Exercise Sheet 10: Randomised Computation

David Carral

January 23, 2020
Exercise 1

Exercise. Show that MajSat is in PP.

MajSat = \{ \phi \mid \phi \text{ is some propositional logic formula that is satisfied by more than half of its assignments} \}

Definition. A probabilistic Turing machine (PTM) is a Turing machine with two deterministic transition functions, \( \delta_0 \) and \( \delta_1 \). A run of a PTM is a TM run that uses either of the two transitions in each step.

Definition. A language \( L \) is in Polynomial Probabilistic Time (PP) if there is a PTM \( M \) such that all of the following hold.

- There is a polynomial function \( f \) such that \( M \) will always halt after \( f(|w|) \) steps on all input words \( w \).
- If \( w \in L \), then \( \Pr [M \text{ accepts } w] > \frac{1}{2} \).
- If \( w \notin L \), then \( \Pr [M \text{ accepts } w] \leq \frac{1}{2} \).
Exercise 1

**Exercise.** Show that MajSat is in PP.

\[
\text{MajSat} = \{ \phi \mid \phi \text{ is some propositional logic formula that is satisfied by more than half of its assignments} \}
\]

**Solution.** Let \( M \) be the PTM that performs the following computation on input \( \phi \).

1. We randomly produce an assignment \( I \) for \( \phi \).
2. \( M \) accepts \( \phi \) iff \( I \models \phi \).

Remarks.

- \( M \) runs in polynomial time in the size of the input.
- If \( \phi \in L \), then the probability of producing an assignment \( I \) with \( I \models \phi \) is strictly larger than \( \frac{1}{2} \) (as we are equally likely to produce any assignment). Hence, \( M \) accepts \( \phi \) with probability (strictly) larger than \( \frac{1}{2} \).
- If \( \phi \notin L \), then the probability of producing \( I \) with \( I \models \phi \) is at most \( \frac{1}{2} \). Hence, \( M \) accepts \( \phi \) with probability smaller or equal than \( \frac{1}{2} \).
Exercise 2

**Exercise.** Show $\text{BPP} = \text{coBPP}$.

**Definition.** A language $L$ is in *Bounded-Error Polynomial Probabilistic Time* (BPP) if there is a PTM $M$ such that all of the following hold.

1. There is a polynomial function $f$ such that $M$ will always halt after $f(|w|)$ steps on all input words $w$.
2. If $w \in L$, then $\Pr[M\text{ accepts } w] \geq \frac{2}{3}$.
3. If $w \notin L$, then $\Pr[M\text{ accepts } w] \leq \frac{1}{3}$.

**Remark.**

$$(2) \land (3) \iff \forall w \in \Sigma^*(\Pr[M(w) = L(w)] \geq \frac{2}{3})$$
Exercise 2

**Exercise.** Show $\text{BPP} = \text{coBPP}$.

**Solution.** We show that $\text{coBPP} \subseteq \text{BPP}$.

1. We show that any arbitrarily chosen $L \in \text{coBPP}$ is also in $\text{BPP}$.
2. By (1), $\overline{L} \in \text{BPP}$.
3. By (2), there is a poly-time PTM $M$ with $\Pr[\overline{L}(w) = M(w)] \geq \frac{2}{3}$ for all $w \in \Sigma^*$.
4. Let $M'$ be the PTM that results from exchanging all accepting and rejecting states in $M$.
5. By (3) and (4), $M'$ is poly-time bounded.
6. By (3) and (4), $\Pr[M(w)] \geq \frac{2}{3}$ for all $w \in \overline{L}$. Hence, $\Pr[M'(w)] \leq \frac{1}{3}$.
7. By (3) and (4), $\Pr[M(w)] \leq \frac{1}{3}$ for all $w \notin \overline{L}$. Hence, $\Pr[M'(w)] \geq \frac{2}{3}$.
8. By (6) and (7), $M'$ is a PTM with $\Pr[L(w) = M'(w)] \geq \frac{2}{3}$.
9. By (5) and (8), $L \in \text{BPP}$.

