TCS **作业四**：Zero-Knowledge Proof, a Cryptographic Primitive
计试 2101 仲星焱
2023 年 7 月 2 日

4.1　任取 $c > 1, 0 < \epsilon < 1$，令 $p(n) = c^{(n^{\epsilon-1})}$ 即可。

4.2　考虑题目中的交互式证明系统 (P, V)，为了证明其 completeness 与一般交互式证明系统的 completeness 等价，我们考虑对于参数 n ，重复执行证明 n 次，一个 P 被拒绝当且仅当在所有轮次当中都被拒绝，因此一个正确的 P 被拒绝的概率是 $1/3^n$，是 negligible ，因此一个正确的 S 被大概率接受。此系统的 completeness 不弱于一般的系统

反过来，对于一般的 (P, V) 只需要在接受的时候有 1/3 概率变为拒绝，也可以发现一般系统的 completeness 不弱于此系统。

综上，两种系统的 completeness 等价。

4.3　1. completeness：正确的 Prover 会被以 1 的概率接受，故此系统 complete

2. soundness：考虑一个 cheating Prover 的策略，显然是每次随机选一个图生成一个同构，然后赌 Verifier 随机选择的图和自己一样，在 n 轮检测当中，全部通过的概率是 $1/2^n$，显然为 negligible，会被以高概率拒绝，故此系统 sound

3. zero-knowledge：考虑 Prover 选取所有同构图的概率是相等的，都是 $1/(n! - 2 - i)$，其中 i 表示证明已经进行过的轮数（为了保证 0 知识，显然不能生成两个原图）。在获取 input 内容，即两个原图之后，所有轮次生成的 G'' 的分布已经确定，返回的映射分布也已经确定，此即 message 的分布，与 Verifier 是否是 cheater 无关，而与其关联的 coin flips 显然也能够通过每轮进行的询问确定分布。故此系统中 Verifier 的 view 的分布可被模拟器完成，所以此系统的 PZK 的。

4.4　考虑这样一个系统，P 需要向 V 证明自己手里有一个秘密 s 位二进制串 θ，V 随机生成一个二进制串 x 给 P，P 返回 $x \oplus \theta$ 供 V 解密。

不难发现返回的 $x \oplus \theta$ 在所有 s 位二进制串中均匀分布，此即 message 的分布，容易验证这个系统是 $pseudo-ZK$，但是由于 simulator 不知道 θ 的真实值，故对于每个分布无法推知对应的 coin flips 的状态，反过来也一样，对于特定的 coin flips，无法推知得到的 $x \oplus \theta$ 的分布，故不可能是 PKZ 的。

4.5　V 的视野中包含以下内容：$g, h, p, q = 2p+1$，每一次收到的 message 包含 j，根据 V 做出的答复还可能收到 f 或 f'。

首先容易注意到 f, f' 在分布上存在细微差别，f 为 $\{1, 2, \ldots, q-1\}$ 当中的均匀分布，而 f' 为 $\{1+e \mod q, 2+e \mod q, \ldots, q-1+e \mod q\}$，由于我们不知道 e 的具体数值，实际上 f' 的分布无法知道。

因此，我们如此设计 σ，首先仿照 V 的随机方式生成 $0,1$，决定我们如何生成询问和回答的 message。假设生成 0，则按照均匀分布生成 f，计算 $j \equiv g^f \pmod p$，否则按照 $\{0, 1, 2, \ldots, q-1\}$ 中的均匀分布生成 f'，计算 $j \equiv g^{f'} h^{-1} \pmod p$。其中 h^{-1} 是 $\mod p$ 意义下的乘法逆元，可以用 $O(\log p)$ 时间（假设乘法是 $O(1)$）或者 $O(\log p \log\log p)$（数据过大，乘法不认为是 $O(1)$）时间预处理。

