Complexité avancée - TD 8

Simon Halfon

November 9, 2016

Exercise 1: Probabilistic Logarithmic Space

Let BPL be the class of languages L for which there exists a probabilistic Turing machine running in polynomial time and logarithmic space (the random tape does not count in terms of space) such that:

- if $x \in L$ then $Pr[M(x,r) = \bot] \leq \frac{1}{3}$
- if $x \notin L$ then $Pr[M(x,r) = \top] \leq \frac{1}{3}$

Show that $\mathsf{BPL} \subseteq P$.

Exercise 2: BPP and oracle machines

Prove that $\mathsf{P}^{\mathsf{BPP}} = \mathsf{BPP}$.

Exercise 3: Primality Although the problem PRIMES is now known to be in P (cf AKS Algorithm), the most effective (in practice) primality tests are probabilistic algorithms. In this exercise we analyze one of these probabilistic algorithm: the Solovay-Strassen primality test, putting PRIMES in coRP. Before PRIMES were proved in P, the result was actually improved to PRIMES $\in \mathsf{ZPP}$.

We first recall the **Fermat test** for a number N.

```
Randomly choose a number $0 < a < N$
If $a^{N-1} \neq 1 \bmod \mathrm{N}$ reject ($N$ is composite)
otherwise accept ($N$ is probably prime)
```

This test is based on Fermat's theorem stating that if p is prime, then $a^{p-1} = 1 \bmod p$ *for all* $0 < a < p$.

A number $0 < a < N$ such that $a^{N-1} \neq 1 \bmod \mathrm{N}$ is called a *Fermat witness* (of compositeness of N).

- Show that the Fermat test on an input number N runs in probabilistic polynomial time (i.e. time polynomial in *log* N).

If N is prime, the Fermat test rejects with probability 0 (no witness can exist). If N is composite the probability of rejecting equals the fraction of Fermat witnesses in $\{1, \ldots, N-1\}$. If this fraction were at least one half, the Fermat test would put PRIMES in coRP. Unfortunately the proportion of Fermat witnesses can be much less, and therefore the above test does not have the coRP error probability bounds.

However under some assumptions, one can prove that the fraction of Fermat witnesses in $\{1, \ldots, N-1\}$ is at least one half.

- For a number N, prove that if there exists at least one Fermat witness $0 < a < N$, which is relatively prime to N, then the fraction of Fermat witnesses in $\{1, .., N-1\}$ is at least one half.

Notice that composite numbers N having no relatively prime Fermat witness in $\{1, .., N-1\}$ exist and are known as *Carmichael numbers* (although they are very rare, only 255 Carmicheal numbers less than 100 000 000, for instance).

Several refinements of the Fermat test have been proposed. The Solovay-Strassen test is one of them. We need some definitions first.

Given an odd prime p and a number a, the *Legendre symbol* of a and p (denoted by $\left(\frac{a}{p}\right)$) is defined as $a^{\frac{p-1}{2}} mod\ p$.

The Legendre symbol can be generalized to an arbitrary odd number (not necessarily prime) as follows.

Given an odd number N and a number A, the *Jacobi symbol* of A and N, denoted by $\left(\frac{A}{N}\right)$ is defined as $\Pi_{i=1}^{k} \left(\frac{A}{p_i}\right)$, where $p_i, i = 1..k$ are all the (not necessarily distinct) prime factors of N (i.e. $N = \Pi_{i=1}^{k} p_i$).

In the sequel assume the following known properties of Jacobi symbols:

Lemma 1

a) if A and N are relatively prime then $\left(\frac{A}{N}\right) \in \{-1, 1\}$, otherwise $\left(\frac{A}{N}\right) = 0$

b) $\left(\frac{A \cdot A'}{N}\right) = \left(\frac{A}{N}\right) \cdot \left(\frac{A'}{N}\right)$

c) $\left(\frac{A+N}{N}\right) = \left(\frac{A}{N}\right)$

d) if A and N are both odd and relatively prime, $\left(\frac{N}{A}\right) \cdot \left(\frac{A}{N}\right) = (-1)^{\frac{A-1}{2}\frac{N-1}{2}}$ (i.e. the two numbers are either equal or opposite)

e) $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$

- Using the properties stated in Lemma 1, show that the Jacobi symbol $\left(\frac{A}{N}\right)$ can be computed from A and N, without knowing the prime factorization of N, in time polynomial in $log(AN)$.

Clearly the Jacobi symbol provides another witness of compositeness (for odd numbers). In fact if N is an odd prime, then $\left(\frac{A}{N}\right) = A^{\frac{N-1}{2}} mod\ N$ for all A, and in particular all $0 < A < N$. However an important property of the Jacobi symbol is that this notion of witness is stronger than the Fermat witness, as stated in the following Lemma:

Lemma 2 For an odd N, if $\left(\frac{A}{N}\right) = A^{\frac{N-1}{2}} mod\ N$ for all $0 < A < N$ relatively prime to N, then N is a prime.

- Using Lemma 2 prove that if N is an odd composite, then for at least half of the numbers $\{0 < A < N | A$ relatively prime to $N\}$ one has $\left(\frac{A}{N}\right) \neq A^{\frac{N-1}{2}} mod\ N$.
- Based on the previous item, provide a coRP algorithm for PRIMES.