We can make an analogous argument to show $\text{BPP} \subseteq \text{coBPP}$. 
Exercise 3

**Exercise.** Show $\text{BPP}^{\text{BPP}} = \text{BPP}$.

**Theorem 21.14.** Consider a language $L$ and a poly-time PTM $M$ for which there is some $c > 0$ such that $\Pr[M(w) = L(w)] \geq \frac{1}{2} + \frac{1}{|w|^c}$ for all $w \in \Sigma^*$. Then, for all $d > 0$, there is a poly-time PTM $M'$ such that $\Pr[M(w) = L(w)] \geq 1 - \frac{1}{2^{|w|^d}}$.

**Solution.** High-level structure.

- Let $L \in \text{BPP}^O$ for some $O \in \text{BPP}$.
- There is some POTM $M^O$ such that $M^O$ that accepts $L$, $M^O$ has error probability smaller than $1/16$, and $M^O$ is time bounded by some polynomial $p(n)$.
- Starting from $M^O$, we define a polytime PTM $M'$ accepting $L$ with error probability smaller than $\frac{135}{256}$. 
Solution.

1. There is some PTM $\mathcal{N}$ that accepts $O$, has error probability $< 2^{-p(n)}$, and is time bounded by some polynomial $q(n)$.

2. Let $\mathcal{M}'$ be the TM that behaves like $\mathcal{M}$ does, but instead of querying the oracle it calls the machine $\mathcal{N}$ directly.

3. We show that $\mathcal{M}'$ accepts $L$ with error probability of $< \frac{1}{3}$.
   
   3.1 By (1), $\Pr[\mathcal{M}'(w) = L(w)] = \left(1 - \frac{1}{2^{p(|w|)}}\right)^{p(|w|)} \cdot \frac{15}{16}$ for all $w \in \Sigma^*$.
   
   3.2 Proof via induction: $(1 - \frac{1}{2^k})^k \geq \frac{9}{16}$ for all $k \geq 2$.
   
   3.3 By (1) and (2), at least $\frac{9}{16} \cdot \frac{15}{16} = \frac{135}{256} > \frac{1}{2}$ of the computations of $\mathcal{M}'$ are correct.
   
   3.4 Hence, $\mathcal{M}'$ accepts $L$ with error probability smaller than $\frac{135}{256}$.

4. We show that $\mathcal{M}'$ is poly-time bounded.
   
   4.1 On input $w$, $\mathcal{M}'$ makes at most $p(|w|)$ "oracle" calls (i.e., calls to $\mathcal{N}$), each of with input of length at most $p(|w|)$. Hence, this takes time at most $q(p(|w|))$ steps.
   
   4.2 $\mathcal{M}'$ is bounded by $p(n) \cdot q(p(n))$.
   
   4.3 Since $p(n)$ and $q(n)$ are polynomials, $p(n) \cdot q(p(n))$ is also a polynomial.
Exercise 4

**Exercise.** Find the error in the following argument that shows $\text{PP} = \text{BPP}$:

Let $L \in \text{PP}$. Then there exists a poly-time bounded PTM accepting $L$ with error probability smaller than $\frac{1}{2}$. Using error reduction, we can make this error arbitrarily small, and in particular smaller than $\frac{1}{3}$. Hence, $L \in \text{BPP}$.

**Theorem 21.14.** Consider a language $L$ and a poly-time PTM $M$ for which there is some $c > 0$ such that $\Pr [M(w) = L(w)] \geq \frac{1}{2} + \frac{1}{|w|^c}$ for all $w \in \Sigma^*$. Then, for all $d > 0$, there is a poly-time PTM $M'$ such that $\Pr [M'(w) = L(w)] \geq 1 - \frac{1}{2|w|^d}$.

