ נלקחים לפי סדר יורד של $(f(u))_{u \in V}$.
אזי רכיבי היער G^t מתלכדים עם רכיבי הקשירות החזקה של G.
<u>הוכחה</u>: יהיו $(d(u), f(u))$ זמני הפתיחה והסגירה של הקדקד $u \in V$ בהרצה הראשונה של ה־DFS, ויהא T_1 יער ב־DFS המתקבל.
יהא T_2 יער ה־DFS המתקבל לאחר הרצת DFS על G^t בסדר יורד של $f(u)$. יהיו $V_1, \ldots, V_m$ רכיבי הקשירות של T_2 עם שורשים $v_1, \ldots, v_m$ לפי סדר קבלתם.
עלינו להראות כי $V_1, \ldots, V_m$ הם רכיבי הקשירות החזקה של G. ראשית נראה כי V_i קשיר חזק. די להראות כי לכל $v \in V_i$ יש מסלולים מכוונים מ־v ל־v_i ומ־v_i ל־v ב־G.
עתה, $v \in V_i$ גורר כי $v_i \overset{T_2}{\rightsquigarrow} v$ ב־G^t ולכן $v \rightsquigarrow v_i$ ב־G.
נעיין במסלול הנ"ל $v_i \rightsquigarrow v$. לפי בחירת סדר הקדקדים ב־DFS השני, $f(v_i) > f(u)$ לכל $u \in V_i$ ובפרט לכל הקדקדים $u \neq v_i$ הנמצאים במסלול $v_i \rightsquigarrow v$. לכן מלמת המסלול השחור נובע כי $v_i \overset{T_1}{\rightsquigarrow} v$ ובפרט $v_i \rightsquigarrow v$ ב־G. לכן V_i קשיר חזק.

עתה נשים לב כי אם $i < j$ אזי אין צלע ב־G^t מ־v_i ל־v_j, ולכן ב־G אין צלע מ־V_j ל־V_i.
מכאן נובע כי ה־V_i־ים הם רכיבי הקשירות החזקה של G.



דוגמא:





זרימה ברשתות

רשת זרימה היא גרף מכוון $G=(V,E)$ עם זוג קדקדים מיוחדים שונים:
s הנקרא מקור (source) ו־t הנקרא בור (sink), ופונקציה אי שלילית $c: E \to \mathbb{R}^+$.
$c(e)$ נקרא הקבול (capacity) של הצלע e.
לקדקד $u \in V$ נסמן $T^-(u)=\{w \ : \ wu \in E\}$, $T^+(u)=\{v \ : \ uv \in E\}$. לפונקציה $f: E \to \mathbb{R}$ ולקדקד $u \in V$ נסמן

$$f^+(u)=\sum_{v\in T^+(u)} f(uv)\ ,\ f^-(u)=\sum_{w\in T^-(u)} f(wu)$$

$f: E \to \mathbb{R}^+$ תקרא זרימה (flow) ברשת אם $0 \le f(e) \le c(e)$ לכל $e \in E$, ולכל $u \in V \setminus \{s,t\}$ $\quad f^+(u)=f^-(u)$.
ערך הזרימה f מוגדר ע"י $val(f)=f^+(s)-f^-(s)$.

דוגמא: G מתאר מערכת כבישים חד־סטריים מ־s ל־t.
קבול כל צלע, דהיינו קטע כביש, הינו מספר הרכבים לשעה שקטע זה יכול לשאת (זו פונקציה של רוחב קטע הכביש, איכותו וכול'). המטרה היא למצוא את מקסימום המכוניות לשעה שאפשר להעביר מ־ s ל־ t.
לקבוצת קדקדים לאו דווקא זרות $A, B \subset V$ נגדיר

$$f(A,B)=\sum_{(a,b)\in A\times B\cap E} f(ab)$$

לקבוצת קדקדים $S \subset V$ נסמן $\bar{S} = V \setminus S$. חתך $s-t$ היא חלוקה $(S,\bar{S})$ כך ש $s \in S$, $t \in \bar{S}$.

<u>טענה</u>: לכל זרימה f ולכל חתך $s-t$ $(S,\bar{S})$ מתקיים

$$val(f) = f(S,\bar{S}) - f(\bar{S},S)$$

<u>הוכחה</u>:

$$val(f) = f^+(s) - f^-(s) = \sum_{u \in S} \big(f^+(u) - f^-(u)\big) = f(S,V) - f(V,S) =$$

$$= \big[f(S,S) + f(S,\bar{S})\big] - \big[f(S,S) + f(\bar{S},S)\big] = f(S,\bar{S}) - f(\bar{S},S)$$

$\square$

לחתך $s-t$ $(S,\bar{S})$ נגדיר את קבול החתך ע"י

$$cap(S,\bar{S}) = \sum_{uv \in S \times \bar{S} \cap E} c(uv)$$

<u>דואליות חלשה</u>: לכל זרימת f וחתך $s-t$ $(S,\bar{S})$ מתקיים

$$val(f) \le cap(S,\bar{S})$$

<u>הוכחה</u>:

$$val(f) = f(S,\bar{S}) - f(\bar{S},S) \le f(S,\bar{S}) =$$

$$= \sum_{uv \in S \times \bar{S} \cap E} f(uv) \le \sum_{uv \in S \times \bar{S} \cap E} c(uv) = cap(S,\bar{S})$$

יהיו $u,v \in V$.
אוסף סדור של צלעות $(e_1,\ldots,e_m)$ יקרא מסלול $u-v$ (לא מכוון) אם קיימת סדרת קדקדים שונים $u = v_0, v_1, \ldots, v_m = v$ כך שלכל $1 \le i \le m$
או $e_i = v_{i-1}v_i$ או $e_i = v_i v_{i-1}$.
אם $e_i = v_{i-1}v_i$ נאמר ש־ e_i בכוון המסלול,
ואם $e_i = v_i v_{i-1}$ נאמר ש־ e_i נגד כוון המסלול.
בהנתן מסלול P וזרימה f נגדיר את <u>העודף של f על צלע $e_i \in P$</u> ע"י

$$\varepsilon_{f,P}(e_i) = \begin{cases} c(e_i) - f(e_i) & e_i = v_{i-1}v_i \\ f(e_i) & e_i = v_i v_{i-1} \end{cases}$$

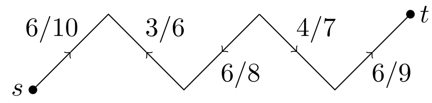
<u>העודף של f על P</u> יוגדר כ־ $\underline{\varepsilon}_{f,P} = \min_{1 \le i \le m} \varepsilon_{f,P}(e_i)$

<u>טענה</u>: אם P מסלול $s-t$ (כלומר $v_m = t$, $v_0 = s$) אזי קיימת זרימה $\tilde{f}$ המקיימת $val(\tilde{f}) = val(f) + \underline{\varepsilon}_{f,P}$.

<u>הוכחה</u>: נגדיר

$$\tilde{f}(e) = \begin{cases} f(e) & e \notin P \\ f(e) + \varepsilon_{f,P} & e = v_{i-1}v_i \\ f(e) - \varepsilon_{f,P} & e = v_i v_{i-1} \end{cases}$$

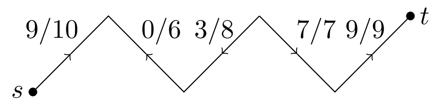
מתקיים כי $0 \le \tilde{f}(e) \le c(e)$.
כמוכן $\tilde{f}^{+}(u) = \tilde{f}^{-}(u)$ לכל $u \neq s,t$.
<u>דוגמא</u>: זרימה נוכחית:



$$\varepsilon_{f,P}(e) \quad 4 \quad 3 \quad 6 \quad 3 \quad 3$$

$$\varepsilon_{f,P} = \min_{e \in P} \varepsilon_{f,P}(e) = 3$$

זרימה מעודכנת:



התוצאנ הבסיסית בנושא זרימות ברשתות היא האפיון הבא של הזרימה המקסימלית שהוכח ע"י Ford-Fulkenson.

<u>משפט הזרימה המקסימלית והחתך המינימלי Max Flow Min Cut (MFMC)</u>

$$\max\left\{val(f) \;:\; \text{זרימה ברשת } f\right\} = \min\left\{cap(S,\bar{S}) \;:\; \text{חתך } (s,t) \; (S,\bar{S})\right\}$$

<u>הוכחה</u>: הראינו כי $\max_{f} val(f) \le \min_{(S,\bar{S})} cap(S,\bar{S})$
לכן, כדי להשלים את ההוכחה יש להראות שקיימת זרימה f וקיים חתך $s-t$ $(S,\bar{S})$ כך ש־ $val(f) = Cap(S,\bar{S})$. תהא f זרימה ברשת עם ערך $val(f)$ מקסימלי. נסמן

$$S = \left\{ u \in V \;:\; \begin{array}{r} \text{קיים מסלול } s-u \; P \\ \text{כך ש־ } \varepsilon_{f,P} > 0 \end{array} \right\}$$

מהטענה נובע כי $s \in S$, $t \notin \bar{S}$, אחרת אפשר היה לקבל זרימה $\tilde{f}$ עם ערך גדול יותר.

<u>טענה</u>:

(i) אם $uv \in S \times \bar{S} \cap E$ אזי $f(uv) = c(uv)$

(ii) אם $vu \in \bar{S} \times S \cap E$ אזי $f(vu) = 0$

<u>הוכחה:</u>

(i) יהא P מסלול $s-u$ כך ש־ $\underline{\varepsilon}_{f,P} > 0$
נגדיר $P' = P \cup \{uv\}$ אזי P' מסלול $s-v$ ומתקיים

$$\underline{\varepsilon}_{f,P'} = \min\{\underline{\varepsilon}_{f,P}\ ,\ c(uv) - f(uv)\}$$

מאידך $\underline{\varepsilon}_{f,P'} = 0$ כי $v \notin S$ ולכן $c(uv) = f(uv)$.

(ii) יהא P מסלול $s-u$ כך ש־ $\underline{\varepsilon}_{f,P} > 0$. נגדיר $P'' = P \cup \{vu\}$ אזי P'' מסלול $s-v$ ומתקיים

$$\underline{\varepsilon}_{f,P''} = \min\{\underline{\varepsilon}_{f,P}\ ,\ f(vu)\}$$

מאידך $\underline{\varepsilon}_{f,P''} = 0$ כי $v \notin S$ ולכן $f(vu) = 0$

$\square$

מהטענה נובע כי

$$val(f) = f(S,\bar{S}) - f(\bar{S},S) = \sum_{uv \in S \times \bar{S} \cap E} f(uv) - \sum_{vu \in \bar{S} \times S \cap E} f(vu) =$$

$$= \sum_{uv \in S \times \bar{S} \cap E} c(uv) = cap(S,\bar{S})$$

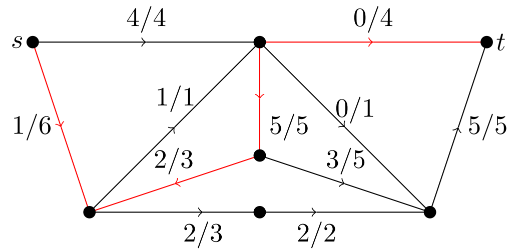
$\square$

הוכחת משפט MCMF מראה גם את התוצאה הבאה:
<u>משפט:</u> אם כל הקבולים ברשת טבעיים אזי יש זרימה מקסימלית שלמה f, כלומר $f(e) \in \mathbb{N}$ לכל $e \in E$.

