1. נראה אלגוריתם split(A, n, k) המקבל כקלט את A ומוציא

כפלט את $B_1,\dots,B_k$ כך שלכל $i<j$! $x\in B_i, y\in B_j$ מתקיים

$x<y$, B_i כולל , $|B_i|=n$! $\bigcup_{i=1}^{k} B_i = A$.

Split (A, n, k)

if $k=1$, $B_1 \leftarrow A$, Stop.

else $s \leftarrow \lceil \frac{k}{2} \rceil n$ - smallest element of A

compute $A_1 \leftarrow \{x\in A : x\le s\}$, $A_2 \leftarrow \{x\in A : x>s\}$

$\{B_1,\dots,B_{\lfloor \frac{k}{2}\rfloor}\} \leftarrow$ split $(A_1, n, \lfloor \frac{k}{2}\rfloor)$, $\{B_{\lfloor \frac{k}{2}\rfloor+1},\dots,B_k\} \leftarrow$ split$(A_2, n, \lceil \frac{k}{2}\rceil)$.

נסמן סיבוכיות של split(A, n, k) ב- $f(n,k)$, וסיבוכיות של בחירת ע"י $g(n)\le c_0 n$

אזי

$$f(n,k) \le c_0 n + n + f(n,\lfloor \tfrac{k}{2}\rfloor) + f(n,\lceil \tfrac{k}{2}\rceil) = (c_0+1)n + f(n,\lfloor \tfrac{k}{2}\rfloor) + f(n,\lceil \tfrac{k}{2}\rceil)$$

טענה: אם $k=2^t$ אזי $f(n,k)\le c n k \log_2 k$ כאשר $c=\frac{c_0+1}{2}$

הוכחה: אינדוקציה על t. $t=0$ ברור.

$$f(n,2^t) \le (c_0+1)kn + 2f(n,\tfrac{k}{2}) \le (c_0+1)kn + 2cn\tfrac{k}{2}\log_2\tfrac{k}{2} = cnk\log_2 k$$

לגבי k כללי, אם $2^{t-1}<k\le 2^t$ אזי

$$f(n,k) \le f(n,2^t) \le cn2^t\cdot t \le cn\cdot(2k)\cdot(\log_2 k+1) \le O(nk\log_2 k)$$

ב. מספר האפשרויות לחלוקת kn איברים ל-k קבוצות בגודל n איברים הוא $\binom{kn}{n,\dots,n}$ לכן סיבוכיות של הבע"ח

ב-אל. לפחות

$$\log_2\binom{kn}{n,\dots,n} = \log_2\frac{(kn)!}{(n!)^k} = \log_2(kn)! - k\log_2 n! = \Omega(nk\log_2 k)$$

2. א. ערך הצרימה המקסימלית = קבוע המתקן המינימלי. מאחר וכל

צלע היא בעלת קבוע 5 או 7 הרי שקבוע כל מתקן

הוא מהצורה $5a+7b$ כאשר $a,b\geq 0$ שלמים. אבל 23

אינו מהצורה הנ"ל, ולכן ערך הצרימה המקסימלית אינו 23.

ב. יהיו $\{e_1,\dots,e_{n-1}\}$ ו- $\{f_1,\dots,f_{n-1}\}$ שני עצים פורשים מינימליים

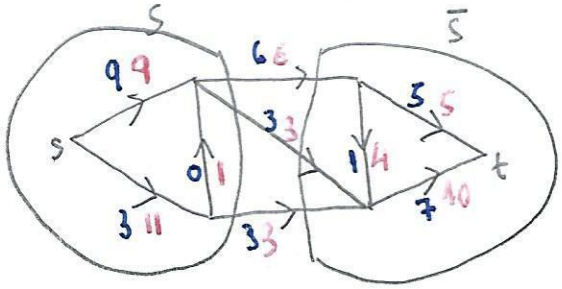
ערוכים, כך: $w(e_1)\leq\dots\leq w(e_{n-1})$ ו- $w(f_1)\leq\dots\leq w(f_{n-1})$.

ראינו כי $w(e_i)=w(f_i)$ לכל $1\leq i\leq n-1$, ובפרט $w(e_1)=w(f_1)$, $w(e_2)=w(f_2)$.