**Solution.** Step by step counter-example.

1. Let $L \in \text{PP}$.
2. There is some PTM $M$ such that $\Pr[M(w) = L(w)] > \frac{1}{2}$ for all $w \in \Sigma^*$ and $M$ is time bounded by some polynomial $p(n)$.
3. It is possible that the $\Pr[M(w) = L(w)] = \frac{1}{2} + \frac{1}{2^p(n)}$ (discuss MajSat).
4. We cannot apply Theorem 21.14 to verify the existence of a machine $M'$ that characterises $L$ with bounded error probability of at most $\frac{1}{3}$. 
Exercise 5

Exercise. Let $\mathcal{M}$ be a polynomial-time PTM. We say that $\mathcal{M}$ has error probability smaller than $\frac{1}{3}$ if and only if, for all $w \in \Sigma^*$, $Pr[\mathcal{M} \text{ accepts } w] < \frac{1}{3}$ or $Pr[\mathcal{M} \text{ accepts } w] \geq \frac{2}{3}$. Show that deciding whether a polynomial-time probabilistic TM has error probability smaller than $\frac{1}{3}$ is undecidable.

Solution. High-level idea.

1. We define a many-one reduction from $E_{TM}$ (i.e., the empty word problem).
2. Let $\mathcal{M}$ be a TM.
3. We construct a 2-tape PTM $\mathcal{N}$ with error probability $< \frac{1}{3}$ iff $\mathcal{M}$ accepts the empty word iff $\langle \mathcal{M} \rangle \in E_{TM}$.

On input $w$, the 2-tape PTM $\mathcal{N}$ performs the following computation.

1. Make a coin flip and reject if the result is heads.
2. Otherwise, simulate $\mathcal{M}$ on the empty word using the working tape for $|w|$ steps.
3. If this simulation accepts, the machine accepts. Otherwise, it rejects.

Discuss: If $\langle \mathcal{M} \rangle \notin E_{TM}$, then $\mathcal{N}$ rejects all inputs.
Exercise 5

**Exercise.** Let $\mathcal{M}$ be a polynomial-time probabilistic Turing machine. We say that $\mathcal{M}$ has *error probability smaller than* $\frac{1}{3}$ if and only if, for all $w \in \Sigma^*$, $\Pr[\mathcal{M} \text{ accepts } w] < \frac{1}{3}$ or $\Pr[\mathcal{M} \text{ accepts } w] \geq \frac{2}{3}$. Show that deciding whether a polynomial-time probabilistic TM has error probability smaller than $\frac{1}{3}$ is undecidable.

**Solution.** On input $w$, the 2-tape PTM $\mathcal{N}$ performs the following computation.

1. Make a coin flip and reject if the result is heads.
2. Otherwise, simulate $\mathcal{M}$ on the empty word using the working tape for $|w|$ steps.
3. If this simulation accepts, the machine accepts. Otherwise, it rejects.

**Discuss:** If $\langle \mathcal{M} \rangle \notin E_{TM}$, then $\mathcal{N}$ rejects all inputs.

We show that if $\langle \mathcal{M} \rangle \in E_{TM}$, then there is some input word $w$ that $\mathcal{N}$ accepts with probability $\frac{1}{2}$.

1. For some $k \geq 0$, the TM $\mathcal{M}$ accepts $\varepsilon$ after $k$ steps.
2. By (1), any word $w$ with $|w| \geq k$ is accepted by $\mathcal{N}$ with probability $\frac{1}{2}$.
3. By (2), the PTM $\mathcal{N}$ does not have error probability $< \frac{1}{3}$.

Since $\mathcal{N}$ can be computed from $\mathcal{M}$, we obtain a reduction from $E_{TM}$ (which is undecidable) to the problem of recognising poly-time PTMs with error probability $< \frac{1}{3}$.
Exercise 6

Exercise. Show that \( \text{NP} \subseteq \text{PP} \).

Solution.