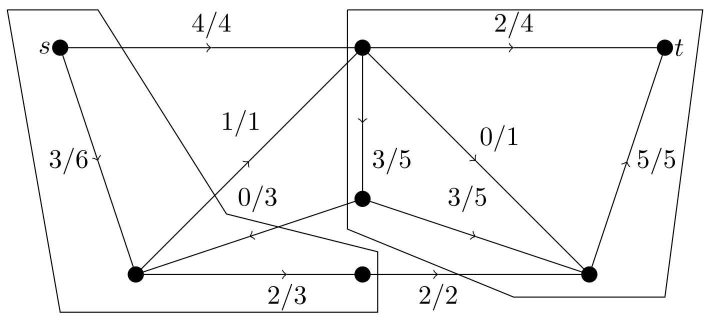
<u>הוכחה:</u> תהא f זרימה מקסימלית בין כל הזרימות השלמות.
אם P מסלול $s-t$, אזי $\underline{\varepsilon}_{f,P} \in \mathbb{N}$ ולכן בגלל המקסימליות של $val(f)$ נובע כי $\underline{\varepsilon}_{f,P} = 0$ ולפיכך החתך $(S,\bar{S})$ שהוגדר בהוכחת משפט MCMF מקיים $val(f) = Cap(S.\bar{S})$ ולכן f זרימה מקסימלית ברשת. $\square$

<u>אלגוריתם למציאת זרימה מקסימלית ברשת</u>

נגדיר $f_1 = 0$. נניח שהגדרנו זרימות $f_1, \ldots, f_k$. אם קיים מסלול $s-t$ P המקיים $\underline{\varepsilon}_{f_k,P} > 0$ אזי נגדיל את f_k לאורך המסלול P לזרימה $f_{k+1} = \tilde{f}_k$ כמתואר בטענה.
אם אין P כנ"ל אזי f_k זרימה מקסימלית.
<u>דוגמא:</u>



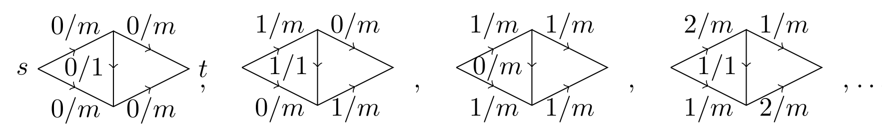
$$\underline{\varepsilon}_{f,P} = \min\{5, 2, 5, 4\} = 2$$



הערות:

1. האלגוריתם הנ"ל מתכנס לזרימה מקסימלית (שלמה) אם כל הקבולים שלמים מאחר וכל צעד באלגוריתם מגדיל את הזרימה בלפחות אחד.

   שיקול דומה מראה שהאלגוריתם מתכנס לזרימה מקסימלית אם כל הקבולים רציונליים. אך גם במקרים אלה, מספר האטרציות יכול להיות מעריכי בגודל הקלט, למשל, סדרת ההרחבות



   מגיעה לזרימה מקסימלית אחרי $2m$ צעדים.

   מאידך גודל הקלט בביטים הוא $O(\log m)$.

2. אם הקבולים אינם רציונלים, האלגוריתם הנ"ל אינו בהכרח מתכנס.

אלגוריתם יעיל לבעיית הזרימה

תהא $G=(V,E)$ רשת זרימה עם פונקציות קבול $c: E \to R^+$,
ותהא f זרימה על G. לכל צלע $e=uv \in E$ נתאים שתי צלעות חדשות $\overleftarrow{e}=vu$ (גם אם הצלע vu הופיעה אף היא ב־G).
נגדיר גרף מכוון $G_f=(V,E_f)$ כאשר

$$E_f=\{\vec{e} \in E \ : \ f(e)<c(e)\} \cup \{\overleftarrow{e} \ : \ e \in E \ , \ f(e)>0\}$$

מסלול $s-t$ P יקרא f־לא רווי אם $\varepsilon_{f,P}>0$.

טענה: קיים מסלול $s-t$ f־לא רווי $\Leftrightarrow$ קיים ב־G_f מסלול מכוון מ־s ל־t.
הוכחה: יהא $s=v_0,v_1,\ldots,v_m=t$ מסלול f־לא רווי עם צלעות $e_1,\ldots,e_m$ כאשר $e_i=v_{i-1}v_i$ או $e_i=v_iv_{i-1}$.
נגדיר עתה צלעות $g_1,\ldots g_m \in E(G_f)$ ע"י

$$g_i=\begin{cases} \vec{e}_i & e_i=v_{i-1}v_i \\ \overleftarrow{e_i} & e_i=v_iv_{i-1} \end{cases}$$

ברור כי הצלעות $g_1,\ldots,g_m$ הן מסלול מכוון מ־s ל־t ב־G_f.
כוון שני דומה.

אלגוריתם Edmonds-Karp :

אתחול: $f_1=0$

אטרציה: בהנתן f_k בנה את הגרף המכוון G_{f_k}.

חפש מסלול מכוון מאורך מינימלי בין s ל־t ע"י BFS.

אם אין מסלול כזה, סיים. $f = f_k$ היא זרימה מקסימלית ברשת.
אחרת, יהא $g_1, \dots, g_m$ מסלול מינימלי מכוון ב־G_{f_k} מ־s ל־t.
יהיו $e_1, \dots, e_m \in E(G)$ כך שלכל i $g_i = \vec{e_i}$ או $g_i = \overleftarrow{e}_i$.
$P = \{e_1, \dots, e_m\}$ הוא מסלול f_k לא־רווי.
נגדיר זרימה חדשה f_{k+1} על G ע"י

$$f_{k+1}(e) = \begin{cases} f_k(e) & e \notin \{e_1, \dots, e_m\} \\ f_k(e_i) + \varepsilon_{f_k,P} & g_i = \vec{e_i} \\ f_k(e_i) - \varepsilon_{f_k,P} & g_i = \overleftarrow{e}_i \end{cases}$$

אנו נראה כי אלגוריתם EK מסתיים אחרי $O(|V||E|)$ אטרציות.
לגרף מכוון $H = (V, E)$ נגדיר

$$d^+_G(u) = |\{v \ : \ uv \in E\}| \ , \ d^-_G(u) = |\{w \ : \ wu \in E\}| \quad \forall u \in V$$

<u>טענה</u>: יהיו $s \neq t$ קדקדים ב־H כך ש:

$$d^+_G(s) - d^-_G(s) = k > 0 \quad \text{ו־} \quad d^+_G(u) = d^-_G(u) \text{ לכל } u \neq s,t$$

אזי קיימים ב־H k מסלולים מכוונים זרים בצלעות מ־s ל־t.

<u>הוכחה</u>: אנדוקציה על k. בלי הגבלת הכלליות H אינו מכיל מעגלים מכוונים, כי השמטת מעגל מכוון אינה משנה את תנאי הדרגה במשפט.
נגדיר $v_0 = s$, מאחר ו־$d^+_G(v_0) \geq k > 0$ הרי שיש צלע, $E \ni v_0v_1$. מאחר ו־$d^+(v_1) = d^-(v_1) \geq 1$ הרי שיש צלע $E \ni v_1v_2$. נמשיך באופן זה לבנות מסילה מכוונת P_k שבהכרח תגיע לקדקד t.
נשמיט את המסילה המכוונת P_k מ־s ל־t. הגרף החדש $G' = (V, E - P)$ מקיים $d^+_{G'}(s) - d^-_{G'}(s) = k - 1$ ו $d^+_{G'}(u) = d^-_{G'}(u) \quad \forall u \neq s,t$.
לכן לפי הנחת האנדוקציה מכיל $k - 1$ מסלולים מכוונים, $P_1, \dots, P_{k-1}$, זרים בצלעות מ־s ל־t.
המסילות $P_1, \dots, P_k$ מקיימות את הדרוש.

$\square$

<u>משפט Edmonds- Karp</u>
יהיו $f_1, f_2, \dots$ הזרימות המתקבלות כך ש־f_{k+1} מתקבלת מ־f_k ע"י הגדלת הזרימה f_k על המסלול P_k ב־G_{f_k}. אזי

(i) $|E(P_k)| \leq |E(P_{k+1})|$

(ii) אם $k < l$ ו־P_k , P_l מכילים צלעות נגדיות $\vec{e}$, $\overleftarrow{e}$ אזי

$$|E(P_k)| + 2 \leq |E(P_l)|$$

(iii) אלגוריתם E_k מסתיים אחרי $\geq O(|V||E|)$ אטרציות.

הוכחה: (i) נגדיר גרף מכוון $H = (V, E(H))$ ע"י

$$E(H) = E(P_k) \cup E(P_{k+1}) - \bigcup_{\{\overrightarrow{e}, \overleftarrow{e}\} \subset E(P_k) \cup E(P_{k+1})} \{\overrightarrow{e}, \overleftarrow{e}\}$$

טענה: $E(H) \subset E(G_{f_k})$

הוכחה: ברור כי $E(P_k) \subset E(G_{f_k})$. תהא $g \in E(P_{k+1}) - E(G_{f_k})$.
אזי או ש־ $g = \vec{e}$ כאשר $e \in E$ ואזי $f_k(e) = c(e)$, $f_{k+1}(e) < c(e)$.
או ש־ $g = \overleftarrow{e}$ כאשר $e \in E$ ואזי $f_k(e) = 0$, $f_{k+1}(e) > 0$.
במקרה הראשון נובע כי $\overleftarrow{e} \in E(P_k)$,
ובמקרה השני נובע כי $\vec{e} \in E(P_k)$.
בכל מקרה הזוג $e, \overleftarrow{e} \not\ni E(H)$, ולכן $E(H) \not\ni g$.

הגרף H מקיים $d^+_H(s) - d^-_H(s) = 2$ ו־ $d^+_H(u) = d^-_H(u)$ לכל $u \neq s, t$ ולכן לפי טענה קודמת, H מכיל שני מסלולים זרים בקשתות Q_1, Q_2 מ־ s ל־t.
$E(G_{f_k}) \supset Q_1, Q_2$ לכן ממינימליות $|E(P_k)|$ נובע כי $|E(P_k)| \leq |E(Q_i)|$ $\quad i = 1, 2$ ולכן

$$2|E(P_k)| \leq |E(Q_1)| + |E(Q_2)| \leq |E(P_k)| + |E(P_{k+1})|$$

ולכן $|E(P_k)| \leq |E(P_{k+1})|$.

