Lecture 13

Gidon Rosalki

2025-06-29

This content will not appear in the exam this year!

1 Complexity sets, with randomness

We want to extend the TM model such that we can use random algorithms, which include a runtime. This means that the results of the algorithm can be dependent on random coin flips. We will add to the TM a tape of random coins. At the start of a run, this tape will only include 1 or 0, in every cell, at equal probability, independently in each cell.

We will define the complexity set for this TM machine.

Definition 1.1 (ZPP)**.** *This is the set of all the language L such that they have a TM M that decides L, in an expected time that is polynomial. That is to say, the runtime is on average (by the random coins), it is bound by a polynomial.*

Theorem 1.

$$P \subseteq ZPP$$

Proof . If $L \in P$, then there is a deterministic polynomial TM that decides it. We can add to this machine a coins tape, and so we get a machine that always runs in polynomial time, and thus also runs in expected polynomial time. □

Definition 1.2 (RP)**.** *The set RP contains all the languages L such that there exists a TM M that runs in polynomial time (always). It holds that*

- $w \in L \implies \mathbb{P}\left[M\left(w\right) = q_{acc}\right] \geq \frac{1}{2}$
- $w \notin L \implies \mathbb{P}\left[M\left(w\right) = q_{rej}\right] = 1$

Theorem 2.

$$RP \subseteq NP$$

Proof . We will consider the polynomial recogniser for a language in NP, in comparison to a machine that is RP. In both cases:

- The runtime is polynomial
- If $w \notin L$, then it always holds that $M\left(w\right) = q_{\text{rej}}$
- If $w \in L$ then there is a run such that $M\left(w\right) = q_{\text{acc}}$. In the RP machine, the requirement is that half of the runs will return q_{acc}

Therefore, the RP machine is a specific case of a polynomial recogniser □

Theorem 3. $P \subseteq RP$

Proof . In both cases, the machine runs in polynomial time. In both cases, the machine always responds q_{rej} in the case where $w \notin L$. The machine in P will always return q_{acc} when $w \in L$, and this means it returns q_{acc} more than $\frac{1}{2}$ of the time. □

Definition 1.3 (coRP)**.** *The set coRP contains all the languages L such that $\overline{L} \in RP$. Or, in other words, $L \in coRP$* ***if and only if*** *there exists a TM M for L such that:*

- *M always runs in polynomial time*
- *For every $w \in L$, $M\left(w\right) = q_{acc}$*
- *For every $w \notin L$, it holds that $\mathbb{P}\left[M\left(w\right) = q_{rej}\right] \geq \frac{1}{2}$*

Explanation:

$$\begin{aligned} L \in \text{coRP} &\Leftrightarrow \overline{L} \in \text{RP} \\ &\Leftrightarrow \text{There is an RP machine for } \overline{L} \\ &\Leftrightarrow \text{There is a coRP machine for } L \end{aligned}$$

Where the final transition is possible from swapping the q_{acc} and q_{rej} states.

Theorem 4.

$$RP \cap coRP = ZPP$$

Proof . Below ☐

Definition 1.4. *The set BPP contains all the languages L such that there is a TM M that runs in polynomial time, that correctly answers* $\geq \frac{2}{3}$ *(both ways, both for in and not in)*

This is to say:

$$\begin{aligned} w \in L &\implies \mathbb{P}\left[M\left(w\right) = q_{\text{acc}}\right] \geq \frac{2}{3} \\ w \notin L &\implies \mathbb{P}\left[M\left(w\right) = q_{\text{rej}}\right] \geq \frac{2}{3} \end{aligned}$$

Exercise 1.

$$P \subseteq BPP$$

Solution. In both cases, the machine runs in polynomial time, and a deterministic polynomial machine that decides L will necessarily guarantee that the probability to respond correctly is always greater than $\frac{2}{3}$. ☐

Theorem 5.

