1. א. נתאר אלגוריתם רקורסיבי למיון x: תחילה נחשב את החציון w של $\{x_i\}_{i=1}^{N}$ ב- CN השוואות. ע"י N השוואות נוספות נחשב את

$$A_1 = \{x_i : x_i < w\} \qquad A_2 = \{x_i : x_i > w\}$$

אזי $|A_i| = N_i = k_i l$ כאשר $N_i \le \frac{N}{2}$ ו- $k_i \le \frac{k}{2}$.

נמיין עתה ברקורסיה את A_1 ו- A_2.

נסמן ב- $f(N,k)$ את מס' ההשוואות המירבי שיבצע האלגוריתם.

<u>טענה:</u> $f(N,k) \le (C+1) N \log_2 k$

<u>הוכחה:</u> באינדוקציה על k. ב- $k=1$ ברור כי $f(N,1)=0$.

יהא $k>1$, אזי

$$f(N,k) \le CN + N + f(N_1,k_1) + f(N_2,k_2) \le (C+1)N + (C+1)N_1 \log_2 k_1 + (C+1) N_2 \log_2 k_2 \le$$

$$\le (C+1)N + (C+1)N \log_2\left(\frac{k}{2}\right) = (C+1) N \log_2 k$$

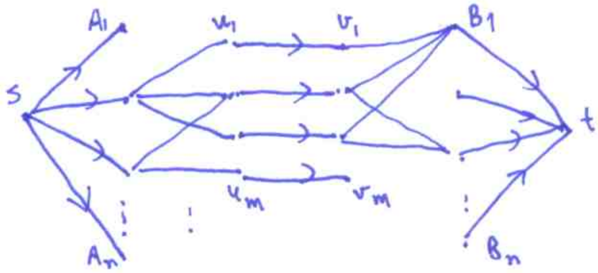
ב. מס' התמורות המתקבלות כפלט של אלגוריתם הממ"ין x כנ"ל הוא לפחות כמספר החלוקות בסדורות $[N] = A_1 \cup \dots \cup A_k$ כאשר $|A_i| = l$, כלומר $\binom{N}{l,\dots,l}$. לכן מס' ההשוואות על קלט מסוים יהיה לפחות:

$$\log_2 \binom{N}{l,\dots,l} = \log_2 \frac{N!}{(l!)^k} = \log_2 \frac{N!}{\left(\left(\frac{N}{k}\right)!\right)^k} \ge$$

$$N \log_2 k \,(1-o(1)).$$

2. ב. בה"ג כלליות $\bigcup_{i=1}^{n} A_i \cup \bigcup_{i=1}^{n} B_i = \{1,\dots,m\}$.

נעיין בגרף המכוון (הבא):



עם הצלעות:

(s,A_i) : $1\le i\le n$

(B_j,t) : $1\le j\le n$

(u_i,v_i) : $1\le i\le m$

אם $j\in A_i$ (A_i,u_j) כשכל הקיבולים $\equiv 1$.

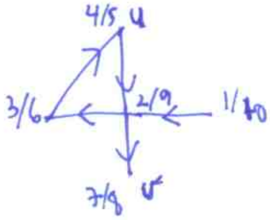
אם $i\in B_j$ (v_i,B_j)

אזי קיימת תמורה $\sigma\in S_n$ ואיברים שונים $x_1,\dots,x_n$ כך ש- $x_i\in A_i\cap B_{\sigma(i)}$, אם"ם קיימת זרימה ברשת שערכה הוא n.

3. א. אם $v\to u$ ב-G אזי $f(u)>d(v)$ ולכן אם $d(u)<d(v)$ אזי $d(u)<d(v)<f(u)$ ולכן v צאצא של u ב-T.

הצלע vu אינה בהכרח ב-T:

ב. לא. דוגמא:



ג. $f(u_2)<f(u_1)$. אחרת $f(u_1)<f(u_2)$ ומכיוון ש- $f(u_1)>d(u_2)$

הרי ש- $d(u_2)<f(u_1)<f(u_1)<f(u_2)$ ואזי

u_1 צאצא של u_2 ובפרט יש מסלול מכוון מ-u_2 ל-u_1 בסתירה

להנחת האציקליות. לכן $f(u_2)<f(u_1)$ ובדומה

$f(u_3)<f(u_2)$ ולכן $f(u_1)>f(u_3)$.

4. ג. $N=231=3\cdot7\cdot11 \Rightarrow \varphi(N)=2\cdot6\cdot10=120$.

$13\in Z^*_{120}$ לכן קיים d כך ש- $13d=1+120\lambda$ ואז לכל $x\in Z^*_N$

$$D(E(x))\equiv_N D(x^{13})\equiv_N x^{13d}=x^{1+120\lambda}=x\cdot x^{\varphi(N)\cdot 120}\equiv_N x$$

בנוסף E חח"ע ועל. נחשב d:

a	b	$\lfloor \frac{b}{a} \rfloor$	x	y
13	120	9	37	-4
3	13	4	-4	1
1	3	3	1	0
0	1	-	0	1

$\Rightarrow$ $1=37\cdot13-4\cdot120$

לכן $d=37$.

5. ב. לגרף $G=(V,E)$ נגדיר גרף $G'=(V\cup V_0,E')$ כאשר $|V_0|=2|E|$, $|E'|=2E$, כך ש- G' הוא איחוד זר של G עם $|E|$ צלעות בודדות:

$G=$  $\longrightarrow$ $G'=$ 

נגדיר רדוקציה מ- L_1 ל- L_2 ע"י $f((G,k))=(G',k)$.

<u>טענה:</u> $(G,k)\in L_1 \iff (G',k)\in L_2$.

<u>הוכחה:</u> $(G,k)\in L_1 \Rightarrow$ קיימת $S\subset V$ המכסה את כל צלעות G, $|S|\le k$.

ברור כי S מכסה בדיוק מחצית מצלעות G', לכן $(G',k)\in L_2$.

להיפך, נניח $(G',k)\in L_2$. אזי קיימת $S\subset V'$ המכסה לפחות מחצית מצלעות G'.

נסמן $T=S\cap V$, $T_0=S\cap V_0$. T_0 מכסה $\le|T_0|$ מהצלעות הנוספות,

לכן T מכסה לפחות $|E|-|T_0|$ מהצלעות של G. ע"י הוספת $|T_0|$ קודקודים ל- T נקבל קבוצה המכסה כל צלע של G. לכן $\tau(G)\le|T|+|T_0|=|S|\le k$.

6. ב. $\Rightarrow L_2\in NPC$. מאידך $L_3\in P$ כי מס' הקבוצות בגודל $|V|-10$ הינו $\binom{|V|}{|V|-10}=\binom{|V|}{10}\le|V|^{10}$ הוא פולינומי ב- $|V|$.