(ii) נשים לב כי מהוכחת (i) נובע כי אם P_k, P_{k+1} מכילים צלעות נגדיות $e, \overleftarrow{e}$ אזי

$$2|E(P_k)| \leq |E(Q_1)| + |E(Q_2)| \leq |E(P_k)| + |E(P_{k+1})| - 2$$

ולכן $|E(P_k)| + 2 \leq |E(P_{k+1})|$. זה מוכיח את המקרה $l = k + 1$. המקרה הכללי מוכח באינדוקציה על $l - k$.
ובאופן דומה: אם קיים $k < i < l$ כך ש־ P_k, P_i מכילים צלעות נגדיות אזי לפי הנחת האנדוקציה וסעיף (i):

$$|E(P_k)| + 2 \leq |E(P_i)| \leq |E(P_l)|$$

אחרת P_k, P_i אינם מכילים צלעות נגדיות ל $k < i < l$.
נגדיר עתה $H = (V, E(H))$ ע"י

$$E(H) = E(P_k) \cup E(P_l) - \bigcup_{\{e, \overleftarrow{e}\} \subset E(P_k) \cup E(P_l)} \{e, \overleftarrow{e}\}$$

ונמשיך כבסעיף (i).

(iii) בהנתן זרימה f ומסלול $s - t$ לא רווי P כך ש

$$\underline{\varepsilon}_{f,P} = \max_{e \in P} \varepsilon_{f,P}(e) > 0$$

נאמר כי $e \in P$ היא צואר בקבוק ל־f אם $\underline{\varepsilon}_{f,P} = \varepsilon_{f,P}(e)$.
נעיין בסדרת הזרימות $f_1, f_2, \ldots, f_m$ ובסדרת מסלולי ההרחבה $P_1, P_2, \ldots, P_m$.
ברור כי כל P_k מכיל צלע שהיא צואר בקבוק ל־f_k.

תהא $g \in \overrightarrow{E} \cup \overleftarrow{E}$, ונניח כי g הוא צואר בקבוק במסילות $P_{i_1}, P_{i_2}, \ldots, P_{i_r}$
$i_1 < \cdots < i_r$, אזי בהכרח קיימים

$$i_1 < j_1 < i_2 < j_2 < i_3 < \cdots < i_{r-1} < j_{r-1} < i_r$$

כך שהצלע ההפוכה ל־g מופיעה ב־ P_{j_l} $1 \le l \le r-1$. לכן לפי (ii)

$$|P_{i_l}| + 4 \le |P_{j_l}| + 2 \le |P_{i_{l+1}}|$$

ולכן

$$|V| - 1 \ge |P_{i_r}| \ge |P_{i_1}| + 4(r-1)$$

ולכן

$$\frac{|V|-1}{4} + 1 \ge r$$

ולכן

$$m \le \left(\frac{|V|-1}{4} + 1\right) \cdot 2|E| = O(|V||E|)$$

$\square$

שמושים של משפט הזרימה המקסימלית והחתך המינימלי

בעייה: נתונות n קבוצות כדורגל $1, \ldots, n$. קבוצות i, j משחקות ביניהן a_{ij} משחקים. כל קבוצה מקבלת נקודה אחת על כל ניצחון ואפס על כל הפסד. האם יש מהלך משחקים שבסופו כל קבוצה i תצבור $\ge b_i$ נקודות?

פתרון: נגדיר רשת $G = (V, E)$ עם

$$V = \{s\} \cup \{u_i\}_{i=1}^n \cup \{v_{ij}\}_{i \ne j = 1}^n \cup \{t\}$$

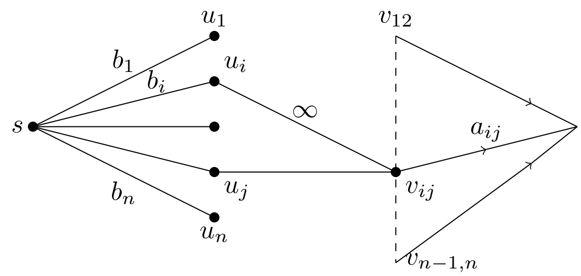
$$E = \{su_i\}_{i=1}^n \cup \{u_i\ v_{ij}\}_{i \ne j} \cup \{v_{ij}\ t\}_{ij}$$

וקבולים

$$c(su_i) = b_i \quad , \quad c(u_i\ v_{ij}) = \infty \quad , \quad c(v_{ij} t) = a_{ij}$$

טענה: יש מהלך משחקים שבו קבוצה i תצבור $\ge b_i$ נקודות לכל $1 \le i \le n$ אם ורק אם יש ברשת זרימה f שערכה $\sum_{ij} a_{ij}$.

הוכחה: נניח כי יש מהלך משחקים כנ"ל ונגדיר
$f(su_i) =$ מספר נצחונות של קבוצה i,
$f(u_i\ v_{ij}) =$ מספר נצחונות של קבוצה i על קבוצה j, ו־ $f(v_{ij} t) = a_{ij}$.
ברור כי f היא זרימה ב־G שערכה $\sum_{ij} a_{ij}$. הכוון ההפוך דומה.



<u>מסקנה</u>: קיים מהלך משחקים כנ"ל אם ורק אם לכל $K \subset [n]$

$$\sum_{ij\in\binom{K}{2}} a_{ij} \le \sum_{i\in K} b_i \qquad (*)$$

<u>הוכחה</u>: <u>הכרחיות</u>: נסמן ב־$\theta(i,j)$ את מספר המשחקים בהם i ניצח את j אזי

$$\sum_{ij\in\binom{K}{2}} a_{ij} = \sum_{\{ij\}\in\binom{K}{2}} [\theta(i,j)+\theta(j,i)] =$$

$$= \sum_{i\in K}\left[\sum_{\substack{j\in K\\ j\ne i}} \theta(i,j)\right] \le \sum_{i\in K} b_i$$

<u>מספיקות</u>: נניח כי $(*)$ מתקיים. יהא $(S,\bar{S})$ חתך s,t ברשת

$$S = \{s\}\cup\{u_i \ : \ i\in I\}\cup\{v_{rs} \ : \ \{r,s\}\in P\}$$
$$\bar{S} = \{t\}\cup\{u_i \ ; \ [n]-I\}\cup\{v_{rs} \ ; \ \{r,s\}\in\binom{[n]}{2}-P\}$$

אם קיים $i\in I$ כך ש־ $\{i,j\}\notin P$ עבור j כלשהוא אזי $c(S,\bar{S})=\infty$.
אחרת $P\supset\binom{[n]}{2}-\binom{\bar{I}}{2}$.
לכן

$$Cap(S,\bar{S}) \ge \sum_{i\notin I} b_i + \sum_{ij\in\binom{[n]}{2}-\binom{\bar{I}}{2}} a_{ij} \ge \sum_{ij} a_{ij}$$

כי

$$\sum_{ij\in\binom{\bar{I}}{2}} a_{ij} \le \sum_{i\in\bar{I}} b_i$$

$\square$

כיסויים וזווגים בגרפים דו־צדדיים

יהא $G=(V,E)$ גרף פשוט לא מכוון כלשהוא.
$M \subset E$ נקראת זווג (matching) אם $e_1 \cap e_2 = \emptyset$ לכל $e_1 \neq e_2 \in M$.
$S \subset V$ קראת כסוי (cover) אם $S \cap e \neq \emptyset$ לכל $e \in E$.
נסמן

$$\nu(G) = \max\{|M| \;:\; M \subset E \text{ זווג}\}$$

$$\tau(G) = \min\{|S| \;:\; S \subset V \text{ כיסוי}\}$$

ברור כי $\nu(G) \leq \tau(G)$ אך לא תמיד יש שיויון. למשל

$$\nu(K_n) = \left\lfloor \frac{n}{2} \right\rfloor \;,\; \tau(K_n) = n-1$$

משפט König: אם $G=(V=A\cup B, E)$ דו צדדי אזי

$$\nu(G) = \tau(G)$$

הוכחה: נגדיר רשת $H=(V',E')$ על ידי

$$V' = \{s\} \cup V \cup \{t\}$$
$$E' = \{sa\}_{a\in A} \cup E \cup \{bt\}_{b\in B}$$

וקבולים $c(e') \equiv 1$ לכל $e' \in E'$.

טענה: (i) לכל זרימה שלמה f ב־H מתקיים $val(f) \leq \nu(G)$.
(ii) לכל חתך $s-t$ $(S,\bar{S})$ ב־H מתקיים $\tau(G) \leq Cap(S,\bar{S})$.

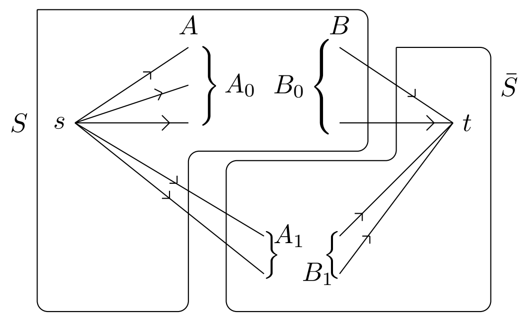
הוכחה: (i) אם f זרימה שלמה ב־H אזי
$M=\{ab \in E \;:\; f(ab)=1\}$ הוא זווג שגודלו

$$|H| = |\{ab \in E \;:\; f(ab)=1\}| =$$

$$= \sum_{ab \in A\times B \cap E} f(ab) = f(\{s\}\cup A, B\cup\{t\}) = val(f)$$

לכן

$$val(f) \leq \nu(G)$$



יהא $(S,\bar{S})$ חתך הנתון ע"י
$$\begin{aligned} S &= \{s\} \cup A_0 \cup B_0 \\ \bar{S} &= \{t\} \cup A_1 \cup B_1 \end{aligned}$$

$$Cap(S,\bar{S}) = |A_1| + e(A_0,B_1) + |B_0|$$

נבחר מכל צלע ב־$E(A_0,B_1)$ קדקד ותהא C הקבוצה המתקבלת. ברור כי $A_1 \cup C \cup B_0$ כיסוי של G שגודלו $Cap(S,\bar{S})$. לכן

$$Cap(S,\bar{S}) \geq \tau(G)$$

$\square$

תהא עתה f זרימה שלמה מקסימלית ויהא $(S,\bar{S})$ חתך מינימלי אזי

$$\nu(G) \geq val(f) = Cap(S,\bar{S}) \geq \tau(G)$$

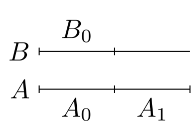
ולפיכך $\nu(G) = \tau(G)$.