$$BPP \subseteq EXP$$

Proof . Let there be $L \in$ BPP, and M a BPP machine for L. We will use M to build M', that decides L in exponential time.
M' will run as follows:
Run over all the options for random coin flips. For every possibility (for a string over $\{0, 1\}$), M' will run $M\left(w\right)$. M' will count how many times it receives q_{acc}, and answer according to the majority.
Correctness: Trivial, since a run over a particular coin tape is deterministic.
Runtime: Every run of $M\left(w\right)$ requires polynomial time. There are 2^l runs, where l is the number of cells on the coin tape. However, since M runs in polynomial time, it can only manage to read at most a polynomial number of coins, which is to say $l \leq poly\left(n\right)$, and so in total the runtime of M' is

$$\leq poly\left(n\right) \cdot 2^{poly(n)}$$

which is to say, limited by an exponential value of n. ☐

Our next theorem is that RP $\subseteq$ BPP. However, we will first show that the size of the mistake is a constant, as small as we would like. We will write $RP\left(p\right)$ like the set RP, but with the one way mistake $\leq p$. Therefore, RP $= RP\left(\frac{1}{2}\right)$

Theorem 6.

$$RP = RP\left(\frac{1}{2}\right) = RP\left(\frac{1}{4}\right)$$

Which is to say $L \in RP$ ***if and only if*** *there is a TM that runs in polynomial time, and enables*

$$\begin{aligned} w \in L &\implies \mathbb{P}\left[M\left(w\right) = q_{acc}\right] \geq \frac{3}{4} \\ w \notin L &\implies \mathbb{P}\left[M\left(w\right) = q_{rej}\right] = 1 \end{aligned}$$

Proof . It is clear that $RP\left(\frac{1}{4}\right) \subseteq RP\left(\frac{1}{2}\right)$. We now need to show that $RP\left(\frac{1}{2}\right) \subseteq RP\left(\frac{1}{4}\right)$: Let there be $L \in RP$, which is to say that there exists a TM M that runs in polynomial tie, and there is a one way failure of probability $\leq \frac{1}{2}$. We will use it to make a TM M' that runs in polynomial time, with one way failure probability $\leq \frac{1}{4}$.
Construction: M' will run as follows: Run $M\left(w\right)$ twice, and return q_{rej} **if and only if** in both runs $M\left(w\right) = q_{\text{rej}}$.
Runtime: Trivial, runtime of M is polynomial, and so too the runtime of M'
Correctness: If $w \notin L$, then it always holds that $M\left(w\right) = q_{\text{rej}}$, and so $M'\left(w\right) = q_{\text{rej}}$. If $w \in L$, then $\mathbb{P}$

$$\begin{aligned} w \notin L &\implies \mathbb{P}\left[M\left(w\right) = q_{\text{rej}}\right] = 1 \implies \mathbb{P}\left[M'\left(w\right) = q_{\text{rej}}\right] = 1 \\ w \in L &\implies \mathbb{P}\left[M\left(w\right) = q_{\text{rej}}\right] \leq \frac{1}{2} \implies \mathbb{P}\left[M'\left(w\right) = q_{\text{rej}}\right] \leq \left(\frac{1}{2}\right)^2 = \frac{1}{4} \end{aligned}$$

☐

So, to return to the theorem we wanted

Theorem 7.

$$RP \subseteq BPP$$

Proof . Through the above theorem:

$$RP = RP\left(\frac{1}{3}\right)$$

Which is to say, theer is a polynomial TM with a one way failure rate that is $\leq \frac{1}{3}$, which is a specific case of a machine BPP, where we can have a two way failures rate of $\leq \frac{1}{3}$. ☐

Theorem 8.

$$coRP \subseteq BPP$$

Proof .

Theorem 9. *BPP is closed to inverse, which is to say BPP = coBPP.*

Proof . By swapping the states q_{acc} and q_{rej}, on a BPP machine, we get a BPP machine for the inverse language ☐

So from that helpful theorem, we can now show:

$$\begin{aligned} L \in coRP &\implies \overline{L} \in RP \\ &\implies \overline{L} \in BPP \\ &\implies L \in BPP \end{aligned}$$

☐

What about NP?

$$P \subseteq ZPP \subseteq RP \subseteq NP \subseteq EXP$$

We are left with the theorem that we did not prove earlier:

Theorem 10.

$$RP \cap coRP = ZPP$$

Proof . We will assume that $L \in RP \cap coRP$, and show that $L \in ZPP$. That is to say that there is an RP machine for L, and that there is a coRP machine for L. Both machines run in polynomial time, both with a (different) one way failure rate.

