Practical session 9

Exercise 1 Present a two-sided error monte-carlo random algorithm, that given 3 polynomials, outputs 1 if and only if exactly two of them are identical.

Solution
Let PIT denote the Schwartz-Zippel Algorithm for verifying polynomial identities that was presented in Lecture 7 (except that the algorithm outputs 1 if it finds the two polynomials it compares to be identical, and 0 otherwise). We now present our algorithm for the problem at hand.

Algorithm 0.1. *Input: 3 polynomials P, Q, and R.*

1. *Let* $b_1 = \mathrm{PIT}(P, Q)$, $b_2 = \mathrm{PIT}(Q, R)$, *and* $b_3 = \mathrm{PIT}(P, R)$.
2. *Output 1 if exactly one of the* b_i*'s is 1, and output 0 otherwise.*

Let S be the set from which the PIT algorithm samples numbers. Let us recall the failure probability of PIT, on input P and Q. If $P \equiv Q$, then $\Pr(\mathrm{PIT}(P, Q) = 1) = 1$. If $P \not\equiv Q$, then $\Pr(\mathrm{PIT}(P, Q)) \le \deg(P - Q)/|S|$. We next analyze Algorithm 0.1. Let OUT denote the output of Algorithm 0.1. There are 3 cases to consider. For the first case, let us assume that exactly two of the polynomials are identical. By symmetry we may assume that $P \equiv Q \not\equiv R$. Then b_1 always equals 1. Hence Algorithm 0.1 outputs the wrong answer if and only if $b_2 = 1$ or $b_3 = 1$. Thus, the probability of failure is

$$\Pr(OUT = 0) = \Pr(\mathrm{PIT}(Q, R) = 1 \vee \mathrm{PIT}(P, R) = 1) \le \frac{\deg(Q - R) + \deg(P - R)}{|S|},$$

where the above inequality holds by a union bound. Next, we assume that none of the three pairs of polynomials are identical, i.e., that $P \not\equiv Q \not\equiv R \not\equiv P$. Failure occurs if and only if $OUT = 1$. Thus, failure occurs if and only exactly one of b_1, b_2, b_3 is equal to 1. For $i \in \{1, 2, 3\}$ let E_i be the event that only b_i equals 1. Then

$$\begin{aligned}
\Pr(OUT = 1) &= \Pr(E_1 \vee E_2 \vee E_3) \\
&\le \Pr(E_1) + \Pr(E_2) + \Pr(E_3) \\
&\le \Pr(\mathrm{PIT}(P, Q) = 1) + \Pr(\mathrm{PIT}(Q, R) = 1) + \Pr(\mathrm{PIT}(P, R) = 1) \\
&\le \frac{\deg(P - Q) + \deg(Q - R) + \deg(P - R)}{|S|},
\end{aligned}$$

where the first inequality holds by a union bound and the second inequality holds since $E_1 \subseteq \{\mathrm{PIT}(P, Q) = 1\}$, $E_2 \subseteq \{\mathrm{PIT}(Q, R) = 1\}$, and $E_3 \subseteq \{\mathrm{PIT}(P, R) = 1\}$. For the final case, assume that $P \equiv Q \equiv R$. Then it always holds that $b_1 = b_2 = b_3 = 1$. Therefore Algorithm 0.1 always outputs 0 implying that the probability of failure is 0.

To summarize, if the algorithm outputs 0, then it is wrong with probability at most

$$\max\left\{\frac{\deg(P-Q)+\deg(Q-R)}{|S|}, \frac{\deg(P-Q)+\deg(P-R)}{|S|}, \frac{\deg(Q-R)+\deg(P-R)}{|S|}\right\}$$

and if the algorithm outputs 1, then it is wrong with probability at most

$$\frac{\deg(P-Q)+\deg(Q-R)+\deg(P-R)}{|S|}.$$

Exercise 2 Let $L : \{0,1\}^* \to \{0,1\}$ and let M be a randomized algorithm such that

$$\forall x \in \{0,1\}^*\ M(x) \in \{0,1\} \text{ and } \Pr(M(x) = L(x)) \geq \frac{1}{2} + \varepsilon,$$

for some $\varepsilon > 0$. Show that for any $t > 0$, there exists a randomized algorithm M_t, such that

$$\forall x \in \{0,1\}^*\ \Pr(M_t(x) = L(x)) \geq 1 - 2^{-t}.$$

Solution

Fix $t > 0$, and define M_t as follows:

Algorithm 0.2. *Input:* $x \in \{0,1\}^*$.

1. *Execute $M(x)$ k times, for some k to be determined later, where each execution is independent of all other executions.*
2. *Let $b_i \in \{0,1\}$ be the output of the ith execution.*
3. *Output* $\mathrm{maj}(b_1, \ldots, b_k)$.

We now analyze M_t. Let $x \in \{0,1\}^*$ and let X be the number of b_i's that are equal to $L(x)$. Then $X \sim \mathrm{Bin}(k, p)$, for some $p \geq \frac{1}{2} + \varepsilon$, implying that $\mathbb{E}(X) \geq (\frac{1}{2} + \varepsilon)k$. Hence

$$\begin{aligned}
\Pr(M_t(x) \neq L(x)) &= \Pr\left(X < \frac{1}{2}k\right) \\
&\leq \Pr\left(X - \mathbb{E}(X) < \frac{1}{2}k - \left(\frac{1}{2} + \varepsilon\right)k\right) \\
&\leq \Pr(X \leq \mathbb{E}(X) - \varepsilon k) \\
&\leq e^{-\frac{2\varepsilon^2 k^2}{k}} \\
&= e^{-2\varepsilon^2 k},
\end{aligned}$$

where the third inequality is by Chernoff's inequality for a binomial random variable (see Lecture 1). Taking $k = \left\lceil \frac{t \ln 2}{2\varepsilon^2} \right\rceil$ then implies

$$\Pr(M_t(x) = L(x)) \geq 1 - e^{-2\varepsilon^2 k} \geq 1 - 2^{-t}.$$