Exercise of Chapter 7

Xiaoyu Chen

1 Exercise 7.6

Provide a formal statement of Fact 1.5 using the notion of witness-checking predicates.

1.1 Solution

First we provide a formal version for Fact 1.5.

Fact 7.5 (Formal Statement)**.** *Suppose we have a witness-checking predicate* $\chi : \Sigma^* \times \Sigma^* \to \{0, 1\}$*, from which we could define two problem* φ *and* f *such that* $\forall x \in \Sigma^*$*,*

$$\varphi(x) \Leftrightarrow \exists \omega \in \Sigma^*.\chi(x, \omega) \wedge |\omega| \leq P(|x|)$$
$$f(x) = |\omega \in \Sigma^* : \chi(x, \omega) \wedge |w| \leq P(|x|)|$$

Then f *does not admit a* $FPRAS$ *unless* $PR = NP$*.*

Though the problem itself does not require a proof of this fact, I give one here for a better understanding.

Proof. If f has a $FPRAS$, then we have a function S such that,

$$\Pr[e^{-\varepsilon} f(x) \leq S(x) \leq e^{\varepsilon} f(x)] \geq \frac{3}{4}$$

which could be calculated in polynomial time. So we could define a witness-checking predicate χ' for φ as

$$X'(x, \omega) := [S(x) > 0]$$

Then we have:

1. If $\varphi(x)$, then $f(x) > 0$, then $e^{-\varepsilon} > 0$ and $e^{\varepsilon} > 0$. Thus, $\Pr[S(x) > 0] \geq \Pr[e^{-\varepsilon} f(x) \leq S(x) \leq e^{\varepsilon}] \geq \frac{3}{4}$.
2. If $\neg\varphi(x)$, then $f(x) = 0$, then $e^{-\varepsilon} = e^{\varepsilon} = 0$. Thus, $\Pr[S(x) = 0] \geq \frac{3}{4}$ and hence $\Pr[S(x) > 0] \leq \frac{1}{4}$.

So, φ is in BPP.

Then, to go further, we want φ to be some practical NPC problem, i.e. SAT problem. (I get this idea from a online material). Suppose we have a SAT problem ϕ which has k variables $x_1, x_2, \cdots, x_k$. To make things more easy, we could construct another witness-checking predicate χ'' from χ' by calling χ' polynomial times, such that

1. If $\varphi(\phi)$, then $\Pr[\chi''(\phi, \omega)] \geq 1 - 2^{-m}$
2. If $\neg\varphi(\phi)$, then $\Pr[\chi''(\phi, \omega)] \leq 2^{-m}$.

We try to construct a witness-checking predicate χ^* for SAT problem.

```
witness-checking predicate X*(φ, ω) begin
    if ¬χ''(φ, ω) then
        return false
    end
    for i in [1, n] do
        x_i ← 0
        Get a new problem φ_1 by fix variables from x_1 to x_i
        if ¬χ''(φ_1, ω_1) then
            /* Here ω_1 is some random solution for φ_1          */
            x_i ← 1 // also modify x_i in φ_1
        end
    end
    ω_1 ← {x_1, x_2, ··· , x_n}
    return χ(φ, ω_1)
end
```

When $\neg\varphi(\phi)$, if $\neg\chi''(\phi, \omega)$, $\chi^*(\phi, \omega)$ returns *false*. If $\chi''(\phi, \omega)$, then χ^* will construct a solution ω_1 by using χ'' polynomial times. And if $\neg\chi(\phi, \omega_1)$, then χ^* will return *false*. So, these ensures that $\neg\varphi(\phi) \Rightarrow \neg\chi^*(\phi, \omega)$ for all ω.