设 $S = \{X | X\text{中有对}Prover\text{的1询问}\}$ 对于 distinguisher 假设 $D(X) = 1$ 当且仅当 $X \in S$，即询问了 f'，此时 $|Pr(D(X)=1) - Pr(D(Y)=1)|$ 达到最大，假设进行 n 轮，单次询问中 V 进行 0 询问的概率是 z，进行 1 询问的概率是 w。有

$$
\begin{aligned}
|Pr(D(X)=1) - Pr(D(Y)=1)| &\le \sum_{s \in S} |Pr(X=s) - Pr(Y=s)| \\
&= \sum_{i=0}^{n} w^i z^{n-i} \binom{n}{i} \frac{1}{(2p)^{n-i}} \left(\frac{1}{(2p)^i} - \frac{1}{(2p+1)^i}\right) \\
&= \frac{1}{(2p)^n} - \left(\frac{z}{2p} + \frac{w}{2p+1}\right)^n \\
&< \frac{1}{(2p)^n}
\end{aligned}
$$

显然 negligible，进而是 computationally indistinguishable，进而该证明是 CZK 的。

话说这不是直接证明是 SZK 了吗。

4.6　直接令 P 在最后一轮以 negligible 概率无视询问直接泄露原映射即可。

4.7　等价，考虑如下证明。

先证明 def 10 下可区分，def 8 下必然可区分，令 $U = \{u|Pr(A(X) = u) > Pr(A(Y) = u)\}$，则

$$\sum_v |Pr(A(X) = v) - Pr(A(Y) = v)| = 2\sum_{v\in U} Pr(A(X) = v) - Pr(A(Y) = v)$$

非 negligible。

于是我们定义一个 distinguisher $D, D(X) = [X \in U]$，则对于这个 distinguisher，不难发现 $|Pr(D(X) = 1) - Pr(D(Y) = 1)| = 2\sum_{v\in U} Pr(A(x) = v) - Pr(A(Y) = v)$ 非 negligible，但是 def 8 中已经包含了所有 distinguisher，也有这个 distinguisher，与假设矛盾，

再证明 def 8 下可区分，def 10 下必然可区分，不难发现对于任意 distinguisher ，由加法交换律和绝对值的性质可以知道 $\forall D, |Pr(D(X) = 1) - Pr(D(Y) = 1)| \le \sum_v |Pr(A(X) = v) - Pr(A(Y) = v)|$，由于 def8 下可区分，前者非 negligible，后者显然非 negligible，进而 def10 下可区分。

由此，def 8 和 def 10 完全等价。

4.8　(a) 不成立，没有保证随机变量独立，一个显然的的反例就是如果 x, y 同分布且 x 与 $\bar{x}$ 同分布，其中 $\bar{x}$ 是 x 的反码串，而 $u = x + 1$ ，$v = \bar{y} + 1$ 此处 $+1$ 相当于将 x, y 视为 s 位二进制数进行无符号加法。

不难验证 x 与 $\bar{y}$ 也是同分布的，但是 $(x, u), (y, v)$ 就显然存在较大差异，下面给出一个具体的反例：

$$P(x = 0^s) = P(x = 1^s) = 1/2, \text{otherwise } P(x = t) = 0$$
$$P(y = 0^s) = P(y = 1^s) = 1/2, \text{otherwise } P(y = t) = 0$$
$$P(u = 0^{s-1}1) = P(u = 0^s) = 1/2, \text{otherwise } P(u = t) = 0$$
$$P(v = 0^{s-1}1) = P(v = 0^s) = 1/2, \text{otherwise } P(v = t) = 0$$
$$x =^c y, u =^c v$$
$$P(x = 0^s, u = 0^{s-1}1) = P(x = 1^s, u = 0^s) = 1/2$$
$$P(y = 0^s, v = 0^s) = P(y = 1^s, v = 0^{s-1}1) = 1/2$$

$$(x,u) \neq^c (y,v)$$

(b) 成立。

不加证明地，我们给出断言，有限个 negligible 的函数/变量之和仍然是 negligible。考虑极限的求和规则显然。

要求考虑所有 distingguisher, 即考虑所有本质不同的取值即可

$$\begin{aligned}\forall t \in \{0,1\}^s, |Pr(x=t) - Pr(x=t)| &= |\sum_{t'} Pr(x=t, u=t') - \sum_{t'} Pr(y=t, v=t')| \\ &\leq \sum_{t'} |Pr(x=t, u=t') - Pr(y=t, v=t')|\end{aligned}$$

而 $|Pr(x=t, u=t') - Pr(y=t, v=t')|$ 由给出条件知是 negligible 的。

故 $\forall t, |Pr(x=t) - Pr(y=t)|$ 是 negligible，$x =^c y$，同理 $u =^c v$。