ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 3

3.1 Definition of Interactive Proofs

An *interactive proof* of membership for some language L is a protocol between two interactive probabilistic algorithms P and V that satisfies the following properties:

(i) COMPLETENESS: If $x \in L$, then P makes V accept with probability at least $p = 3/4$.

(ii) SOUNDNESS: If $x \notin L$, then any probabilistic algorithm P' makes V accept with probability at most $q = 1/2$.

The class of all languages L for which there exists an interactive proof (P, V) with a polynomially bounded verifier V is denoted by **IP**. Note that the prover P is assumed to be unbounded, i.e., there are no restrictions on its computing power.

a) Name a language that is not in **IP**.

b) Show that a deterministic prover is as powerful as a probabilistic one, i.e., prove that for every interactive proof (P, V), there exists a deterministic $\widehat{P}$ such that $(\widehat{P}, V)$ is an interactive proof that accepts the same language. HINT: $\widehat{P}$ may use P and V (but only with fixed random coins).

c) Show that a language L for which there exists an interactive proof (P, V) with a deterministic verifier V is in **NP**.

d) Show that a language L for which there exists an interactive proof with $q = 0$ is in **NP**.

e) Argue that the definition of **IP** is independent of the actual choice of p and q. More precisely, given an interactive proof (P, V) with parameters $1 > p > q > 0$, construct an interactive proof (P', V') with parameters p', q' for $1 > p' > q' > 0$.

HINT: Use Hoeffding's inequality. Let $\varepsilon > 0$ and let $X_1, \dots, X_n$ be i.i.d. Bernoulli random variables where $\overline{X} = \frac{1}{n} \sum X_i$ and $E[\overline{X}] = \mu$. Then it holds that:

$$P[\overline{X} \leq \mu - \varepsilon] \leq e^{-2n\varepsilon^2}$$
$$P[\overline{X} \geq \mu + \varepsilon] \leq e^{-2n\varepsilon^2}$$

3.2 Geometric Zero-Knowledge

In this exercise we consider geometric constructions using a ruler (without markings) and a compass (Lineal and Zirkel). The operations we consider are those that we know from high school, namely to draw a line through two points, to draw a circle with center at one point that goes through another point, to obtain the intersection between two lines/two circles/a line and a circle, and to copy circles.[1][2]

a) An *angle* is a geometric object consisting of two rays (half-lines) with a common end point. Show how one can add and subtract two angles, i.e., given angles α and β, construct $\alpha + \beta$ and $\alpha - \beta$ using the above operations.

A well-known result from abstract algebra states that the trisection of an arbitrary angle cannot be drawn in the above sense.

b) Peggy claims that she knows[3] the trisection α of a publicly known angle $\beta = 3\alpha$. Construct an interactive protocol that allows her to prove this claim. You may assume that Peggy can generate a random point on a circle and that Vic can flip a fair coin.

c) Prove that your protocol is complete and argue (informally) why it is a proof of knowledge.

d) Prove that your protocol is zero-knowledge.

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

The Fiat-Shamir protocol allows Peggy to prove to Vic that some given number $z \in \mathbb{Z}_m^*$ $(m = p \cdot q)$ is a quadratic residue.

a) Describe an interactive protocol (P, V) that allows Peggy to prove to Vic that a given number $a \in \mathbb{Z}_m^*$ is *not* a quadratic residue. You may assume that Peggy is computationally unbounded.

b) Argue that your protocol is complete and sound. Is your protocol a proof of a statement, or is it a proof of knowledge (or both)?

c) Argue that your protocol leaks no information to the *honest* verifier V, who follows the protocol instructions.

d) Does this hold for a *cheating* verifier V' as well?

---

[1] This last operation can actually be performed with the other three.

[2] If you desire, you may play with the applet on `www.geogebra.org`.

[3] i.e., holds a copy of the geometric object α.