$\square$

יהא $G = (A \cup B, E)$ גרף דו־צדדי. ל־$I \subset A$ נסמן

$$\Gamma(I) = \{b \in B \ : \ \exists a \in A \ , \ (a,b) \in E\}$$

<u>משפט Hall</u>: אם $|\Gamma(I)| \geq |I|$ לכל $I \subset A$ אזי G מכיל זווג המכסה את כל קדקדי A.



<u>הוכחה</u>: תהא $S \subset A \cup B$ המכסה את כל צלעות G. $B_0 = B \cap S$, $A_0 = A \cap S$.

נסמן $A_1 = A - A_0$, אזי $\Gamma(A_1) \subset B_0$ ולכן

$$|A| - |A_0| = |A_1| \leq |\Gamma(A_1)| \leq |B_0|$$

ולכן $|S| = |A_0| + |B_0| \geq |A|$. לכן לפי משפט König יש זווג בגודל $|A|$.

$\square$

<u>קשירות צלעית בגרפים מכוונים</u>

יהא $G=(V,E)$ גרף מכוון ויהיו s,t קדקדים שונים ב־ V. נגדיר

$\lambda_G(s,t) =$ מספר מקסימלי של מסלולים מכוונים זרים בקשתות מ־ s ל־ t

$k_G(s,t) =$ מספר מינימלי של קשתות ב־E שהשמטתן מנתקת את s מ־t

<u>משפט Menger</u>: $\lambda_G(s,t) = k_G(s,t)$

<u>הוכחה</u>: ברור כי $\lambda_G(s,t) \le k_G(s,t)$.
כוון שני: נתייחס ל־G כרשת כשכל הקבולים שווים ל־1.

<u>טענה</u>: (i) לכל זרימה שלמה f ב־G מתקיים $val(f) \le \lambda_G(s,t)$.
(ii) לכל חתך $s-t$ $(S,\bar{S})$ ב־G מתקיים $Cap(S,\bar{S}) \ge k_G(s,t)$.

<u>הוכחה</u>: (i) תהא f זרימה שלמה ב־G. נגדיר $E' = \{e \in E \ : \ f(e)=1\}$ אזי הגרף $G'=(V,E')$ מקיים $d^+(u)=d^-(u)$ לכל $u \ne s,t$ ו־$d^+(s)-d^-(s)=val(f)$.
לכן, לפי טענה שהוכחנו בשעור הקודם, G מכיל $val(f)$ מסלולים זרים בקשתות מ־s ל־t, ולכן $\lambda_G(s,t) \ge val(f)$.

(ii) יהא $(S,\bar{S})$ חתך $s-t$ ב־G. אזי ברור כי $S \times \bar{S} \cap E$ היא קבוצת צלעות הפוגשת כל מסלול מכוון מ־s ל־t.
לכן

$$k_G(s,t) \le |S \times \bar{S} \cap E| = Cap(S,\bar{S})$$

תהא עתה f זרימה שלמה מקסימלית ו־$(S,\bar{S})$ חתך מינימלי אזי

$$val(f) \le \lambda_G(s,t) \le k_G(s,t) \le Cap(S,\bar{S}) = val(f)$$

ולכן

$$\lambda_G(s,t) = k_G(s,t)$$

$\square$

<u>צירקולציות</u>

יהא $G=(V,E)$ גרף מכוון ופונקציות $\alpha,\beta : E \to \mathbb{R}$ כך שלכל $e \in E$

$$\alpha(e) \le \beta(e)$$

<u>צירקולציה</u> ב־G היא העתקה $g : E \to \mathbb{R}$ המקיימת

(i) $g^+(u) = g^-(u)$ לכל $u \in V$

$\alpha(e) \le g(e) \le \beta(e)$ (ii)

נגדיר רשת חדשה $H = (V', E')$ $\quad V' = \{s,t\} \cup V$

$$E' = E \cup \{su \ : \ u \in V\} \cup \{ut \ : \ u \in V\}$$

עם קבולים

$$c(e) = \begin{cases} \beta(e) - \alpha(e) & e = uv \in E \\ \alpha(V,u) & e = su \\ \alpha(u,V) & e = ut \end{cases}$$

כאשר כמקודם $\alpha(V,u) = \sum_{v \in V} \alpha(vu)$, $\alpha(u,V) = \sum_{v \in V} \alpha(uv)$

טענה: קיימת צירקולציה ב־G אם ורק אם קיימת זרימה ב־H שערכה $\alpha(V,V)$.

הוכחה: תהא $g : E \to \mathbb{R}$ צירקולציה. נגדיר $f : E' \to \mathbb{R}$ על ידי

$$f(e) = \begin{cases} g(e) - \alpha(e) & e = uv \in E \\ \alpha(V,u) & e = (su) \\ \alpha(u,V) & e = (ut) \end{cases}$$

אזי לכל $u \neq s,t$

$$f^+(u) = [g^+(u) - \alpha^+(u)] + \alpha^+(u) = g^+(u)$$
$$f^-(u) = [g^-(u) - \alpha^-(u)] + \alpha^-(u) = g^-(u)$$

לכן f זרימה וערכה הוא

$$val(f) = f(s,V) = \alpha(V,V)$$

להיפך, נניח f זרימה ב־H שערכה הוא $\alpha(V,V)$.
אזי $f(su) = \alpha(V,u)$ ו־$f(ut) = \alpha(u,V)$ לכל $u \in V$.
נגדיר לכל $uv \in E$ $\quad g(uv) = f(uv) + \alpha(uv)$.
ברור כי $\alpha(e) \le g(e) \le \beta(e)$ לכל $e \in E$.

$$g^+(u) = f(u,V) + \alpha(u,V) = f^+(u) = f^-(u) = f(V,u) + \alpha(V,u) = g^-(u)$$

$\square$

הערה: אלגוריתם EK והטענה דלעיל נותנים אלגוריתם יעיל למציאת צירקולציה ב־G אם יש כזו.

משפט (Hoffman): קיימת צירקולציה ב־G $\Leftrightarrow$ לכל חתך $(S,\bar{S})$

$$\alpha(S,\bar{S}) \le \beta(\bar{S},S)$$

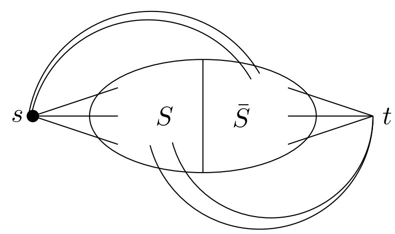
הוכחה: אם f צירקולציה ב־G אזי לכל חתך $(S,\bar{S})$

$$\alpha(S,\bar{S}) \le f(S,\bar{S}) = f(\bar{S},S) \le \beta(\bar{S},S)$$

כוון שני: לפי הטענה די להראות כי אם $\alpha(S,\bar{S}) \leq \beta(\bar{S},S)$ לכל חתך $(S,\bar{S})$ ב־ G אזי יש ב־H זרימה שערכה $\alpha(V,V)$.
לפי משפט MCMF די להראות כי לכל חתך (s,t) ב־H $(s \cup S, t \cup \bar{S})$ מתקיים $Cap(s \cup S, \bar{S} \cup t) \geq \alpha(v,V)$ ואכן

$$\begin{aligned} Cap(s \cup S, \bar{S} \cup t) &= \alpha(V,\bar{S}) + \left[\beta(S,\bar{S}) - \alpha(S,\bar{S})\right] + \alpha(S,V) \\ &= \alpha(V,V) - \alpha(V,S) + \left[\beta(S,\bar{S}) - \alpha(\bar{S},S)\right] + \alpha(\bar{S},S) - \alpha(S,\bar{S}) + \alpha(S,V) \\ &\geq \alpha(V,V) - \alpha(S,S) - \alpha(\bar{S},S) + \alpha(\bar{S},S) - \alpha(S,\bar{S}) + \alpha(S,S) + \alpha(S,\bar{S}) \\ &= \alpha(V,V) \end{aligned}$$

□



אלגוריתם אריתמטיים והצפנה צבורית

תזכורת מאריתמטיקה:

$\mathbb{Z} =$ חוג השלמים. מסמנים $a|b$ אם a מחלק את b, דהיינו אם קיים $q \in \mathbb{Z}$ כך ש־ $qa = b$.

חלוק עם שארית: ל־$a, b \in \mathbb{Z}$ ו־$a > 0$ קיימת הצגה יחידה $b = qa + r$ כאשר $q \in \mathbb{Z}$. $0 \leq r < a$. q, r נתונים על ידי

$$q = \left\lfloor \frac{b}{a} \right\rfloor \ , \ r = b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a$$

המחלק המשותף המקסימלי של a, b

$$qcd(a,b) = \max\{d > 0 \ : \ d|a,b\}$$

טענה: אם $b = qa + r$ אזי $gcd(a,b) = gcd(r,a)$

דוגמא:

$$gcd(57,72) = gcd(15,57) = gcd(12,15) = gcd(3,12) = gcd(0,3) = 3$$

אלגוריתם אוקלידס למציאת gcd

יהיו $b \geq a \geq 0$ $\quad (a,b) \neq (0,0)$.

נגדיר $c_1 = b \ , \ c_2 = a$. נניח שהגדרנו $c_1, \ldots, c_k$ $k \geq 2$.

אם $c_k = 0$ אזי $gcd(a,b) = c_{k-1}$. אחרת נחלק עם שארית $c_{k-1} = 0 \leq a_{k+1} < a_k$ $q_k c_k + c_{k+1}$, ונקבל על ידי זה את c_{k+1}.

סבוכיות אלגוריתם אוקלידס

תהא $\{f_k\}_{k=0}^{\infty}$ סדרת פיבונצ'י:

$$f_0 = 0 \ , \ f_1 = 1 \ , \ f_k = f_{k-1} + f_{k-2} \qquad k \geq 2$$

תזכורת:

$$f_k = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right]$$

נסמן ב־ $E(a,b)$ את מספר האטרציות (חלוקות עם שארית) שמבצע אלגוריתם אוקלידס על הזוג (a,b).

טענה: לכל $k \geq 0$ $\quad E(f_k, f_{k+1}) = k$

הוכחה: אינדוקציה על k: $k = 0$ ברור. יהא $k > 0$ אזי

$$E(f_k, f_{k+1}) = 1 + E(f_{k+1} - f_k, f_k) = 1 + E(f_{k-1}, f_k) = 1 + (k-1) = k$$

$\square$

<u>טענה</u>: יהא $k \geq 1$. אם $f_k \geq b$ או $f_{k-1} \geq a$ אזי $E(a,b) \leq k$.

