Practical session 8

Exercise 1 (Solovay-Strassen primality test)
For an odd prime number p and a positive integer $a < p$ let

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

be the Legendre symbol. For a natural odd number n and a natural number a which is relatively prime to n, let

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdot \ldots \cdot \left(\frac{a}{p_m}\right)^{k_m},$$

be the Jacobi symbol, where $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ is the factorization of n into prime numbers. You are given the fact that the Jacobi symbol can be calculated efficiently. Consider the following algorithm due to Solovay and Strassen.

Algorithm 0.1 (Solovay-Strassen)**.**
Input: A positive odd integer n.

1. *Choose $a \in \{2, \ldots, n-1\}$ uniformly at random.*
2. *if $\gcd(a, n) \neq 1$ return "composite".*
3. *else, if $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$ return "composite".*
4. *else return "prime".*

Let us recall two facts proved in Number Theory regarding the Legendre symbol:

Fact 0.2. *(Multiplicity) The Legendre symbol, and hence, the Jacobi symbol is multiplicative, i.e., for all positive integers $a, b < n$ which are relatively prime to n it holds that*

$$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right).$$

Fact 0.3. *(Euler's criterion) For an odd prime p and for every positive integer $a < p$ it holds that*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Use the following lemma, due to Solovay and Strassen, to show that Algorithm 0.1 outputs the correct answer if n is prime, and if n is composite, then Algorithm 0.1 outputs an incorrect answer with probability at most $1/2$.

Lemma 0.4. *Let n be an odd composite natural number. Then there exists $a \in \{2, \ldots, n-1\}$ such that $\gcd(a, n) = 1$ and $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$.*

Solution

If n is prime, then $\gcd(a, n) = 1$ and by Euler's criterion it holds that $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$. Therefore the algorithm outputs "prime" which is the correct output. Assume that n is odd and composite. Call a number $a \in \{2, \ldots, n-1\}$ a *witness* if $\gcd(a, n) = 1$ and $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$. We show that, among the numbers $a \in \{2, \ldots, n-1\}$ which are relatively prime to n, the number of witnesses is at least as large as the number of non-witnesses. Let $\{a_1, \ldots, a_m\} \subseteq \{2, \ldots, n-1\}$ be the set of all numbers that are *not* witnesses, where each a_i is relatively prime to n. Fix a witness a whose existence is guaranteed by Lemma 0.4. Then for every $1 \leq i \leq m$ it holds that

$$\begin{aligned}(a \cdot a_i)^{(n-1)/2} \bmod n &\equiv a^{(n-1)/2} \bmod n \cdot a_i^{(n-1)/2} \bmod n \equiv a^{(n-1)/2} \bmod n \cdot \left(\frac{a_i}{n}\right) \\ &\not\equiv \left(\frac{a}{n}\right) \cdot \left(\frac{a_i}{n}\right) = \left(\frac{a \cdot a_i}{n}\right).\end{aligned}$$

As $a \cdot a_i$ is relatively prime to n, it follows that $a \cdot a_i$ is a witness. Since, moreover, the function $a_i \mapsto a \cdot a_i \bmod n$ is injective (as $\gcd(a, n) = 1$), the number of witnesses is at least the number of non-witnesses. We conclude that the probability that a non-witness is sampled is at most $1/2$.

Exercise 2 (Freivalds' algorithm)

The following is an algorithm for verifying matrix multiplication.

Algorithm 0.5. *Input: Three $n \times n$ matrices A, B, and C.*

1. *Sample a vector $\mathbf{r}$ from $\{0,1\}^n$ uniformly at random (i.e., $\mathbf{r}$ is a vector of length n whose every entry is either 0 or 1).*
2. *Compute $\mathbf{v} = A \cdot (B \cdot \mathbf{r}) - C \cdot \mathbf{r}$.*
3. *Output "yes" if $\mathbf{v}$ is the all 0 vector, and "no" otherwise.*

Prove that if $AB = C$, then the algorithm always outputs "*yes*", and otherwise it outputs "*yes*" with probability at most $1/2$.

Solution

Assume that $AB = C$. Then for all $\mathbf{r} \in \{0,1\}^n$ it holds that

$$\mathbf{v} = A \cdot (B \cdot \mathbf{r}) - C \cdot \mathbf{r} = (AB) \cdot \mathbf{r} - C \cdot \mathbf{r} = C \cdot \mathbf{r} - C \cdot \mathbf{r} = (0, \ldots, 0)^T.$$

Therefore the algorithm always outputs "*yes*" which is the correct output. Assume then that $AB \neq C$. Let $D = AB - C$, and let d_{ij} be the element in the ith row and jth column of D. Let

$\mathbf{v} = (v_1, \ldots, v_n)^T$. As $AB \neq C$, there exists some entry $d_{ij} \neq 0$. We will show that $v_i = 0$ with probability at most $1/2$. For all $\mathbf{r} \in \{0,1\}^n$ we may write

$$v_i = \sum_{k=1}^{n} d_{ik} r_k = d_{ij} r_j + x_{\mathbf{r}},$$

where $x_{\mathbf{r}} = \sum_{k \neq j} d_{ik} r_k$. Observe that

$$\Pr\left(v_i = 0 \mid x_{\mathbf{r}} = 0\right) = \Pr\left(r_j = 0\right) = \frac{1}{2},$$

and that

$$\Pr\left(v_i = 0 \mid x_{\mathbf{r}} \neq 0\right) = \Pr\left(r_j = 1 \wedge d_{ij} = -x_{\mathbf{r}}\right) \leq \Pr\left(r_j = 1\right) = \frac{1}{2}.$$

By the Law of Total Probability it follows that

$$\begin{aligned}\Pr\left(v_i = 0\right) &= \Pr\left(v_i = 0 \mid x_{\mathbf{r}} = 0\right) \cdot \Pr\left(x_{\mathbf{r}} = 0\right) + \Pr\left(v_i = 0 \mid x_{\mathbf{r}} \neq 0\right) \cdot \Pr\left(x_{\mathbf{r}} \neq 0\right) \\ &\leq \frac{1}{2} \cdot \Pr\left(x_{\mathbf{r}} = 0\right) + \frac{1}{2} \cdot \Pr\left(x_{\mathbf{r}} \neq 0\right) = \frac{1}{2}.\end{aligned}$$

Therefore

$$\Pr\left(\text{Output is “}yes\text{”}\right) = \Pr\left(\mathbf{v} = (0, \ldots, 0)^T\right) = \Pr\left(v_k = 0 \text{ for every } k \in [n]\right) \leq \Pr\left(v_i = 0\right) \leq \frac{1}{2}.$$