When $\varphi(\phi)$, consider the probablity for $\chi^*(\phi, \omega)$. We only need to analysis the worst case for this, i.e. when there is only one ω such that $\chi(\phi, \omega)$. To achieve $\chi^*(\phi, \omega)$, we need to avoid wrong choice made by χ''. Note that we have $k + 1$ choices made by χ'' and each of them have probability at less than 2^{-m} to be wrong. So, in this case,

$$\Pr[\chi^*(\phi, \omega)] \geq (1 - 2^{-m})^{k+1} \geq \frac{1}{2}$$

for some appropriate m.

So, its clear that χ^* reaches the requirement of RP and we have φ is in RP, which implies that $NP \subseteq RP$. Together with $RP \subseteq NP$, we have $RP = NP$. $\square$

2 Exercise 7.10

Complete the proof of Theorem 7.9. To keep technical complexity to a minimum, assume the graph G is triangle-free, i.e., contains no cycles of length 3.

2.1 Solution

Suppose there are two states $x, y \in \Omega$, the distance $d(x, y)$ between them is defined as the hamming distance between them. Then, to use the path-coupling method, we need to design the coupling. The coupling is defined between the pairs (X_0, Y_0), where $d(X_0, Y_0) = 1$. Since $d(X_0, Y_0) = 1$, we could assume that there exists a vertex v where $X_0(v) = 0$ and $Y_0(v) = 1$ without loss of generality.

```
/* Update the status of two vertices                                */
Update(X, u, w, a, b) begin
    X_1 ← X, where X_1(u) = a and X_1(v) = b
    if X_1 is a independent set then
        return X_1
    end
    return X
end
/* define the coupling for d(X_0, Y_0) = 1                          */
Coupling(X_0, Y_0) begin
    Choose an edge {u, w} ∈ E, u.a.r.
    /* general cases for selecting (a, b)                           */
    Select (a, b) from {(0, 0), (0, 1), (1, 0)}, u.a.r.
    /* If v ∈ {u, w}, then we only select (a, b) from the
       feasible combinations                                        */
    if u = v ∨ w = v then
        /* assume u = v, without loss of generality                 */
        if X_0(ℕ(w) \ {u}) = 1 then
            Select (a, b) from {(0, 0), (1, 0)}, u.a.r.
        end
    end
    Update(X_1, u, w, a, b), Update(Y_1, u, w, a, b)
    return (X_1, Y_1)
end
```

After that, we are going to analysis the value of $\mathbb{E}[d(X_1, Y_1)]$. Denote the neighbor of v by $\mathbb{N}(v)$, and $\mathbb{N}[v] := \{v\} \cup \mathbb{N}(v)$. Then, any edge $\{u, w\}$ of G must belongs to one of the following three classes.

1. $u \notin \mathbb{N}[v] \wedge w \notin \mathbb{N}[v]$, i.e., v is not the neighbor of edge $\{u, w\}$.
2. $u \in \mathbb{N}(v) \wedge w \notin \mathbb{N}[v]$, i.e., v is a neighbor of edge $\{u, w\}$.
3. $u = v \wedge w \in \mathbb{N}(v)$, i.e., v is an end point of edge $\{u, w\}$.

Since G is triangle-free, we do not need to consider the case $u \in \mathbb{N}(v) \wedge w \in \mathbb{N}(v)$.

For the first case: Note that X_1 and Y_1 will satisfies the requirement for a independent set simutaneously, because the status of all the neighbors of edge $\{u, w\}$ are the same in X_0 and Y_0. So in this case

$$d(X_1, Y_1) = d(X_0, Y_0)$$

For the second case: Recall that $X_0(v) = 0$ and $Y_0(v) = 1$. Intuitively, we have the following circumstance

$$v \longrightarrow u \longrightarrow w \longrightarrow \mathbb{N}(w) \setminus \{u\}$$

Since $X_0(\mathbb{N}(w) \setminus \{u\}) = Y_0(\mathbb{N}(w) \setminus \{u\})$, we only need to consider whether there is any vertex in $\mathbb{N}(w) \setminus \{u\}$ in the independent set. Let $\delta = d(X_1, Y_1) - d(X_0, Y_0)$.