<u>הוכחה</u>: אינדוקציה על k: המקרה $k = 1$ ברור. נניח $k \geq 2$.
נחלק עם שארית $b = qa + r \quad 0 \leq r < a$
אם $a \leq f_{k-1}$ אזי

$$E(a,b) = 1 + E(r,a) \qquad \overset{\substack{\text{אינדוקציה} \\ \downarrow}}{\leq} \qquad 1 + (k-1) = k$$

אחרת $f_k \geq b$, $a \leq f_{k-1}$ ואזי

$$r \leq b - a \leq f_k - f_{k-1} = f_{k-2}$$

ושוב לפי הנחת האנדוקציה

$$E(a,b) = 1 + E(r,a) \leq 1 + (k-1) = k$$

$\square$

<u>טענה</u>: לכל $\mathbb{Z}^2 \ni (a,b) \neq (0,0)$ קיימים $x, y \in \mathbb{Z}$ כך ש־

$$\gcd(a,b) = x \cdot a + y \cdot b$$

<u>הוכחה</u>: בלי הגבלת הכלליות $0 \leq a \leq b$. נוכיח את הטענה באינדוקציה על a. אם $a = 0$ אזי $\gcd(0,b) = b = 0 \cdot a + 1 \cdot b$.
נניח $a > 0$. נחלק עם שארית $b = \left\lfloor \frac{b}{a} \right\rfloor \cdot a + r \quad 0 \leq r < a$.
לפי הנחת האינדוקציה קיימים $x', y' \in \mathbb{Z}$ כך ש

$$\gcd(r,a) = x' \cdot r + y' \cdot a$$

ואזי

$$\gcd(a,b) = \gcd(r,a) = x' \cdot r + y' \cdot a = x' \left(b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a \right) + y' \cdot a$$

$$\left(y' - x' \left\lfloor \frac{b}{a} \right\rfloor \right) \cdot a + x' \cdot b$$

נסמן $(x,y) = \left(y' - x' \left\lfloor \frac{b}{a} \right\rfloor \ , \ x' \right)$, אזי $\gcd(a,b) = x \cdot a + y \cdot b$.

<u>דוגמא:</u> $(a,b)=(21,111)$

a	b	$\left\lfloor \frac{b}{a} \right\rfloor$	x	y
21	111	5	16	-3
6	21	3	-3	1
3	6	2	1	0
0	3	$-$	0	1

יהא $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\{0,1,\dots,n-1\}$ חוג השאריות מודולו n,
ותהא $\mathbb{Z}_n^*=\{a\in\mathbb{Z}_n \ : \ \gcd(a,n)=1\}$ החבורה הכפלית של האיברים ההפיכים ב־ $\mathbb{Z}_n$.
חישוב ההפכי ב־$\mathbb{Z}_n^*$ מתבצע באופן הבא: יהא $a\in\mathbb{Z}_n^*$ אזי קיימים $(x,y)\in\mathbb{Z}^2$ כך ש־
$x\cdot a+y\cdot n=\gcd(a,n)=1$ ולכן $a^{-1}\equiv x(mod\ n)$.

<u>משפט השארית הסיני</u>

יהיו $n_1,\dots,n_k$ זרים בזוגות אזי ההעתקה

$$F:\mathbb{Z}_{n_1\dots n_k}\to\mathbb{Z}_{n_1}\oplus\cdots\oplus\mathbb{Z}_{n_k}$$

הנתונה ע"י

$$F(x)=(x(mod\ n_1),\dots,x(mod\ n_k))$$

היא איזימורפיזם של חוגים.

<u>הוכחה:</u> ברור כי F היא הומומורפיזם של חוגים.
ההעתקה F חח"ע: אם $F(x)=F(y)$ אזי $x(mod\ n_i)=y(mod\ n_i)$ כלומר $n_i|y-x$
לכל $1\le i\le k$ ולכן $n_1\cdots n_k|y-x$, כלומר $x\equiv y(mod\ n_1\cdots n_k)$.
העובדה כי ההעתקה F היא על נובעת מחח"ע F ומכך ש ־

$$|\mathbb{Z}_{n_1\cdots n_k}|=n_1\cdots n_k=|\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_1}|$$

גרסא אלגוריתמית למשפט השאריות הסיני.
כמקודם יהיו $n_1,\dots,n_k$ זרים בזוגות לכל $1\le i\le k$ $\quad \prod_{j\ne i} n_j\in\mathbb{Z}_{n_i}^*$ ולכן קיים $\alpha_i\in\mathbb{Z}_{n_i}^*$
כך ש־

$$\left(\prod_{j\ne i} n_j\right)\alpha_i\equiv 1(mod\ n_i)$$

<u>טענה:</u> יהיו $a_i\in\mathbb{Z}_{n_i}$ $\ 1\le i\le k$. אזי
$x=\sum_{i-1}^{k} a_i\left(\prod_{j\ne i} n_j\right)\alpha_i$ מקיים $x\equiv a_\ell(mod\ n_\ell)$ לכל $1\le\ell\le k$.

<u>הוכחה:</u>

$$\begin{aligned} x(mod\ n_\ell) &= \sum_{i=1}^{k} a_i\left(\prod_{j\ne i} n_j\right)\alpha_i(mod\ n_\ell) \\ &= a_\ell\prod_{j\ne i} n_j\alpha_\ell(mod\ n_\ell)=a_\ell(mod\ n_\ell) \end{aligned}$$

דוגמא: $(n_1,n_2,n_3)=(5,6,7)$

$$\alpha_1=(n_2n_3)^{-1}(mod\ n_1)=42^{-1}(mod\ 5)=3$$
$$\alpha_2=(n_1n_3)^{-1}(mod\ n_2)=35^{-1}(mod\ 6)=5$$
$$\alpha_3=(n_1n_2)^{-1}(mod\ n_3)=30^{-1}(mod\ 7)=4$$

לכן

$$\begin{aligned} x &= 42\cdot 3a_1+35\cdot 5a_2+30\cdot 4a_3 \\ &= 126a_1+175a_2+120a_3 \end{aligned}$$

מקיים $x(mod\ n_i)=a_i$ לכל $1\le i\le 3$.

טענה: אם $n_1,\dots,n_k$ זרים בזוגות אזי F היא איזומורפיזם של חבורות אבליות

$$F:\mathbb{Z}^*_{n_1,\dots,n_k}\to\mathbb{Z}^*_{n_1}\times\cdots\times\mathbb{Z}^*_{n_k}$$

הוכחה: אם $x\in\mathbb{Z}^*_{n_1\cdots n_k}$ אזי $x(mod\ n_i)\in\mathbb{Z}^*_{n_i}$ לכל $1\le i\le k$
ולכן $F(x)\in\mathbb{Z}^*_{n_1}\times\cdots\times\mathbb{Z}^*_{n_k}$.
כמוכן, אם $(a_1,\dots,a_k)\in\mathbb{Z}^*_{n_1}\times\cdots\times\mathbb{Z}^*_{n_k}$ ו־ $x\in\mathbb{Z}_{n_1,\dots,n_k}$ מקיים $F(x)=(a_1,\dots,a_k)$
אזי $\gcd(x,n_i)=1$ לכל $1\le i\le k$ ולכן $\gcd(x,n_1\cdots n_k)=1$, כלומר $x\in\mathbb{Z}^*_{n_1\cdots n_k}$.

מספר האיברים ב־ $\mathbb{Z}^*_n$ מסומן ב $\varphi(n)$ ונקרא פונקציית אוילר של n.

טענה: אם $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ כאשר p_i ראשוניים שונים ו־ $\alpha_i\ge 1$ אזי

$$\varphi(n)=\sum_{i=1}^{k}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

הוכחה: נובע מהכפליות

$$\varphi(n)=\left|\mathbb{Z}^*_{p_1^{\alpha_1}\cdots p_k^{\alpha_k}}\right|=\left|\mathbb{Z}^*_{p_1^{\alpha_1}}\times\cdots\times\mathbb{Z}^*_{p_k^{\alpha_k}}\right|=\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$$

ומכך ש־ $\varphi(p_i^{\alpha_i})=p_i^{\alpha_i}-p_i^{\alpha_i-1}$.

המשפט הקטן של פרמה:
אם $\gcd(a,n)=1$ אזי $a^{\varphi(n)}\equiv 1(mod\ n)$.

הוכחה: $a\in\mathbb{Z}^*_n$ לכן ב־ $\mathbb{Z}^*_n$:

$$a^{\varphi(n)}=a^{|\mathbb{Z}^*_n|}=1$$

סבוכיות של פעולות אריתמטיות ב־ $\mathbb{Z}_n$

טענה: הסבוכיות של פעולות אריטמטיות ב־ $\mathbb{Z}_n$ חסומה כלהלן:

פעולה	סבוכיות
חבור	$O(\log n)$
כפל	$O(\log^2 n)$
חלוק עם שארית	$O(\log^2 n)$
העלאה בחזקה	$O(\log^3 n)$

<u>הוכחה:</u> החסמים לגבי חבור, כפל וחלוק עם שארית נובעים מידית מהאלגוריתמים הסטנדרטים לפעולות אלה. נתאר עתה אלגוריתם יעיל להעלאה בחזקה.

יהא $0 \le b \le n$, ויהא $a \in \mathbb{Z}_n$.

נכתוב $b = \sum_{i=0}^{t} b_i z^i$, $b_i \in \{0,1\}$, $t \le \log n - 1$.

נגדיר ברקורסיה סדרה $c_0, \ldots, c_t \in \mathbb{Z}_n$ כדלקמן:

$$c_0 = a^{b_t},$$
$$c_k \equiv_n c_{k-1}^2 \cdot a^{b_{t-k}} \quad 1 \le k \le t \text{ לכל}$$

קל לבדוק כי $a^b \equiv c_t (mod\ n)$. מאחר וחישוב c_k מתוך c_{k-1} מבוצע ע"י שלושה כפלים, סיבוכיותו היא $O(\log^2 n)$ ולכן הסבוכיות הכוללת הוא

$$t \cdot O(\log^2 n) = O(\log^3 n)$$

<u>אלגוריתמים הסתברותיים</u>

עד כה עסקנו באלגוריתמים דטרמיניסטיים, כאלה שפלט האלגוריתם תלוי אך ורק בקלט, ושתי הרצות שונות של אותו אלגוריתם על אותו קלט ייצרו אותו פלט. כמו שנראה בהמשך, ישנם מצבים בהם כדאי לאפשר לאלגוריתם להטיל מטבעות במהלך הריצה, בתנאי שההסתברות לפלט מוטעה תהיה קטנה למדי. ננסח את הדברים בדרך (סמי־)פורמלית.

תהא $\{0,1\}^*$ קבוצת כל המחרוזות הסופיות של 0 ו־1. ל־ $x = (x_1, \ldots, x_n) \in \{0,1\}^*$ נסמן $|x| = n$. שפה היא תת קבוצה $L \subset \{0,1\}^*$.

כל בעיית הכרעה אפשר לקודד כשפה $L \subset \{0,1\}^*$.