כמו כן $\{e_1,e_2\}$ הוא יער מינימלי בן שתי צלעות. אבל $\{f_1,f_2\}$ גם

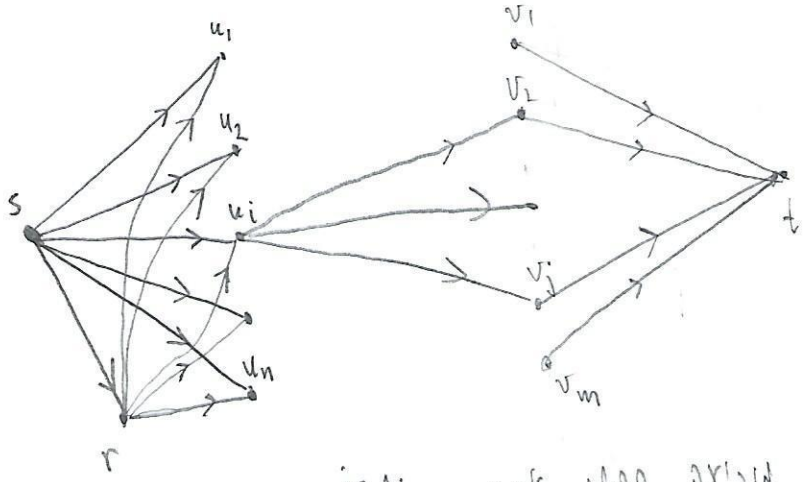
הוא יער בן שתי צלעות ולכן $w(f_1)=w(e_1)$ ולכן $w(e_1)=w(e_2)=w(f_1)=w(f_2)$.

3. א.



$\max val(f) = 12 = cap(S,\bar{S})$

ב. בהנ"ל $\bigcup_{i=1}^{n} A_i = \{1,\dots,m\}$. נגדיר רשת:



הצלע u_iv_j מופיעה ברשת אם $j\in A_i$.

הקבועים נתונים ע"י: $c(u_iv_j)=1$ אם הצלע u_iv_j נמצאת ברשת

$c(r,u_i)=l_i-k_i$, $c(s,u_i)=k_i$, $c(s,r)=m-\sum_{i=1}^{n}k_i$, $c(v_j,t)=1$.

3.ג. (המשך). מראים שקיימת $\{B_i\}_{i=1}^{n}$ מתת־קבוצות $B_i \subseteq A_i$ $k_i \le |B_i| \le k_i$

! $\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} B_i$, אפס קיימת מלמעלה קבוצה שמרכבת m.

4.א. $561 = 3 \cdot 11 \cdot 17$

ב. $\varphi(561) = 2 \cdot 10 \cdot 16 = 320$,

$183^{-1} \pmod{320} = 7$

ולכן $D(y) = y^7$ היא פו' הפענוח.

ג. $x^2 \equiv 1 \pmod{561}$ אם

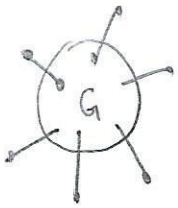
$$(*) \quad \begin{cases} x \equiv \pm 1 \pmod 3 \\ x \equiv \pm 1 \pmod{11} \\ x \equiv \pm 1 \pmod{17} \end{cases}$$

כל בחירה של ± 1 יכולה נותנת פתרון שונה, ולפיכך יש $2^3 = 8$ פתרונות.

פתרון $(*)$ בעזרת משפט השאריות הסיני נותן שקבוצת הפתרונות של $x^2 \equiv 1 \ (561)$

היא $\{1, 67, 188, 254, 307, 373, 494, 560 = -1\}$

5. א. ההתאמה

$f(G) =$ 

הינה רדוקציה פולינומיאלית של L_1 ל- L_2, לכן $L_1 \le_p L_2$.

ב. $L_1 \le_p L_2$ ו- $L_2 \in NP$, $L_1 \in NPC$ $\Leftarrow$ $L_2 \in NPC$.

ההתאמה

$h(G) = G \underbrace{\cdots}_{m \text{ נק' מבודדות}}$

כאשר $m = 4|V|$ $V =$ קדקדי G, הינה רדוקציה

פולינומיאלית של L_2 ל- L_3. לכן $L_2 \le_p L_3$

מאחר! - $L_3 \in NP$ ו- $L_2 \in NPC$ נובע כי $L_3 \in NPC$.