Definice 1 (PRAS, FPRAS)**.** *Polynomiální randomizované aproximační schéma* (PRAS) pro problém P je randomizovaný algoritmus $\mathcal{A}$, který na vstupu x a $\varepsilon > 0$ běží v čase $|x|^{\mathcal{O}(1)}$ a vydá hodnotu $\mathcal{A}(x)$ splňující $\Pr\left[(1-\varepsilon)\#x \leq \mathcal{A}(x) \leq (1+\varepsilon)\#x\right] \geq \frac{3}{4}$. FPRAS je PRAS, který běží v čase polynomiálním v $|x|$ i $1/\varepsilon$.

Věta 1 (Estimator Theorem)**.** Polož $\rho = |G|/|U|$. Existuje Monte Carlo metoda, která dává ε-aproximaci $|G|$ s pravděpodobností aspoň $1-\delta$, pokud $N \geq \frac{4}{\varepsilon^2 \rho} \ln \frac{2}{\delta}$, kde N je počet nezávislých náhodných vzorků z univerza U.

Značení:

- $G = (U \cup V, E)$ je bipartitní graf, $|U| = |V| = n$
- m_k značí počet párování velikosti k v grafu G (*k-párování*)
- pro hranu $e \in E$ označme m_e počet k-párování obsahujících hranu e a m_{ne} počet k-párování neobsahujících hranu e
- $r_k = m_k/m_{k-1}$

Procházka po kostrách – $\mathcal{M}$: Začneme v libovolné kostře X grafu G.

1. Vyber uniformně náhodně hrany e, f.
2. Pokud $X - e + f$ je kostra, posuň se do ní s pstí $1/2$ a jinak zůstaň v X.

Příklady

1. (minule) Buď $G = (U \cup V, E)$ je bipartitní graf, $|U| = |V| = n$ s $\delta(G) > n/2$. Ukažte, že $r_k \leq n^2$.
2. (minule) Buď $G = (U \cup V, E)$ je bipartitní graf, $|U| = |V| = n$ s $\delta(G) > n/2$. Ukažte, že pro libovolné párování m velikosti nanejvýš $n-1$ existuje zlepšující cesta délky nanejvýš 3.
3. (minule) Buď $G = (U \cup V, E)$ je bipartitní graf, $|U| = |V| = n$ s $\delta(G) > n/2$. Ukažte, že pro libovolné $2 \leq k \leq n$ a párování m velikosti k existuje nanejvýš n^2 párování velikosti $k-1$ takových, že pro každé z nich je možné nalézt zlepšující cestu délky nanejvýš 3, která je zlepší na m.
4. Buď $G = (U \cup V, E)$ je bipartitní graf, $|U| = |V| = n$ s $\delta(G) > n/2$. Ukažte, že $1/n^2 \leq r_k \leq n^2$. (Použijte předchozí 3 cvičení.)
5. Graf G_k vznikne z grafu $G = (U \cup V, E)$ tak, že přidáme $n-k$ vrcholů do každé partity a spojíme každý nový vrchol se všemi starými vrcholy v opačné partitě.

   Ukažte, že pro R podíl perfektních a skoroperfektních párování v G_k platí

   $$R = \frac{m_k}{m_{k+1} + 2(n-k)m_k + (n-k+1)^2 m_{k-1}}.$$

6. Ukažte, že $\mathcal{M}$
   - je ireducibilní a aperiodický,
   - pokud pro kostry X, Y platí $P(X,Y) > 0$, potom $P(X,Y) = \frac{1}{2m(n-1)}$ a
   - je reverzibilní.

   Dále ukažte, že jeho stacionární distribuce dává uniformní distribuci na kostrách grafu G. Délka nejkratší cesty z libovolné kostry X do libovolné kostry Y je polovina jejich symetrické diference.

7. Ukažte, že rozhodování zda permanent matice $M \in \{0,1\}^{n\times n}$ má hodnotu $k \in \mathbb{N}$ je v IP.

Definice 2 (Interaktivní protokoly)**.** Mějme dva hráče – verifier V a prover P. Verifier V běží v polynomiálním čase (ve velikosti vstupního slova w) a může používat náhodné bity. Jazyk L je v IP, pokut existují V a P, že pro každého Q a slovo w platí

Completeness pokud $w \in L$, potom $\Pr[V$ přijme důkaz od $P] \geq 2/3$ a

Soundness pokud $x \notin L$, potom $\Pr[V$ přijme důkaz od $Q] \leq 1/3$.

Jak na to? Označme $M^{1,i}$ matici M bez prvního řádku a i-tého sloupce. Označme $D(x)$ matici $(n-1)\times(n-1)$, kde prvky jsou polynomy stupně n, takovou že $\forall i \in [n]\colon D(i) = A_{1,i}$. Permanent $\operatorname{perm}(D(x))$ je polynom stupně $n(n-1)$ v x.

Věta 2. Všimněte si, že

- $\operatorname{perm}(M) = \sum_{i=1}^{n} M_{1,i} \operatorname{perm}\big(M^{1,i}\big)$
- $\operatorname{perm}(M) \leq n! \leq 2^{n^2}$.

Protokol:

- Pokud $n \leq 2$ zkontrolujte a vydejte odpověď.
- Nechte si od P poslat prvočíslo $2^{n^2} < p < 2^{2n^2}$ a ověřte, že se opravdu jedná o prvočíslo.
- Pro $n > 1$ si řekněte P o polynom $g \in \mathcal{F}_p[x]$ (stupně nanejvýš n^2) takový, že $g(x) = \operatorname{perm}(D(x))$. Poté zkontrolujte, že $k = \sum_{i=1}^{n} M_{1,i} \operatorname{perm}(D(i))$.
- Dále rekurzivně zkontrolujte že $\operatorname{perm}(D(a)) = g(a)$ pro náhodné $a \in \mathcal{F}_p$.

Věta 3. Ukažte, že pokud $g(x) \neq \operatorname{perm}(D(x))$, potom $\Pr_a[g(a) = \operatorname{perm}(D(a))] \leq n^2/p$.

Bonus: Ukažte, že pokud V pro rozhodování jazyka L nepoužívá náhodné bity, pak L je v NP.