<u>דוגמאות:</u>

$$L = \{G \ : \ G \text{ גרף דו־צדדי}\}$$
$$L = \{X \in \mathbb{N} \ : \ x \text{ ראשוני}\}$$

אלגוריתם (דטרמיניסטי) המכריע שייכות לשפה L הוא אלגוריתם A הפועל על מחרוזות סופיות ומייצר פלט ב־ $\{0,1\}$ כך ש־

$$\{x \ : \ A(x) = 1\} = L$$

אלגוריתם הסתברותי ε־טוב לשפה L הוא אלגוריתם B המקבל כקלט $x \in \{0,1\}^*$ ומשתנה מקרי w (המייצג מספר הטלות מטבע) כך ש ־

$$Pr\left[B(w,x) = 0 \mid x \in L\right] = 0$$

וגם

$$Pr\left[B(w,x) = 1 \mid x \notin L\right] < \varepsilon$$

כלומר, אם הפלט של B הוא 0 אזי בבטחון $x \notin L$,

מאידך אם $x \in L$ אזי $B(w,x) = 1$ בהסתברות $1 - \varepsilon$.

<u>דוגמא (מלאכותית במקצת):</u>

נתון קלט $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ ונתון כי מתקיימים אחד משני התנאים הבאים:

I. $x = (0, \ldots, 0)$

או

II. $|\{i \;:\; x_i = 0\}| = \frac{n}{2}$

בעייה: קבע האם x מקיים I או II.

אלגוריתם דטרמיניסטי לבעייה: בדוק את x_i $\;1 \le i \le \frac{n}{2}+1$ בזה אחר זה.
אם אחד מהם הוא 1 אזי x מקיים II. אחרת x מקיים I.
אלגוריתם זה יבצע במקרה הרע ביותר $\frac{n}{2}+1$ בדיקות.
נתאר עתה אלגוריתם הסתברותי לבעייה המבצע הרבה פחות בדיקות, ויחד עם זאת טועה בהסתברות נמוכה. יהא $\varepsilon > 0$.

אלגורתם B: יהא $s = \lceil \log_2 \frac{1}{\varepsilon} \rceil$. ל $k=1$ עד $k=s$ בצע:
בחר $1 \le i \le n$ באופן מקרי. אם $x_i = 1$ קבע $B(x) = \mathrm{II}$ וסיים.
אם $x_i = 0$ עבור ל־ k הבא. אם ב־s ההגרלות קבלנו $x_i = 0$ נקבע $B(x) = \mathrm{I}$.

$$Pr\left[B(x) = \mathrm{II} \mid \text{מקיים I } x\right] = 0$$
$$Pr\left[B(x) = \mathrm{I} \mid \text{מקיים II } x\right] = \left(\tfrac{1}{2}\right)^s < \varepsilon$$

מספר הבדיקות שבצענו הוא $s = \lceil \log_2 \frac{1}{\varepsilon} \rceil$.
לדוגמא, אם אנו מוכנים לקבל תשובה מוטעית בהסתברות של 2^{-50}, די להסתפק ב־ 50 בדיקות במקום $\frac{n}{2}+1$.

מציאת ראשוניים גדולים
משפט המספרים הראשוניים PNT (Hadamard, de la Vallee-Poussin)
נסמן ב־$\pi(x) = |\{p :\ \text{ראשוני } p \le x\}|$
אזי
$$\pi(x) \sim \frac{x}{\ln x}$$
משפט המספרים הראשוניים אומר כי הצפיפות של המספרים הראשוניים עד x היא בערך $\frac{1}{\ln x}$, ולכן אם נבדוק נניח $10 \ln x$ מספרים החל מ־x הרי שסביר שביניהם נמצא מספר ראשוני.
הבעיה המרכזית היא כיצד לקבוע האם מספר נתון n הוא ראשוני.
דרך פשוטה לעשות זאת היא לבדוק האם n מתחלק ב־k עבור $k < \sqrt{n}$ כלשהוא. ברור עם זאת שחפוש על $\sqrt{n}$ מספרים כאשר $n = 10^{200}$ אינו אפשרי. אנו נתאר אלגוריתם הסתברותי ε־טוב לבדיקת ראשונות עם זמן ריצה $O(\log_{\frac{1}{3}} \log^3 n)$.

עדים לפריקות
יהא $n > 1$ איזוגי, ונכתוב $n - 1 = 2^t u$ $\;2 \not| u$.
נגדיר

$$W_1(n) = \{a \in \mathbb{Z}_n^* \;:\; a^{n-1} \not\equiv 1 (mod\ n)\}$$
$$W_2(n) = \{a \in \mathbb{Z}_n^* \;:\; \exists 1 \le i \le t\ a^{2^{i-1}u} \not\equiv \pm 1 (mod\ n)\ ,\ a^{2^i u} \equiv 1 (mod\ n)\}$$

טענה: $W_1(n) \cup W_2(n) \neq \emptyset \Leftarrow n$ פריק.

הוכחה: אם $a \in W_1(n)$ אזי $a^{n-1} \not\equiv 1 (mod\ n)$ ולכן לפי המשפט הקטן של פרמה n פריק.

אם $a \in W_2(n)$ אזי $\lambda = a^{2^{i-1}u} \not\equiv_n \pm 1$ ומקיים $\lambda^2 \equiv 1(mod\ n)$.
כלומר למשוואה $z^2 - 1 = 0$ יש לפחות שלושה שורשים ב־$\mathbb{Z}_n$: $\pm 1, \lambda$. לכן $\mathbb{Z}_n$ אינו שדה ולכן n פריק.

<u>הערה:</u> מספר פריק n עבורו $W_1(n) = \emptyset$ נקרא מספר Carmichael.
למשל $n = 3 \cdot 11 \cdot 17 = 561$ הוא מספר כזה.
ידוע כי יש אינסוף מספרי קרמייקל.

<u>טענה:</u> אם $W_1(n) \neq \emptyset$ אזי $|W_1(n)| \geq \dfrac{\varphi(n)}{2}$

<u>הוכחה:</u> $G_1 = \mathbb{Z}_n^* - W_1(n) \neq \mathbb{Z}_n^*$ היא תת חבורה של $\mathbb{Z}_n^*$, ולכן $|G_1| \leq \frac{\varphi(n)}{2}$ ולכן $W_1(n) \geq \frac{\varphi(n)}{2}$.

<u>טענה:</u> אם n פריק ו־$W_1(n) = \emptyset$ (כלומר n מספר כרמייקל) אזי $|W_2(n)| \geq \frac{\varphi(n)}{2}$.
<u>הוכחה:</u> ראשית נשים לב כי $n \neq p^l$ כאשר p ראשוני ו־$l \geq 2$.
ואכן, אם $n = p^l$ כנ"ל אזי ידוע כי $\mathbb{Z}_n^*$ ציקלית מסדר $\varphi(n) = p^{l-1}(p-1)$.
יהא α יוצר של $\mathbb{Z}_n^*$ אזי $\alpha^{p^l - 1} \not\equiv 1(mod\ p^l)$. כי הסדר של α הוא $p^{l-1}(p-1)$ ו $p^{l-1}(p-1) \not| p^l - 1$.
נכתוב, על כן, $n = n_1 n_2$ כאשר $\gcd(n_1, n_2) = 1$, $n_1, n_2 > 1$.
יהא $0 \leq j \leq t$ המקסימלי כך שקיים $\alpha \in \mathbb{Z}_n^*$ המקיים $\alpha^{2^j u} \equiv -1(n)$.
(קיים j כזה כי $(-1)^u \equiv -1(n)$).
נגדיר

$$G_2 = \{x \in \mathbb{Z}_n^* \ : \ x^{2^j u} \equiv \pm 1(mod\ n)\}$$

<u>טענה:</u> $\mathbb{Z}_n^* - G_2 \subset W_2(n)$
<u>הוכחה:</u> יהא $x \in \mathbb{Z}_n^* - G_2$. אזי $x^{2^j u} \not\equiv \pm 1(n)$. יהא i מינימלי כך ש־ $x^{2^i u} \equiv 1(n)$
(קיים כזה כי $x^{2^t u} = x^{n-1} \equiv 1(n)$). אזי $x^{2^{i-1}u} \not\equiv 1(n)$
מאידך אם $x^{2^{i-1}u} \equiv -1(n)$ אזי $i - 1 \leq j$ ולכן $x^{2^j u} \equiv \pm 1(n)$. סתירה.
לכן $x^{2^{i-1}u} \equiv \pm 1(n)$.

<u>טענה:</u> $G_2 \subsetneqq \mathbb{Z}_n^*$
<u>הוכחה:</u> יהא $x \in \mathbb{Z}_n^*$ כך ש:

$$\begin{cases} x \equiv \alpha(n_1) \\ x \equiv 1(n_2) \end{cases}$$

אזי

$$\begin{aligned} &x^{2^j u} \equiv_{n_1} \alpha^{2^j u} \equiv_{n_1} -1 \\ &x^{2^j u} \equiv_{n_2} 1 \end{aligned}$$

ולכן $x^{2^j u} \not\equiv \pm 1(n)$.

<u>מסקנה:</u> $|G_2| \leq \dfrac{\varphi(n)}{2}$ ולכן $|W_2(n)| \geq \frac{\varphi(n)}{2}$.

<u>האלגוריתם ההסתברותי של מילר־רבין לבדיקת ראשוניות</u>
יהא $\varepsilon > 0$. נתאר אלגוריתם ε־טוב לבדיקת ראשוניות של $n > 1$ איזוגי.

נציג $n-1=2^t u$ כאשר $2 \not| u$. יהא $s=\lceil \log_2 \frac{1}{\varepsilon} \rceil$.
עבור $1 \le j \le s$ נבצע את התהליך הבא: נגריל $1 < a_j < n$ מקרי.

I. אם $\gcd(a_j,n) > 1$ הכרז n פריק, סיים.

אחרת, חשב את הסדרה $a_j^u, a_j^{2u}, \ldots, a_j^{2^t u} = a_j^{n-1}$.

II. אם $a_j^{n-1} \not\equiv \pm 1(n)$ הכרז n פריק, סיים.

III. אחרת, יהא i המינימלי כך ש- $a_j^{2^i u} \equiv 1(n)$.

אם $a_j^{2^{i-1}u} \not\equiv \pm 1(n)$ הכרז n פריק, סיים.

IV. אם בכל s האיטרציות n לא הוכרז פריק, הכרז n ראשוני.

נתוח האלגוריתם: אם n הוכרז כפריק בשלב I , אזי $\gcd(a,n) > 1$ ו־n אכן פריק. אם n הוכרז כפריק בשלב II אזי $a \in W_1(n)$ ובפרט $W_1(n) \ne \emptyset$ ולכן n פריק. אם n הוכרז כפריק בשלב III אזי $a \in W_2(n)$ ובפרט $W_2(n) \ne \emptyset$ ולכן n פריק.

