Tutorial 09 – Protocols and randomness

Exercise 1. *Miller–Rabin test*

In this exercice we want to show that testing if a number is prime belongs to RP. To do so, suppose that p is an odd number and denote $p-1 = 2^s d$, where d is odd. We consider the following two sets:

$$W_1 = \left\{a \in \mathbb{Z}_p \setminus \{0\} \colon a^d = 1 \text{ or } -1 \in \{a^d, a^{2d}, \ldots, a^{2^{s-1}d}\}\right\},$$
$$W_2 = \left\{a \in \mathbb{Z}_p \setminus \{0\} \colon a^{2^s d} \neq 1 \text{ or } \left(a^d \neq 1 \text{ and } -1 \notin \{a^d, a^{2d}, \ldots, a^{2^{s-1}d}\}\right)\right\}.$$

(All operations in this exercice are in $\mathbb{Z}_p$, unless stated otherwise.)

1. Prove that if $a \in W_1$, then $a^{2^s d} = 1$. What can you say about the sequence $(a^d, a^{2d}, \ldots, a^{2^{s-1}d}, a^{2^s d})$?

   If $a^d = 1$, then $a^{2^s d} = 1$. If $a^{2^t d} = -1$ for some $t < s$, then $a^{2^{t+1}d} = 1, a^{2^{t+2}d} = 1$ etc. In other words, this sequence is either equal to $(1, 1, \ldots, 1)$ or it finishes by $(\ldots, (-1), 1, 1, \ldots, 1)$.

2. Prove that $W_1 \cap W_2 = \emptyset$ and $W_1 \cup W_2 = \mathbb{Z}_p \setminus \{0\}$.

   The set W_1 consists of $a \in \mathbb{Z}_p \setminus \{0\}$ such that the sequence $(a^d, a^{2d}, \ldots, a^{2^{s-1}d}, a^{2^s d})$ ends with 1 and either starts with 1 or contains -1. The set W_2 contains all the other elements of $a \in \mathbb{Z}_p \setminus \{0\}$: the sequence $(a^d, a^{2d}, \ldots, a^{2^{s-1}d}, a^{2^s d})$ either ends with something different than 1 or it does not start with 1 and does not contain -1.

3. Prove that if p is prime, then $W_2 = \emptyset$.
   Hint: Use Fermat's little theorem and the fact that $\mathbb{Z}_p$ is a field.

   If p is prime, then $a^{p-1} = a^{2^s d} = 1$ by Fermat's little theorem for all $a \in \mathbb{Z}_p \setminus \{0\}$. Moreover, since $\mathbb{Z}_p$ is a field, the polynomial $x^2 = 1$ has exactly two roots in $\mathbb{Z}_p$, namely 1 and -1. In particular, the sequence $(a^d, a^{2d}, \ldots, a^{2^{s-1}d}, a^{2^s d})$ is either equal to $(1, 1, \ldots, 1)$ or contains -1 (more precisely, it finishes by $(\ldots, (-1), 1, 1, \ldots, 1)$). Thus, $W_2 = \emptyset$ and $W_1 = \mathbb{Z}_p \setminus \{0\}$.

4. Suppose that p is a power of a prime number, $p = q^k$ for some $k \geq 2$. Let $a = 1 + q^{k-1}$. Prove that $a^p = 1$ and $a^{p-1} \neq 1$. In particular, $a \in W_2$.

   If we take $a = 1 + q^{k-1}$, then $a^p = (1 + q^{k-1})^p = 1 + pq^{k-1} +$ (higher powers of q) $= 1$ by the binomial expansion. Therefore $a^{p-1} \neq 1$, because this would imply that $1 = a^p = a$.

5. Suppose that p is a power of a prime number as above. Show that $|W_2| \geq |W_1|$.
   Hint: Consider the set $aW_1 = \{ab \colon b \in W_1\}$, where $a = 1 + q^{k-1}$.

   Let $a = 1 + q^{k-1}$ and $b \in W_1$. Then, $(ab)^{p-1} = a^{p-1} \neq 1$, so $ab \in W_2$. Moreover, if $b, b' \in W_1$, then $ab \neq ab'$, because $ab = ab'$ would imply that $b = a^p b = a^p b' = b'$. Hence, $|aW_1| = |W_1|$ and $aW_1 \subseteq W_2$.

6. The Chinese Reminder Theorem states that if $n_1, n_2 \in \mathbb{N}$ are relatively prime and $p = n_1 n_2$, then the map $\mathbb{Z}_p \ni x \to (x \bmod n_1, x \bmod n_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ is a bijection. Prove this theorem.

   This map is an injection. Indeed, if $(x \bmod n_1, x \bmod n_2) = (y \bmod n_1, y \bmod n_2)$, then $x - y$ is divisible by both n_1 and n_2. Since they are relatively prime, we get $p | x - y$ and hence $x = y$ because $x, y \in \mathbb{Z}_p$. Moreover, the sets $\mathbb{Z}_p$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ have the same cardinality, so this map is a bijection.

7. Suppose that $p = n_1 n_2 \in \mathbb{N}$, where $n_1, n_2 > 1$ are relatively prime odd numbers. Prove that there exists $c \in \mathbb{Z}_p$ such that $c \neq \pm 1$ but $c^2 = 1$.

8. Let p be as above. Prove that if the equation $x^k = -1$ has a solution in $\mathbb{Z}_p$, then the equation $x^k = c$ also has a solution.

9. Let p be as above. Show that $|W_2| \geq |W_1|$.
Hint: let $0 \leq t \leq s$ be the highest number such that $x^{2^t d} = -1$ has a solution. Let r be a solution of $x^{2^t d} = c$. Consider the set rW_1.