$X_0(\mathbb{N}(w) \setminus \{u\})$	possible cases to make $\delta = -1$	possible cases to make $\delta = 1$
0	None	$(1, 0)$
1	None	$(1, 0)$

Lets denote the number of edges belong to the second case by n_2, then

$$\begin{aligned}
\mathbb{E}(\delta) &= \frac{n_2}{m} \times \frac{1}{3} \\
&= \frac{n_2}{3m}
\end{aligned}$$

For the third case: Since in this case, we only select (a, b) from feasible combinations, the probability of $d(X_1, Y_1) = 0$ is 1. So if we denote the number of edges belong to the second case by n_3, then

$$\mathbb{E}(\delta) = \frac{-n_3}{m}$$

Put all the cases together, we have

$$\begin{aligned}
\mathbb{E}(\delta) &= \frac{1}{m}\left(\frac{n_2}{3} - n_3\right) \\
&\leq \frac{1}{m}\left(\frac{3n_3}{3} - n_3\right), \qquad \text{Since } n_2 \leq 3n_3 \\
&= 0
\end{aligned}$$

Note

Note that although we complete the proof on the book, it does not mean that we have proved the MC is rapidly mixing. The complete proof bases on a carefully designed distance measure function.

3 Exercise 7.12

Using the same reduction, but improved estimates, show that Proposition 7.11 holds for some Δ less than 1100. (I think $\Delta = 964$ is achievable)

3.1 Solution

First, we could note that we have a loose upper bound for $|J'|$. Actually, we could fix this upper bound, and we have

$$(2^r - 1)^k \le |J'| \le \binom{n}{k}(2^r - 1)^k$$

Recall that we have Stirling Formula for $n!$:

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \le n! \le 2\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

So

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\
&\le \frac{2\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\sqrt{2\pi k}\left(\frac{k}{e}\right)^k\sqrt{2\pi(n-k)}\left(\frac{n-k}{e}\right)^{n-k}} \\
&\le \frac{2\sqrt{n}n^n}{\sqrt{k}\sqrt{2\pi(n-k)}k^k(n-k)^{n-k}} \\
&\le \frac{2\sqrt{4k}(4k)^{4k}}{\sqrt{k}\sqrt{2\pi(4k-k)}k^k(4k-k)^{4k-k}}, \qquad \text{since } k \ge \tfrac{n}{4} \\
&= \frac{4 \times 4^{4k}k^{4k}}{\sqrt{6\pi k} \times k^k 3^{3k} k^{3k}} \\
&= \frac{4 \times 4^{4k}}{\sqrt{6\pi k} \times 3^{3k}} \\
&\le \frac{4^{4k}}{3^{3k}}, \qquad \text{since } 4 \le \sqrt{6\pi k}
\end{aligned}$$

Then we have a more tight bound for $|J'|$

$$(2^r - 1)^k \le |J'| \le \binom{n}{k}(2^r - 1)^k$$

or, taking the natural logarithm,

$$k\ln(2^r - 1) \le \ln|J'| \le 4k\ln 4 - 3k\ln 3 + k\ln(2^r - 1)$$

Consider the following estimate for k

$$\hat{k} = \frac{\ln|J'|}{4\ln 4 - 3\ln 3 + \ln(2^r - 1)}$$

then

$$k\left(\frac{\ln(2^r - 1)}{4\ln 4 - 3\ln 3 + \ln(2^r - 1)}\right) \leq \hat{k} \leq k$$
$$k\left(1 - \frac{4\ln 4 - 3\ln 3}{4\ln 4 - 3\ln 3 + \ln(2^r - 1)}\right) \leq \hat{k} \leq k$$

Note that when $r = 241$,

$$\frac{4\ln 4 - 3\ln 3}{4\ln 4 - 3\ln 3 + \ln(2^r - 1)} \leq \frac{1}{74}$$