מסקנה: אם האלגוריתם הכריז על n כפריק, אזי n אכן פריק.
נדון כעת במקרה ש־n הוכרז כראשוני בשלב IV. אם n אכן ראשוני אזי ההכרזה נכונה.
יתכן, עם זאת, ש־n אינו ראשוני.
נעריך עתה את ההסתברות המותנה

$$Pr\left[n \text{ פריק} \mid n \text{ הוכרז ראשוני} \right]$$

נפריד לשני מקרים:

(i) $W_1(n) \ne \emptyset$. מכך שהכרזנו על n כראשוני נובע כי כל $a_1, \ldots, a_s$ שבחרנו מקיימים $a_i \in \mathbb{Z}_n^* - W_1(n)$. לכן במקרה זה

$$Pr\left[n \text{ פריק} \mid n \text{ הוכרז ראשוני} \right] \le \left(\frac{|\mathbb{Z}_n^* - W_1(n)|}{\varphi(n)} \right)^s = \left(1 - \frac{|W_1(n)|}{\varphi(n)} \right)^s$$

$$\le \left(\frac{1}{2} \right)^s \le \varepsilon$$

(ii) $W_1(n) = \emptyset$. מכך שהכרזנו על n כראשוני נובע כי כל $a_1, \ldots, a_s$ שבחרנו מקיימים $a_i \in \mathbb{Z}_n^* - W_2(n)$. ולכן

$$Pr\left[n \text{ פריק} \mid n \text{ הוכרז ראשוני} \right] \le \left(\frac{|\mathbb{Z}_n^* - W_2(n)|}{\varphi(n)} \right)^s \le \left(1 - \frac{|W_2(n)|}{\varphi(n)} \right)^s$$

$$\le \left(\frac{1}{2} \right)^s \le \varepsilon$$

לכן בכל מקרה

$$Pr\,[n \text{ הוכרז ראשוני} \mid n \text{ פריק}] \leq \varepsilon$$

כלומר האלגוריתם הוא ε־טוב.

סבוכיות אלגורתם מילר־רבין

סבוכיות חשוב הסדרה $a_j^u, \ldots, a_j^{2^t u}$ היא $O(\log^3 n)$

ולכן סבוכיות האלגוריתם היא $O(s\log^3 n) = O(\log\frac{1}{\varepsilon}\cdot\log^3 n)$

הצפנה ציבורית בשיטת RSA

בעיית ההצפנה

נניח כי Alice ו־ Bob רוצים לשלוח ביניהם הודעות מוצפנות כך שצד שלישי המצותת להן לא יוכל לפענח את תוכנן. כיצד יוכלו לעשות זאת?

שיטת ההצפנה הקלאסית

מניחים כי כל הודעה מורכבת מ־n אותיות לועזיות ושכל אות מיוצגת ע"י j, כאשר $0 \leq j \leq 25$. Alice ו־ Bob נפגשים מראש ומחליטים על פונקצית הצפנה סודית E ופונקצית פענוח (סודית גם כן) $D = E^{-1}$. לכל הודעה אפשרית M מתקיים $D(E(M)) = M$.

נביא כמה דוגמאות לצפנים (נניח שההודעה היא $M = (x_1, \ldots, x_n)$):

1. צופן המיוחס ליוליוס קיסר:

$$E(x_1, \ldots, x_n) = ((x_1+3) mod\ 26, \ldots, (x_n+3) mod\ 26)$$

פונקצית הפענוח במקרה זה היא:

$$D(x_1, \ldots, x_n) = ((x_1-3) mod\ 26, \ldots, (x_n-3) mod\ 26)$$

2. צופן מהסוג המתואר בספרי מתח נושנים:

תהי z_i האות הראשונה בעמוד i של הספר "אנה קרנינה" (נניח שבידי Alice ו־ Bob אותה מהדורה). נגדיר:

$$E(x_1, \ldots, x_n) = ((x_1+z_i) mod\ 26, \ldots, (x_n+z_i) mod\ 26)$$

פונקצית הפענוח היא:

$$D(x_1, \ldots, x_n) = ((x_1-z_i) mod\ 26, \ldots, (x_n-z_i) mod\ 26)$$

3. צופן אקראי:

בפגישתם Alice ו־ Bob מגרילים סדרה "מקרית" $(z_1, \ldots, z_n)$ ומגדירים את פונקציות ההצפנה והפענוח כמו בדוגמא הקודמת. אם הסדרה $(z_1, \ldots, z_n)$ היא אכן "מקרית", שיטת הצפנה זו היא בטוחה לחלוטין (להודעה בודדת באורך n).

בשיטת ההצפנה הקלאסית ישנן מספר בעיות:

(א) קשה לייצר סדרות שדומות למקריות.

(ב) השיטה מחייבת <u>תיאום מראש</u> בין Alice ו־ Bob.

<u>שיטת ההצפנה הציבורית</u>

כעת נניח ש ־ Alice מעוניינת לקבל הודעות מוצפנות מציבור גדול של משתמשים <u>מבלי</u> להיפגש איתם מראש. נסמן את מרחב ההודעות האפשריות ב־ $\mathbb{M}$.
הרעיון הוא פשוט: Alice תבחר פונקצית חח"ע ועל $E : \mathbb{M} \to \mathbb{M}$ ותפרסם ברבים (למשל, במדריך הדומה למדריך טלפונים) את האלגוריתם לחישוב הפונקציה E. פונקצית הפענוח תיקרא, כמקודם D ותקיים:

$$\forall M \in \mathbb{M} \ : \ D(E(M)) = M$$

לכאורה, נוצרת בעיה: אם הפונקציה E ידועה לכל, אזי כל מצותת יוכל לחשב את הפונקציה ההופכית $D = E^{-1}$ ולפענח את התקשורת המוצפנת ע"י כך שיעבור על מרחב ההודעות האפשריות $\mathbb{M}$ וימצא את $E(M)$ לכל הודעה $M \in \mathbb{M}$. ברם, אם המרחב $\mathbb{M}$ הוא מספיק גדול (נניח מסדר גודל של 10^{700}) שיטה זו למציאת D אינה מציאותית.
ננסח, אפוא, את הדרישות מפונקצית הצפנה טובה E עבור שיטת ההצפנה הציבורית:

1. E ניתנת לחישוב מהיר על כל קלט $M \in \mathbb{M}$.

2. Alice יכולה לחשב את D במהירות על כל $M \in \mathbb{M}$.

3. למרות ש־ E נתונה, איש מלבד Alice אינו יכול לחשב את D בזמן סביר.

פונקציה כזו נקראת trapdoor function (מונח זה נטבע ע"י Diffie ו־ Hellman בשנת 1976).

<u>שיטת RSA</u>

בשנת 1977 המציאו Rivest, Shamir ו־ Adleman את אלגוריתם RSA שרבים משערים כי הוא ממש trapdoor function. נתאר כעת אלגוריתם הצפנה פופולרי זה:
Alice מוצאת (למשל בשיטת מילר־רבין) שני מספרים ראשוניים p, q גדולים (נניח מסדר גודל של 10^{700}) ומחשבת את $n = pq$. עתה Alice בוחרת מספר e (די גדול) שמקיים $(e, (p-1)(q-1)) = 1$. מרחב ההודעות מוגדר להיות $\mathbb{M} = \mathbb{Z}_n^*$.
Alice מפרסמת את הזוג (n, e) בפומבי ומגדירה את פונקצית ההצפנה $E : \mathbb{M} \to \mathbb{M}$ ע"י:

$$\forall x \in \mathbb{M} \ : \ E(x) = x^e (mod \ n)$$

לאחר מכן Alice מחשבת בעזרת אלגוריתם אוקלידיס את ההופכי ל־e
מודולו $(p-1)(q-1)$, כלומר מוצאת מספר d המקיים

$$de \equiv mod \ (p-1)(q-1)$$

הפונקציה ההופכית ל־E נתונה ע"י:

$$\forall y \in \mathbb{M} \ : \ D(y) \equiv y^d (mod \ n)$$

נוודא שהפונקציה D אכן הופכית ל-E:

$$\forall x \in \mathbb{M} \; : \; D(E(x)) = (x^e)^d mod \; n = x^{1+\lambda(p-1)(q-1)} mod \; n$$

לפי הנוסחה שהוכחנו לפונקצית אוילר, מתקיים:

$$\phi(n) = \phi(pq) = (p-1)(q-1)$$

ולכן, לפי המשפט הקטן של פרמה:

$$x^{1+\phi(n)} (mod \; n) \equiv x (mod \; n)$$

לפיכך:

$$D(E(x)) = x$$

<u>הערה:</u> מאחר והזוג (n, e) ידוע ברבים הרי שע"י פירוק n לגורמים ראשוניים p, q אפשר לחשב את d ואת פונקצית הפענוח D. החסינות של שיטת RSA מבוססת על ההשערה (שטרם הוכחה) כי פירוק מספר לגורמיו היא בעייה חישובית קשה.

מבוא לסבוכיות של חשובים

בעיות אופטימיזציה ובעיות הכרעה

הבעיות האלגוריתמיות בהן עסקנו עד כה הן בדרך כלל בעיות אופטימיזציה, למשל מציאת העץ הפורש המינימלי, מציאת המסלול הקצר ביותר בין זוג קדקדים בגרף, מציאת הזרימה המקסימלי ברשת וכיו"ב.

בעיות הכרעה, הינן, מאידך, בעיות שהתשובה עליהן היא כן או לא.

למשל, בהנתן גרף ממושקל G ומספר k, הכרע האם הגרף מכיל עץ פורש שמשקלו $\geq k$.

בדיון בנושא סבוכיות, מתייחסים בד"כ לבעיות הכרעה בלבד.

הסיבה היא שאם נתונה בעיית אופטימיזציה P, ואם Q בעיית ההכרעה הנגזרת ממנה, אזי אם יש ל־Q אלגוריתם פולונומיאלי, אזי גם ל־P יש אלגוריתם פולינומיאלי ־ יתכן עם מעריך חזקה גדול יותר.

דוגמא: תהא P בעיית האופטימיזציה הבאה: בהנתן גרף $G = (V, E)$ מצא $S \subset V$ כיסוי צלעות מינימלי בגודלו $S = \tau(G)$.

תהא Q בעיית ההכרעה המתאימה: בהנתן זוג (G, k) (k טבעי) קבע האם $\tau(G) \leq k$.

נסמן ב־ $f(n)$ את סיבוכיות P על גרף עם n קדקדים, ונסמן ב־$g(n, k)$ את סבוכיות Q על גרף עם n קדקדים ו־ $1 \leq k \leq n$

טענה: אם $g(n, k) \leq O(n^c)$ לכל $0 \leq k \leq n$ אזי $f(n) \leq O(n^{c+2})$.

