Tutorial 08 – Randomized algorithms

Exercise 1. *ZPP*

Definition (Randomized Polynomial Time)**.** The class RP is defined as the set of languages L such that there exists a polynomial p and a polynomial-time TM M with two halting states q_{accept} and q_{reject}, such that on every input $x \in \Sigma^*$ we have:

- $\Pr_{r\in\{0,1\}^{p(|x|)}}[M(x,r) \to q_{accept} | x \in L] \geqslant 1/2$
- $\Pr_{r\in\{0,1\}^{p(|x|)}}[M(x,r) \to q_{accept} | x \notin L] = 0$

In other words, if $x \notin L$, M will never accept, but it may reject when $x \in L$.

Definition (Zero-error Probabilistic Polynomial time)**.** The class ZPP is defined as the set of languages L such that there exists a polynomial p and a polynomial-time TM M with three halting states q_{accept}, q_{reject} and q_{meh}, such that on every input $x \in \Sigma^*$ we have:

- $\Pr_{r\in\{0,1\}^{p(|x|)}}[M(x,r) \to q_{reject} | x \in L] = 0$ and $\Pr_{r\in\{0,1\}^{p(|x|)}}[M(x,r) \to q_{meh} | x \in L] \leqslant 1/2$
- $\Pr_{r\in\{0,1\}^{p(|x|)}}[M(x,r) \to q_{accept} | x \notin L] = 0$ and $\Pr_{r\in\{0,1\}^{p(|x|)}}[M(x,r) \to q_{meh} | x \notin L] \leqslant 1/2$

In other words, M will never answer incorrectly, but can return « I don't know » (state q_{meh}) with probability $\leqslant \frac{1}{2}$.

1. Recall how to reduce the error to recognize a language in BPP, deduce a similar procedure for RP.
2. Show that $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.
3. Prove that $L \in \mathsf{ZPP}$ iff there exists a probabilistic Turing machine M that recognizes L with probability 1, and whose expected running time is polynomial.

Exercise 2. *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 $(a^d, a^{2d}, \ldots, a^{2^{s-1}d}, a^{2^s d})$?
2. Prove that $W_1 \cap W_2 = \emptyset$ and $W_1 \cup W_2 = \mathbb{Z}_p \setminus \{0\}$.
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.

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, $a \in W_2$.

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* $a = 1 + q^{k-1}$.

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.

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.

Exercise 3. *Polynomial Hierarchy*

You have seen during the course the quantifier definition of the polynomial hierarchy: $L \in \Sigma_i^p$ if there exists a polytime TM M and a polynomial q such that:

$$x \in L \iff \exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \ldots Q_i u_i \in \{0,1\}^{q(|x|)} M(x, u_1, u_2, \ldots, u_i) = 1\,.$$

You have also seen an alternative definition using oracles:

$$\begin{cases} \Sigma_0^p & = \mathsf{P} \\ \Sigma_{i+1}^p & = \mathsf{NP}^{\Sigma_i^p} \end{cases}$$

With PH being defined as $\bigcup_{i \geqslant 0} \Sigma_i^p$.

1. Prove the equivalence between the quantifier-based definition and the oracle-based definition.

2. Give an oracle-based definition for Π_i^p.

3. Show that Σ_i^p is closed under polynomial-time many-one reduction.

4. Show that if there exist a PH-complete problem, then the polynomial hierarchy collapses.

5. Show that if $\Sigma_i^p = \Sigma_{i+1}^p$, then $\mathsf{PH} = \Sigma_i^p$.

6. Propose a family of problems (S_i) such that S_i is Σ_i^p-complete.