ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Solution to Exercise 3

3.1 Definition of Interactive Proofs

a) As an extreme example, the "halting problem" is known to be undecidable and therefore not in **IP**. There are also decidable problems that are not in **IP**. For example, some problems related to the game of Go are **EXPSPACE**-complete.

b) Consider an interactive proof (P, V) for a language L, where P and V are probabilistic. We want to construct a deterministic $\widehat{P}$ so that $(\widehat{P}, V)$ is an interactive proof that accepts the same language.

In the random experiment between the probabilistic P and the probabilistic V, denote by $p^{\mathsf{acc},x}$ the probability that V accepts x. Moreover, let $p_r^{\mathsf{acc},x}$ be the probability that V accepts if P's randomness is fixed to r and p_r that r is chosen as P's randomness.

On input x, $\widehat{P}$ does as follows: It runs the protocol (P, V) with all possible random inputs for both Peggy and Vic and computes for each fixed randomness r of Peggy, the set of fixed randomness s of Vic that are accepted in the protocol (P, V).[1] Then, $\widehat{P}$ chooses to run P with the randomness r' that maximizes $p_{r'}^{\mathsf{acc},x}$. Note that $p_{r'}^{\mathsf{acc},x}$ is the probability that V accepts in an interaction with $\widehat{P}$. Observe that

$$p \leq p^{\mathsf{acc},x} = \sum_r p_r^{\mathsf{acc},x} p_r \leq \sum_r p_{r'}^{\mathsf{acc},x} p_r = p_{r'}^{\mathsf{acc},x} \sum_r p_r = p_{r'}^{\mathsf{acc},x}.$$

Thus, if $x \in L$, the probability that $\widehat{P}$ convinces V is at least p. Conversely, since V is such that it accepts a proof for a word $x \notin L$ with probability at most q no matter which prover it interacts with, $(\widehat{P}, V)$ is trivially sound.

Given the considerations in **b)**, the prover's algorithm is assumed to be deterministic for the remainder of this task.

c) If both P and V are deterministic, for every x there is but a single transcript between P and V. Since (P, V) is an interactive proof, this transcript is accepted by V if and only if $x \in L$. Thus, the transcript serves as an efficiently verifiable witness if $x \in L$ and if $x \notin L$, no transcript can convince V. Thus, $L \in \mathbf{NP}$.

d) Let (P, V) be an interactive-proof protocol with $q = 0$, i.e., V never accepts some $x \notin L$. The situation is similar to that in **c)**: If $x \in L$, the fact that $p > q = 0$ implies that there exists an accepting transcript between P and V, which is a witness for x. If $x \notin L$, $q = 0$ implies that no such transcript exists. Thus, $L \in \mathbf{NP}$.

e) For $n \geq 1$ we define the protocol (P', V') as follows: For input x, the protocol (P, V) is repeated sequentially n times. V' accepts x if and only if V accepted x at least $p^* \cdot n$ times. We show now that for n large enough (P', V') meets the definition of an interactive proof with parameters p', q'. To do that, let us fix $p^* = \frac{p+q}{2}$, and $\epsilon = \frac{p-q}{2}$. For $i = 1, \ldots, n$, let X_i be the random variable that is 1 if V accepts x in the i^{th} round and 0 otherwise, and set $\overline{X} := \frac{1}{n} \sum X_i$ and $\mu := E[\overline{X}]$. Note that $\mu = \mathsf{P}[X_i = 1]$ for any i.

[1] Recall that the prover's algorithm need not be efficient.

Consider now $x \in L$. In that case $\mu = \mathsf{P}[X_i = 1] \geq p^* + \varepsilon$. Hence,

$$\begin{aligned}
\mathsf{P}[V' \text{ rejects } x] &\leq \mathsf{P}[\sum X_i \leq p^* n] \\
&= \mathsf{P}[\sum X_i \leq (p^* + \varepsilon)n - \varepsilon n] \\
&= \mathsf{P}[\overline{X} \leq (p^* + \varepsilon) - \varepsilon] \\
&\leq \mathsf{P}[\overline{X} \leq \mu - \varepsilon] \\
&\leq e^{-2n\varepsilon^2}.
\end{aligned}$$

Consider now $x \notin L$. In that case $\mu = \mathsf{P}[X_i = 1] \leq p^* - \varepsilon$. Hence,

$$\begin{aligned}
\mathsf{P}[V' \text{ accepts } x] &\leq \mathsf{P}[\sum X_i \geq p^* n] \\
&= \mathsf{P}[\sum X_i \geq (p^* - \varepsilon)n + \varepsilon n] \\
&= \mathsf{P}[\overline{X} \geq (p^* - \varepsilon) + \varepsilon] \\
&\leq \mathsf{P}[\overline{X} \geq \mu + \varepsilon] \\
&\leq e^{-2n\varepsilon^2}.
\end{aligned}$$