1. Let \( L \in \text{NP} \).
2. There is a poly-time bounded NDTM \( M \) that decides \( L \) such that every state in \( M \) has at most 2 outgoing transitions for the same input.
3. Let \( M' \) be the PTM defined as follows: \( M' \) is identical to \( M \), but instead of choosing an option non-deterministically, it flips a coin and chooses randomly.
4. For all \( w \in L \), \( \Pr [M' \text{ accepts } w] > 0 \).
5. For all \( w \notin L \), \( \Pr [M' \text{ accepts } w] = 0 \).
6. We construct yet another TM \( M'' \) which, on input \( w \), performs the following computation:
   - Toss a coin and accept if the result is heads.
   - Simulate \( M' \) on \( w \). Accept if and only if this simulation accepts.
7. For all \( w \in L \), \( \Pr [M'' \text{ accepts } w] > \frac{1}{2} \).
8. For all \( w \notin L \), \( \Pr [M'' \text{ accepts } w] = \frac{1}{2} \).
9. \( M'' \) is poly-time bounded.
10. By (7-9), \( L \in \text{PP} \).
Exercise 7

**Exercise.** Show the Schwartz-Zippel lemma: Consider a non-zero multivariate polynomial \( f(x_1, \ldots, x_n) \) of total degree \( \leq d \), and a finite set \( S \) of integers. If \( r_1, \ldots, r_n \) are chosen randomly (with replacement) from \( S \), then \( \Pr[f(r_1, \ldots, r_n)] = 0 \leq d \frac{|S|}{|S|} \).

**Solution.**

1. Theorem: A polynomial of degree \( d \) can have at most \( d \) distinct real roots.
2. Proof via induction: we directly proceed with the induction step.
3. We write \( f(x_1, \ldots, x_n) \) as a polynomial in the first variable
   \[
   f(x_1, \ldots, x_n) = x_1^k \cdot c_k(x_2, \ldots, x_n) + \ldots + (x_1^0 \cdot) c_0(x_2, \ldots, x_n)
   \]
   such that \( c_k(x_2, \ldots, x_n) \) is not the zero polynomial.
4. Let \( E_1 \) to be the event “\( c_k(r_2, \ldots, r_n) = 0 \)” . Randomly choose the values of \( r_2, \ldots, r_n \) and assume that \( E_1 \) did not occur.
5. Let \( g(r_1) = f(r_1, r_2, \ldots, r_n) \)
6. Discuss: \( \Pr[g(r_1) = 0 \mid \neg E_1] \leq \frac{k}{|S|} \) (note that \( g \) is a non-zero polynomial).
7. Let \( E_2 \) be the event “\( g(r_1) = 0 \)”, which is equivalent to “\( f(r_1, \ldots, r_n) = 0 \)”. 

Exercise 7

Exercise. Show the Schwartz-Zippel lemma: Consider a non-zero multivariate polynomial $f(x_1, \ldots, x_n)$ of total degree $\leq d$, and a finite set $S$ of integers. If $r_1, \ldots, r_n$ are chosen randomly (with replacement) from $S$, then $\Pr[f(r_1, \ldots, r_n)] = 0 \leq \frac{d}{|S|}$.

Solution.

- $E_1$ is the event “$c_k(r_2, \ldots, r_n) = 0$”
- $E_2$ be the event “$g(r_1) = 0$” (that is, “$f(r_1, \ldots, r_n) = 0$”)
- $\Pr[E_2 \mid \neg E_1] \leq \frac{k}{|S|}$
- Discuss: $\Pr[E_1] \leq \frac{d-k}{|S|}$

$$
\begin{align*}
\Pr[E_2] &= \Pr[E_2 \land E_1] + \Pr[E_2 \land \neg E_1] \\
&\leq \Pr[E_2 \land E_1] + \Pr[E_2 \mid \neg E_1] \cdot \Pr[\neg E_1] \\
&\leq \Pr[E_1] + \Pr[E_2 \mid \neg E_1] \\
&\leq \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}
\end{align*}
$$