הוכחה: יהא B אלגוריתם לבעייה Q מסבוכיות g.

נתאר אלגוריתם A לבעייה P: יהא $G = (V, E) \quad V = \{v_1, \ldots, v_n\}$

A(G):

$k = 0$

while $B(G, k) =$ False

do $k \leftarrow k + 1$

(* לאחר while זה מתקיים $\tau(G) = k$ *)

i=1

while $B(G - v_1, k - 1) =$ False

do $i \leftarrow i + 1$

(* לאחר while זה מתקיים $\tau(G - v_i) \leq k - 1$ *)

$A(G) = A(G - v_i) \cup \{v_i\}$

נתוח סבוכיות: נניח כי $g(n, k) \leq \alpha n^c$, נראה באנדוקציה כי $f(n) \leq 2\alpha n^{c+2}$.

ואכן מהאלגוריתם נובע כי

$$
\begin{aligned}
f(n) &\leq \sum_{k=0}^{n} g(n, k) + ng(n-1, k-1) + f(n-1) \\
&\leq n \cdot \alpha n^c + n\alpha n^c + 2\alpha(n-1)^{c+2} = 2\alpha(n^{c+1} + (n-1)^{c+1}) \\
&\leq 2\alpha n^{c+2}
\end{aligned}
$$

□

שפות

נסמן ב־ $\{0,1\}^*$ את אוסף המחרוזות הסופיות של אפסים ואחדים.
ל־ $x = (x_1, \ldots, x_n) \in \{0,1\}^*$ נסמן $|x| = n$.
שפה היא תת קבוצה $L \subset \{0,1\}^*$. בעיית ההכרעה הקשורה לשפה L הינה בהנתן $x \in \{0,1\}^*$ האם $x \in L$ או $x \notin L$.
אלגוריתם $A : \{0,1\}^* \to \{0,1\}$ הינו אלגוריתם הכרעה ל־L אם

$$L = \{x \in \{0,1\}^* \;:\; A(x) = 1\}$$

כל בעיות ההכרעה ניתנות לנסוח בעזרת שפות, ע"י קדוד מתאים וסטנדרטי של הקלט הנתון (גרף, רשת וכיו"ב) על וקטור ב־ $\{0,1\}^*$.

המחלקה P

שפה L תקרא פולינומיאלית אם קיים לה אלגוריתם הכרעה A, וקבוע $c > 0$ כך שלכל $x \in \{0,1\}^*$, $A(x)$ מחושב בזמן $O(|x|)^c)$.
אוסף כל השפות הפולינומיאליות יסומן ב־ P.
אנו מכירים דוגמאות רבות לשפות ב־P, למשל:

(i) שפת הגרפים בדו־צדדיים

(ii) שפת הגרפים הדו־צדדיים בעלי זווג מושלם

(iii) שפת הגרפים הממושקלים בעלי עץ פורש שמשקלו ≤ 10

(iv) שפת הגרפים המכילים קליק בגודל ≤ 10

השפות נמצאות ב־P נחשבות ל"טובות" מבחינה חשובית.
ישנן בעיות שידוע שאינן ב־P, למשל האם במשחק דמקה על לוח $n \times n$ יש אסטרטגית נצחון ללבן.

המחלקה NP

יש שפות רבות L שעבורן אם $x \in L$ אזי אורקל יכול להוכיח לנו בזמן פולינומי שאכן $x \in L$. נסמן אוסף שפות זה ע"י NP (Nondeterministic Polynomial).

דוגמאות:

(i) $COVER = \{(G,k) \;:\; \tau(G) \leq k \;,\; k \in \mathbb{N} \;,\text{גרף } G\}$

אם $(G,k) \in COVER$ אזי אורקל יכול לספק לנו קבוצה $S \subset V$ ואנו נבדוק בזמן פולינומי כי $|S| \leq k$ וכי S קבוצה מכסה של G.

(ii) מעגל המילטוני הוא מעגל פשוט העובר דרך כל קדקדי G.

$$HAM = \{G \;:\; \text{גרף המילטוני } G\}$$

אם $G \in HAM$ אזי אורקל לכול לספק לנו סדור של הקדקדים ואנו נוכל לבדוק בזמן לינארי ב־n שהסדור מגדיר מעגל המילטוני.

הגדרה פורמלית של NP

$L \in NP$ אם קיים אלגוריתם $A : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ וקבוע $c > 0$ כך ש־ $A(x,y)$ מחושב בזמן $O\left((|x|+|y|)^c\right)$ וכך ש־

$$L = \{x \in \{0,1\}^* \ : \ \exists y \in \{0,1\}^* \ , \ |y| \leq O(n^c) \ , \ A(x,y) = 1\}$$

<u>טענה</u>: $P \subset NP$
<u>הוכחה</u>: תהא $L \in P$, ויהא $B : \{0,1\}^* \to \{0,1\}$ אלגוריתם הכרעה ל־L כך ש־ $B(x)$ מחושב בזמן $O(|x|^c)$. נגדיר $A : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ ע"י $A(x,y) = B(x)$. אזי $A(x,y)$ מחושב בזמן $O(|x|^c)$ וברור כי

$$L = \{x \ : \ B(x) = 1\} = \{x \ : \ \exists y \ \ A(x,y) = 1 \quad |y| = O(|x|^c)\}$$

$\square$

אנו נשווה בין סיבוכיות של בעיות שונות בעזרת המושג של רדוקציה פולינומיאלית.
<u>הגדרה</u>: נאמר כי השפה L_1 ניתנת לרדוקציה פולינומיאלית לשפה L_2,
ובסימון $L_1 \leq_P L_2$, אם קיים אלגוריתם $f : \{0,1\}^* \to \{0,1\}^*$ וקיים קבוע $c > 0$ כך שמתקיימים התנאים הבאים:

1. $f(x)$ מחושב בזמן $O(|x|^c)$.
2. $f(x) \in L_2 \Leftrightarrow x \in L_1$

<u>דוגמא</u>: מספר הצביעה $\chi(G)$ של גרף G הוא ה־k המינימלי כך שקיימת צביעה $\varphi : V \to [k]$ המקיימת $\{u,v\} \in E \Leftarrow \varphi(u) \neq \varphi(v)$.
עבור i קבוע נסמן ב־ $COL(k)$ את משפחת הגרפים המקיימים $\chi(G) \leq k$. למשל $COL(2)$ היא משפחת הגרפים הדו־צדדיים ולכן $COL(2) \in P$.

<u>טענה</u>: לכל k קבוע, $COL(k) \leq_P COL(k+1)$.
<u>הוכחה</u>: לגרף $G = (V,E)$ נגדיר $f(G) = (V',E')$ כאשר $V' = V \cup \{w\}$ (w קדקד חדש) ו $E' = E \cup \{\{v,w\} \ : \ v \in V\}$.
ברור כי $\chi(f(G)) = 1 + \chi(G)$, ולכן

$$f(G) \in COL(k+1) \Leftrightarrow G \in COL(k)$$

<u>טענה</u>:

(i) אם $L_2 \leq_P L_3$, $L_1 \leq_P L_2$ אזי $L_1 \leq_P L_3$.

(ii) אם $L_1 \leq_P L_2$ ו־ $L_2 \in P$ אזי $L_1 \in P$.

<u>הוכחה</u>: (i) ברור.
(ii) יהא A_2 אלגוריתם הכרעה ל־L_2 כך ש־ $A_2(x)$ מחושב בזמן $O(|x|^{c_2})$. תהא $f : \{0,1\}^* \to \{0,1\}^*$ רדוקציה פולינומיאלית של L_1 ל־L_2 כך ש $f(x)$ מחושבת בזמן $O(|x|^c)$.
אזי $A_1(x) = A_2(f(x))$ הוא אלגוריתם הכרעה ל־L_1, ו־ A_1 מחושב בזמן $O(|x|^{cc_1})$.

$\square$

<u>הגדרה</u>: השפה L נקראת NP־קשה (NP-Hard) אם $L' \leq_P L$ לכל $L' \in NP$.
L נקרא NP־שלמה (NP-Complete או בקיצור NPC) אם $L \in NP$ ו־L היא NP־קשה.

<u>השערה</u>: $P \neq NP$.

<u>הערה חשובה</u>: אם עבור בעיה <u>כלשהיא</u> $L \in NPC$ מתקיים $L \in P$ אזי מהטענה למעלה נובע כי $P = NP$. לכן אם אנו מראים עבור בעייה מסויימת L שהיא ב־NPC אזי, בכפוף להשערה $P \neq NP$, נובע כי אין לה אלגוריתם הכרעה פולינומיאלי.

נוסחא בוליאנית $\phi(x_1, \ldots, x_n)$ נקראית <u>ספיקה</u> אם יש הצבה $x = (x_1, \ldots, x_n) \in (T, F)^n$ כך ש - $\phi(x) = T$.
<u>דוגמא</u>: $(x_7 \vee \neg x_2) \wedge (x_1 \vee x_3)$ ספיקה. $x_1 \wedge \neg x_1$ אינה ספיקה.
נסמן ב־SAT את אוסף הנוסחאות הספיקות.
<u>משפט Cook</u>: $SAT \in NPC$.
בעזרת משפט Cook והטכניקה של רדוקציה פולינומיאלית, ניתן להראות כי בעיות טבעיות רבות נמצאות ב־NPC ולכן, בכפוף להשערה $P \neq NP$, אינן ניתנות להכרעה בזמן פולינומיאלי.
כהדגמה לשיטה זו נראה כי הבעיות הבאות ב־ NPC:

1. נוסחא בוליאנית ϕ היא בconjuctive normal form אם ϕ היא AND של OR־ים באורך שלוש של משתנים או שלילותיהם, למשל

$$\phi = (x_1 \vee \neg x_2 \vee x_4) \wedge (x_3 \vee \neg x_1 \vee x_7)$$

   נסמן ב־ $3CNF$ את אוסף הנוסחאות הנ"ל שהן ספיקות.

2. נסמן ב־ $w(G)$ את גודל הקליק המרבי בגרף G.
   נסמן ב־ $CLIQUE$ את אוסף הזוגות (G, k) כך ש־ $w(G) \geq k$.
3. נסמן ב־ $COVER$ את אוסף הזוגות (G, k) כך ש - $\tau(G) \leq k$.
4. נסמן ב־ $DHAM$ את אוסף הגרפים המכוונים G בעלי מעגל המילטוני מכוון.

קל לבדוק כי $3CNF,\ CLIQUE,\ COVER,\ HAM,\ DHAM,\ COL(3) \in NP$

<u>טענה</u>: $SAT \leq_P 3CNF \leq_P CLIQUE \leq_P COVER \leq_P DHAM$

$$3CNF \leq_P COL(3)$$

<u>מסקנה</u>: כל הבעיות המופיעות בטענה הקודמת הן ב־ NPC.