Concerning the number n of repetitions, note that if for example $p' = 1 - \delta$ and $q' = \delta$ for $\delta > 0$, then completeness and soundness are satisfied if $e^{-2n\varepsilon^2} \leq \delta$. This is the case if and only if $n \geq \frac{1}{2}\varepsilon^{-2}\ln(\delta^{-1})$. This means that δ can be made *negligible*, whereas ε needs to be *noticeable* (asymptotically in the length of the input to P and V) in order for n to be *polynomial*.[2]

3.2 Geometric Zero-Knowledge

a) Given two angles α and β, the angle $\alpha \pm \beta$ can be constructed as follows: Open the compass to an arbitrary angle. Draw a circle around the endpoints of both angles with the resulting radius, which results in four new points $p_\alpha, p'_\alpha, p_\beta, p'_\beta$. Open the compass to the distance between p_α and p'_α. Draw a circle around, say, p_β with the resulting radius and create the line ℓ through p_β and p'_β as well as the intersection points q_β and q'_β of the circle and ℓ. Then, create a line through the endpoint of β and q_β or q'_β, depending on whether $\alpha + \beta$ or $\alpha - \beta$ is to be constructed.

b) A possible protocol for this task is the following one:

Peggy		**Vic**
knows angles α, β s.t. $\beta = 3\alpha$		knows angle β
choose random angle κ create $\tau := 3\kappa$	$\xrightarrow{\tau}$	
	$\xleftarrow{c}$	choose random $c \in_R \{0, 1\}$
create $\rho := \kappa + c\alpha$	$\xrightarrow{\rho}$	check $3\rho \stackrel{?}{=} \tau + c\beta$

c) Completeness: One can easily verify that if Peggy is honest and knows α, Vic will always accept.

Proof of Knowledge: Here we show that if Peggy knows how to answer both challenges, she actually can compute the trisection α. Assume Peggy knows successful

[2] See the the lecture notes, Section 1.1.6, for definitions of negligible, noticeable, and polynomial.

answers ρ, ρ' to both challenges $c = 0$ and $c' = 1$ for the same first message τ. In that case,

$$3\rho = \tau \quad \text{and} \quad 3\rho' = \tau + \beta.$$

Thus, $3\rho' - 3\rho = \beta = 3\alpha$, and, therefore, Peggy may compute the angle α as $\rho' - \rho$.

d) Zero-Knowledge: The protocol is c-simulatable: for a given challenge $c \in \{0, 1\}$, choose a uniform random angle ρ and set $\tau := 3\rho - c\beta$, which is easily checked to result in the correct distribution. Moreover, the size of the challenge space is clearly polynomial.

Therefore, as discussed in the lecture, the protocol is perfectly zero-knowledge.

3.3 The "Complement" of Fiat-Shamir: Proof of Quadratic Non-Residuosity

Let $m = pq$. In the following, denote by QR_m the set of quadratic residues and by QNR_m the set of quadratic non-residues in $\mathbb{Z}_m^*$. Observe that if $a \in \mathrm{QR}_m$, then $a \cdot b \in \mathrm{QR}_m$ if and only if $b \in \mathrm{QR}_m$.

a) The protocol works as follows:

Peggy		**Vic**
knows a		knows a
		choose $b \in_R \{0,1\}, \rho \in_R \mathbb{Z}_m^*$
	$\xleftarrow{\quad y \quad}$	compute $y := a^b \cdot \rho^2$
$b' := 0$ if $y \in \mathrm{QR}_n$ $b' := 1$ otherwise	$\xrightarrow{\quad b' \quad}$	$b' \stackrel{?}{=} b$

Note that Peggy must determine whether y is a quadratic residue, which, however, is of no concern since the prover is permitted to be unbounded.

b) The protocol is a proof of the statement that a is a quadratic non-residue modulo m. It is not a proof of knowledge.

Completeness: If a is a quadratic non-residue, then $a \cdot \rho^2$ is a quadratic non-residue (Section 1.1.5 of the lecture notes), and, obviously, ρ^2 is a quadratic residue. Thus, the unbounded Peggy is able to determine the bit b of Vic correctly.

Soundness: Assume a is a quadratic residue. Then, both $a \cdot \rho^2$ and ρ^2 are uniform random elements of QR_m. Therefore, a cheating prover P''s view is statistically independent of Vic's bit b, which causes Vic to reject with probability at least $1/2$.

c) The view of the honest verifier V can be simulated easily by choosing a random bit b and a random $\rho \in \mathbb{Z}_m^*$ and setting $y := a^b \rho^2$ and $b' := b$.

d) The protocol is not zero-knowledge. A dishonest Vic V' can use the interaction with Peggy to find out whether or not some arbitrary number $a' \in \mathbb{Z}_m^*$ is a quadratic residue modulo m (by setting $y = a'$).