	M_1	M_2
$w \in L$	$\mathbb{P}[M_1(w) = q_{\text{acc}}] \geq \frac{1}{2}$	$\mathbb{P}[M_2(w) = q_{\text{acc}}] = 1$
$w \notin L$	$\mathbb{P}[M_1(w) = q_{\text{rej}}] = 1$	$\mathbb{P}[M_2(w) = q_{\text{rej}}] \geq \frac{1}{2}$

Table 1:

We want to show with M_1 and M_2 to create M which is a ZPP machine for L. This is to say, **always** responds correctly. The runtime of M has the expected runtime of polynomial (by the coins).
Construction: M will run as follows:

1. Run $M_1(w)$. If M_1 responds q_{acc}, then return q_{acc}
2. Run $M_2(w)$. If M_2 responds q_{rej}, then return q_{rej}
3. Return to (1)

Correctness: If in some step, $M_1(w) = q_{\text{acc}}$, then necessarily $w \in L$, and therefore the response of M is correct. If in some step $M_2(w) = q_{\text{rej}}$, then necessarily $w \notin L$, and therefore the response of M is correct.
Runtime: We will assume that $w \in L$. The runtime of M is the runtime of both the machines, times the number of times that $M_1(w)$ will return q_{rej}. We will use i to mark the number of times that this occurred.

$$\mathbb{P}[M(w) = q_{\text{rej}}] \leq \frac{1}{2}$$

Therefore

$$\mathbb{P}[\#(M(w) = q_{\text{rej}}) = i] \leq \left(\frac{1}{2}\right)^i$$

and so the expected runtime is

$$\leq \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i \cdot poly\left(n\right) \cdot i = \theta\left(1\right) \cdot poly\left(n\right)$$
$$= poly\left(n\right)$$

So we have shown that $L \in RP \cap coRP \implies L \in ZPP$.

We will now show

$$L \in ZPP \implies L \in RP \cap coRP$$

We will begin from $L \in ZPP \implies L \in RP$. That is to say, there is a TM M that decides L in polynomial time (on average), which we can use to build a TM M_1 that always runs in polynomial time, with a one way failure rate $\leq \frac{1}{2}$. To resolve this, we will recall Markov's inequality. For some non negative random variable X,

$$\mathbb{P}\left[X > a \cdot \mathbb{E}\left[X\right]\right] \leq \frac{1}{a}$$

We will build M_1 as follows: M_1 will run $M\left(w\right)$ with a counter for the number of steps, and will stop the run should it require more than $2 \cdot \mathbb{E}\left[\#\left(\text{number of steps}\right)\right]$. If M stopped before this, M_1 will return its response, and if M does not stop, then M_1 will return q_{rej}.
Runtime: The runtime of M_1 is 2 times the expected value of the runtime of M, and so is polynomial in n.
Correctness:

$$w \notin L \implies \mathbb{P}\left[M_1\left(w\right) = q_{\text{rej}}\right] = 1$$

If $w \in L$, then M_1 responds correctly **if and only if** $M\left(w\right)$ finishes running in time $\leq 2\cdot$ the expected value, which is to say that M responds incorrectly **if and only if** the runtime of $M\left(w\right) > 2 \cdot \mathbb{E}$. According to Markhov's inequality, this happens with a probability $\leq \frac{1}{2}$. This is to say, if $w \in L$, then

$$\mathbb{P}\left[M'\left(w\right) = q_{\text{acc}}\right] \geq \frac{1}{2}$$

We have finished showing that $ZPP \subseteq RP$. We need to show that $ZPP \subseteq coRP$, and then derive that $ZPP \subseteq RP \cap coRP$. In order to show that $ZPP \subseteq coRP$ we will build a coRP machine M_2 . The construction is almost exactly the same as M_1, but instead if we stop the machine for counting too high, then M_2 will return q_{acc} $\square$