Exercise-Solution

Xu Xiaoquan, Jilin University

xuxq2119@mails.jlu.edu.cn

Problem 1

Observation 1: If $|V(G)| \geq k(d+1)$, G has an independent set of size *k*.

Proof. After selecting any vertex *u* into the independent set I, at most *d* adjacent vertices are forbidden to be selected. Since $|V(G)| \geq k(d+1)$, we are able to achieve $|I| \geq k$ by repeating the above process *k* times.

Algorithm 1: Boolean Check(G,*k*)

(1) If $|V(G)| \geq k(d+1)$ then return TRUE.

(2) If $|V(G)| < k$ then return FALSE.

(3) Choose an arbitrary vertex u in G.

(4) If Check($G \setminus \Gamma^{+}(u)$,$k-1$) return TRUE.

(5) If Check($G \setminus \{u\}$,k) return TRUE.

(6) return FALSE.

Analyzing: The number of the vertices is smaller than $k(d+1)$ at the beginning. Each time it decreases by at least one and branches to two. Thus, the number of total running steps is $\Omega(2^{k(d+1)} \cdot |G|)$. In fact, it is unlikely to reach the bottom of the search tree because of the Step (1) and (2). Besides, Step (4) will probably decreace the vertices more than one.

Problem 2

Before the problem was modified, I had spent a long time designing the following linear time algorithm. If there are any mistakes, would you mind giving me some corrections by email?

Observation 2: Let a,b,c be three vertices in G. Let E' be the edges of G', which is the disjoint union of cliques. The following conditions will not be met at the same time:

$$ab \in E',\ bc \in E',\ ac \notin E'$$

Proof. If $ab \in E'$ and $bc \in E'$, {*a,b,c*} must be in the same clique, which indicates that $ac \in E'$.

Algorithm 2: Boolean Check(G,*k*)

(1) If $|E(G)| <= 1$ return TRUE.

(2) Breadth-First Search(G) from an arbitary vertex *u*. Let R be the set of all the reachable vertices(including *u*). Let dis(*v*) be the shortest disatance from *u* to any vertex *v* in R.

(3) If $\forall v \in R$ s.t. $degree(v) = |R| - 1$, R forms an isolate clique in G'.return Check(G\R,*k*).

(4) If *k*=0 return FALSE.

(5) If $\exists v \in R$ s.t. $dis(v) = 2$, $\exists w \in R$ s.t. $uw, wv \in E$ but $uv \notin E$. Let *a*=*u*, *b*=*w*, *c*=*v*.

(6) Else $\exists v$ s.t. $dis(v)=1$ and $degree(v) \neq |R|-1$. Then we can find a $w \in R$ s.t. $wv \notin E$ but $uw, uv \in E$. Let *a*=*v*, *b*=*u*, *c*=*w*.

//Now (a,b,c) satisfies all the three conditions, which means we must edit one edge to break it.

(7) If Check($G \setminus \{ab\}, k-1$) return TRUE.

(8) If Check($G \setminus \{bc\}, k-1$) return TRUE.

(9) If Check($G \cup \{ac\}, k-1$) return TRUE.

(10) return FALSE.

Analyzing: We have *k* chances of edition at the beginning. Each time it decreases by one and branches to three. The time complexity of each step is linear about |G| because of the traversal. Thus, the number of total running step is $\Omega(3^k \cdot |G|)$

Problem 3

Algorithm 3: Boolean Check(H,k)

(1) If $|E| \leq k$ return TRUE.

(2) If *k*=0 return FALSE.

(3) Choose an arbitrary edge *e* in E.

(4) For each vertex *u* in *e*:

(5) If Check($H \setminus \{u\}, k-1$) return TRUE.

(6) return FALSE.

Analyzing: We have *k* chances of selecting at the beginning. Each time it decreases by one and branches to at most *d*. Thus, the number of total running steps is $\Omega(d^k \cdot |G|)$, which is of the linear rate with respect to |G|.

Problem 4

$$|codeg(a,b) - q/4| = |\sum_{x \in \mathbb{F}_q \setminus \{-a,-b\}} \frac{1}{4}(\chi(x+a)+1)(\chi(x+b)+1) - \frac{q}{4}|$$

$$\leq \frac{1}{4}|\sum_{x \in \mathbb{F}_q}[1+\chi(x+a)+\chi(x+b)+\chi(x+a)(x+b)] - q|$$

$$+\frac{1}{4}|\chi(-a+b)+1| + \frac{1}{4}|\chi(-b+a)+1|$$

$$\leq \frac{1}{4}|\sum_{x \in \mathbb{F}_q}\chi(x+a)| + \frac{1}{4}|\sum_{x \in \mathbb{F}_q}\chi(x+b)| + \frac{1}{4}|\sum_{x \in \mathbb{F}_q}\chi((x+a)(x+b))| + \frac{2}{4} + \frac{2}{4}$$

$$\leq \frac{1}{4}(1-1)\sqrt{q} + \frac{1}{4}(1-1)\sqrt{q} + \frac{1}{4}(2-1)\sqrt{q} + 1$$

$$\leq O(\sqrt{q})$$

Problem 5

Uniformly and independently select a vertex s_i from each V_i.

Bad event $A_{i,j}$ for $1 \le i < j \le r$: $s_i s_j \notin E$.

$$Pr[A_{i,j}] \le 1 - \frac{\rho |V_i||V_j|}{|V_i||V_j|} = 1 - \rho$$

For convenience, $A_{j,i}$ below is a same event as $A_{i,j}$.

(1) General Lovasz local lemma:

$d \triangleq \max[\Gamma(A_{i,j})] = 2(r-2)$.