10. Construct a probabilistic TM M whose expected running time is polynomial that, given $n \geq 0$ written in binary, outputs a random number in the interval $\{0, 1, \ldots, n-1\}$ (with uniform distribution).

11. Prove that testing if a number is prime belongs to RP.

Definition (Interaction of deterministic functions)**.** Let $f, g : \{0,1\}^* \xrightarrow{\{} 0,1\}^*$ be functions. A k-round interaction of f and g on input $x \in \{0,1\}^*$, denoted by $\langle f, g\rangle(x)$ is the sequence of the following strings $a_1, ..., a_k \in \{0,1\}^*$ defined as follows:

$$
\begin{aligned}
a_1 &= f(x) \\
a_2 &= g(x, a_1) \\
&\cdots \\
a_{2i+1} &= f(x, a_1, ..., a_{2i}) \text{ for } 2i < k \\
a_{2i+2} &= g(x, a_1, ..., a_{2i}) \text{ for } 2i + 1 < k
\end{aligned}
$$

The output of f at the end of the interaction denoted $\mathbf{out}_f\langle f, g\rangle(x)$ is defined to be $f(x, a_1, ..., a_k)$ and we assume that this output is in $\{0,1\}$

We can extend the notion of interaction to probabilistic functions (actually, we only need to do so for the verifier). To model an interaction between f and g where f is probabilistic, we add an additional m-bit input r to the function f , that is having $a_1 = f(x, r)$, $a_3 = f(x, r, a_1, a_2)$, etc. The interaction $\langle f, g\rangle(x)$ is now a random variable over $r \in_R \{0,1\}^m$. Similarly the output $\mathbf{out}_f\langle f, g\rangle(x)$ is also a random variable.

Definition (IP)**.** For an integer $k \geqslant 1$, we say that language L is in $\mathbf{IP}[k]$ if there is a probabilistic Turing machine V that runs in time polynomial in $|x|$ which can have a k-round interaction with a function $P : \{0,1\}^* \to \{0,1\}^*$ such that

$$
\begin{aligned}
x \in L &\implies \text{there exists } P \text{ such that } \Pr[\mathbf{out}_V\langle V, P\rangle(x)] \geqslant \frac{2}{3} && \text{(Completeness)} \\
x \notin L &\implies \text{for all } P \text{ , } \Pr[\mathbf{out}_V\langle V, P\rangle(x)] \leqslant \frac{1}{3} && \text{(Soundness)}
\end{aligned}
$$

Exercise 2. *Arthur–Merlin*

The class AM (Arthur–Merlin) is defined as the class of decision problems that can be verified by an *Arthur–Merlin protocol* in which the random bits are public. More precisely, Arthur is the polynomial-time verifier, and Merlin is the prover. Given x, Arthur generates a vector of random bits r and sends (x, r) to Merlin. Then, Merlin sends back a proof y. As a result, Arthur has a tuple (x, r, y). Given this tuple, Arthur must decide in *deterministic* polynomial-time whether to accept or not. Completeness means that if $x \in L$, then Merlin should be able to convince Arthur to accept with probability $2/3$, and soundness means that if $x \notin L$, then Arthur should reject with probability $2/3$, no matter what Merlin does. More formally, a language L belongs to AM if there exist polynomials p, q and a polynomial-time Turing machine M such that

$$x \in L \implies \Pr_{r \in \{0,1\}^{p(|x|)}}[\exists y \in \{0,1\}^{q(|x|)} M(x,r,y) \text{ accepts}] \geq 2/3 \quad \text{(completeness)}$$
$$x \notin L \implies \Pr_{r \in \{0,1\}^{p(|x|)}}[\forall y \in \{0,1\}^{q(|x|)} M(x,r,y) \text{ rejects}] \geq 2/3 \quad \text{(soundness).}$$

1. Show that NP $\subseteq$ AM, BPP $\subseteq$ AM, and AM $\subseteq$ IP.
2. How to amplify the probabilities in the definition of AM?
3. If A, B are two languages, then we say that A reduces to B under a *randomized* polynomial-time reduction if there exists a probabilistic polynomial-time Turing machine M such that

$$\forall x \in \{0,1\}^*,\ \Pr[x \in A \iff M(x) \in B] \geq 2/3\,.$$

   Show that $L \in$ AM if and only if L reduces to SAT under a randomized polynomial-time reduction (this class is also denoted as BP $\cdot$ NP).
4. Show that AM $\subseteq$ NP/poly.
5. Show that AM $\subseteq \Sigma_3^p$.

Exercise 3. *Quadratic residuosity*

For $n \geq 1$ we denote by $\mathbb{Z}_n^* \subseteq \{1, 2, \ldots, n-1\}$ the set of all numbers that are relatively prime with n. We say that $x \in \mathbb{Z}_n^*$ is a *quadratic residue modulo n* if there exists $y \in \mathbb{Z}_n^*$ such that $y^2 = x \bmod n$. The *Quadratic Residuosity* problem asks, given (x, n), to decide if x is a quadratic residue modulo n or not.

1. Prove that $\mathbb{Z}_n^*$ forms a group (with multiplication modulo n as the group operation).
2. Prove that quadratic residues form a subgroup in $\mathbb{Z}_n^*$.
3. Prove that if x is a quadratic residue, then the cardinality of the set $\{y \in \mathbb{Z}_n^* \colon y^2 = x \bmod n\}$ does not depend on x (i.e., it depends only on n).
4. Give an interactive proof for showing that x is *not* a quadratic residue modulo n.
   Hint: If x is not a quadratic residue, then xy^2 also is not.