$\mathrm{e}p(d+1) \le 1 \Leftrightarrow \mathrm{e}(1-\rho)(2r-3) \le 1 \Leftrightarrow \rho \ge 1 - \frac{1}{\mathrm{e}(2r-3)}$

(2) Cluster expansion lemma:

$\Gamma^+(A_{i,j}) = \{A_{k,j} \mid k \in [r] \setminus \{i,j\}\} \cup \{A_{i,k} \mid k \in [r] \setminus \{i,j\}\} \cup \{A_{i,j}\}$.

According to symmetry, let $\mu = \mu_{A_{i,j}}, \forall 1 \le i < j \le r$.

In the following, we consider the three cases of the size of I:

1.$|I| = 0$: $\prod_{B \in I} \mu_B = 1,\ I = \emptyset$. :1 ways

2.$|I| = 1$: $\prod_{B \in I} \mu_B = \mu,\ I = \{A_{p,q}\}\ (p \in \{i,j\} \text{ or } q \in \{i,j\} \text{ but } p \ne q)$. :(2$r$-3) ways

3.$|I| = 2$: $\prod_{B \in I} \mu_B = \mu^2,\ I = \{A_{p,j}, A_{i,q}\}\ (p,q \in [r] \setminus \{i,j\} \text{ but } p \ne q)$. :($r$-2)($r$-3) ways

Thus, $\frac{\mu_A}{\sum_{indep. I \subseteq \Gamma^+(A)} \prod_{B \in I} \mu_B} = \frac{\mu}{1 \cdot 1 + (2r-3) \cdot \mu + (r-2)(r-3) \cdot \mu^2}$

$$= \frac{1}{\frac{1}{\mu} + (2r-3) + (r-2)(r-3)\mu} \le \frac{1}{(2r-3) + 2\sqrt{(r-2)(r-3)}}$$

The equality holds when $\mu = \frac{1}{\sqrt{(r-2)(r-3)}}$.

$$1 - \rho \le \frac{\mu_A}{\sum_{indep. I \subseteq \Gamma^+(A)} \prod_{B \in I} \mu_B} \Leftrightarrow \rho \ge 1 - \frac{1}{(2r-3) + 2\sqrt{(r-2)(r-3)}}$$

(3) Shearer's lemma:

We can observe that the dependency graph is exactly $L(K_r)$. Therefore :

$$\vec{p} \in \mathcal{S} \Leftrightarrow 1 - \rho = p < \frac{1}{4(r-2)} \Leftrightarrow \rho > 1 - \frac{1}{4(r-2)}$$

The above conditions are strictly tighter one by one.

Problem 6

(1) Suppose a randomized algorithm only needs $g\left(\frac{N}{t}\right) < \Theta\left(\frac{N}{t}\right)$ queries.

Let $g(x)f(x) = \Theta(x)$. When $x = \frac{N}{t} \to \infty$, $f(x) \to \infty$.

But the probability of failure $Pr[fail] = (1 - \frac{1}{x})^{g(x)} = \left(\left(1 - \frac{1}{x}\right)^x\right)^{\Theta\left(\frac{1}{f(x)}\right)}$

$\to \exp\left(\Theta\left(\frac{1}{f(x)}\right)\right) \to 1$, which leads to a contradiction.

(2) If $t = N/4$, then $\theta = \arcsin\sqrt{t/N} = \pi/6$.

The probability of seeing a solution after the first time $p_1 = (\sin(3\theta))^2 = (\sin(\pi/2))^2 = 1$.

Thus, the Grover's algorithm always finds a solution with certainty after just one query.

Problem 7

(1) Since I, X, Y, Z are linear independent, and all the 2×2 matrices forms a 4-dimensional linear space, I, X, Y, Z are a basis of space. Then any 2×2 matrix can be written as a linear combination of I, X, Y, Z.

(2) $\rho = c_0 I + c_1 X + c_2 Y + c_3 Z = \begin{pmatrix} c_0 + c_3 & c_1 - ic_2 \\ c_1 + ic_2 & c_0 - c_3 \end{pmatrix}$

$Tr(\rho) = 2c_0 = 1 \quad \Rightarrow \quad c_0 = \frac{1}{2}$

$\rho^\dagger = \rho \Rightarrow \bar{c}_0 I + \bar{c}_1 X + \bar{c}_2 Y + \bar{c}_3 Z = c_0 I + c_1 X + c_2 Y + c_3 Z \quad \Rightarrow \bar{c}_i = c_i \Rightarrow c_i \in \mathbb{R}$

$|\rho - \lambda I| = \begin{vmatrix} c_0 + c_3 & c_1 - ic_2 - \lambda \\ c_1 + ic_2 - \lambda & c_0 - c_3 \end{vmatrix} = \lambda^2 - 2c_0\lambda + c_0^2 - (c_1^2 + c_2^2 + c_3^2) = 0$

All the eigenvalues of ρ are non-nagetive $\Rightarrow \frac{1}{2}(2c_0 \pm \sqrt{4c_0^2 - 4[c_0^2 - (c_1^2 + c_2^2 + c_3^2)]}) \geq 0$

$\Rightarrow c_1^2 + c_2^2 + c_3^2 \leq c_0^2 = \frac{1}{4}$

The equality holds if and only if the eigenvalues of ρ are $\{0,1\}$, therefore ρ is a rank-one matrix. Conversely, if ρ is a rank-one matrix, 0 must be its eigenvalue. Since $\lambda_1 + \lambda_2 = 2c_0 = 1$, another eigenvalue of ρ must be 1.