Indian Association for the Cultivation of Science

(Deemed to be University under *de novo* Category)

Master's/Integrated Master's-PhD Program/ Integrated Bachelor's-Master's Program/PhD Course

Theory of Computation II: COM 5108

Lecture IV

Instructor: Goutam Biswas *Autumn Semester 2023*

1 Randomized Computation

A Turing machine model is augmented with the capability of making random choice (flip a coin) of transition during computation.

1.1 Probabilistic Turing Machine

A *probabilistic Turing machine* is a mathematical model for *randomized algorithms*. This machine is structurally similar to a non-deterministic machine. But their computations are very different.

A class of randomized algorithms (and the corresponding machine model) may give erroneous results. But the probability of error can be made very low (as low as the probability of software or hardware failure or the probability of some other catastrophic event). These are known as *Monte Carlo* algorithms. Another class of algorithms give correct result on termination. But the termination is not guaranteed or bounded by specified time e.g. polynomial. But its expected running time is "good" (polynomial). These are known as *Las Vegas* algorithms. In case of *Monte Carlo* decision algorithms the error may be one sided (say for positive results) or may be both sided (for both positive and negative results).

Randomness is introduced in a Turing machine model essentially in two different ways. The machine may have a pair of transition functions that are selected uniformly at random from each configuration. The other ways is to introduce a tape contains a sequence of random bits. The machine is essentially deterministic and takes the input and the random bits into consideration for transition. A more formal definition of the first kind of machine is as follows.

Definition 1. A *probabilistic Turing machine (PTM) M* has two transition functions δ_0 and δ_1. At each step of computation M "flips a fair coin" and chooses one of them with equal probability $(1/2)$ to go to the next configuration. The choice at any state is independent of the previous choices.
Finally the machine halts either in *accept (output 1)* or in *reject (output 0)*

state. A random variable $M(x)$ (x is the input) is associated with with the output of the machine. We talk about $Pr[M(x) = 1]$ and $Pr[M(x) = 0]$.
If the machine halts within $T(|x|)$ time on all inputs $x \in \{0,1\}^*$, and irrespective of the outcome of coin toss, we call it $T(n)$-time bounded, where $n = |x|$.

If a PTM is running for t steps, the computation tree will have 2^t branches. Each branch will be taken with a probability $1/2^t$. The probability of acceptance of an input x is the fraction of branches where M finally writes 1 as output i.e. $Pr[M(x) = 1]$.

Let $L \subseteq \{0,1\}^*$. We use the notation $L(x) = 1$ if $x \in L$, and $L(x) = 0$ if $x \notin L$. We define the first time bounded probabilistic complexity class.

1.2 One-Sided Error: RP

Definition 2. A language $L \subseteq \{0,1\}^*$ is in the class $RTIME(T(n))$ if there is a $T(n)$ ($T : \mathbb{N}_0 \to \mathbb{N}_0$) time bounded probabilistic Turing machine (PTM) M, so that

$$\begin{aligned} x \in L &\Rightarrow Pr[M(x) = 1] \geq 2/3, \\ x \notin L &\Rightarrow P[M(x) = 1] = 0. \end{aligned}$$

There is one sided error. If $x \notin L$, then no branch of computation *accepts* x. But if $x \in L$, some branches of computation may *reject* x. If $M(x) = 1$, then $x \in L$. But if $M(x) = 0$, then with some probability ($\leq \frac{2}{3}$) that $x \in L$. The value $2/3$ is rather arbitrary. It can be replaced by a value $\geq 1/2$.

The *randomized polynomial* time complexity class $\mathbf{RP} = \bigcup_{i>0} RTIME(n^i)$. A language L is in **RP** if there is polynomial time bounded PTM M with one sided error mentioned above.

Example 1. Following algorithm to decide $COMPOSITE = \{n \in \mathbb{N} : n \text{ is a composite number}\}$ though runs in polynomial time, has one sided error. It uses *Fermat Test*. According to the Fermat's Little Theorem, if p is a prime and $p \not| a$, then $a^{p-1} \equiv 1 \pmod{p}$. The contrapositive statement is, if $\gcd(a, n) = 1$ and $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.

isCompositeFT1(n)
  `if` $n = 1, 2$ `return 0`
  $a \leftarrow \text{rand}\{2, \cdots n-2\}$
  `if` $(a^{n-1} \bmod n) \neq 1$ `return` 1 // composite
  `else return` 0 // most likely prime, a pseudo prime

If the procedure returns 1 i.e. $(a^{n-1} \bmod n) \neq 1$, then n is certainly composite. But if it returns 0, there is no certainty[1].

$$\begin{aligned} x \in \text{COMPOSITE} &\Rightarrow Pr[M(x) = 1] \geq ??, \\ x \notin \text{COMPOSITE} &\Rightarrow P[M(x) = 1] = 0. \end{aligned}$$

If $L \in \mathbf{RP}$ and $x \in L$, according to the definition of **RP** there are more than $2/3$ branches of *accepting* computation of a polynomial time bounded PTM M. Treating the **RP** machine as an NTM, one accepting branch is sufficient to accept x. Therefore $\mathbf{RP} \subseteq \mathbf{NP}$.

[1] $2^{340} \equiv 1 (\text{mod } 341)$ and $341 = 11 \times 31$. And there are those composite Carmichael numbers n, such that for every $a \in \mathbb{Z}_n^*$, $a^{n-1} \equiv 1 (\text{mod } n)$. It passes the Fermat test.

Definition 3. A language $L \subseteq \{0,1\}^*$ is in the class **coRP** if there is a polynomial time bounded PTM M such that

$$\begin{aligned} x \in L &\Rightarrow Pr[M(x) = 0] = 0, \\ x \notin L &\Rightarrow P[M(x) = 0] \geq 2/3. \end{aligned}$$

In this case if the output is 0, then we are certain that $x \notin L$. But if the output is 1 we are not sure. In fact $\mathbf{coRP} = \{L : \overline{L} \in \mathbf{RP}\}$.

1.2.1 Primality: a randomized algorithm

There are composite numbers called the *Carmichael numbers* for which the *Fermat Test* fails for all elements of $\mathbb{Z}_n^* = \{m \in \mathbb{N} : \gcd(m,n) = 1\}$. The smallest Carmichael number is $561 = 3 \times 11 \times 17$. For all elements of $\mathbb{Z}_{561}^* = \{1, 2, 4, 5, \cdots, 560\}$, $2^{560} \equiv 4^{560} \equiv 5^{560} \equiv \cdots \equiv 1 (\text{mod } 561)$. So there is no Fermat witness (of n is composite) in $\mathbb{Z}_{561}^*$. Following algorithm uses another test along with the Fermat test to decide the primality of a positive integer with high probability.

PRIME: input $n \in \mathbb{N}$

1. If n is even, then *accept* if $n = 2$; otherwise *reject*.
2. Select $a_1, \cdots, a_k$ from $\mathbb{Z}_n^+ = \{1, \cdots, n-1\}$.
3. For each $i = 1, \cdots, k$ do the following:
   (a) Compute $a_i^{n-1} \bmod n$. *Reject* if the value is $\neq 1$.
   (b) Compute the sequence $t_0, \cdots, t_l$, where $n - 1 = s \cdot 2^l$, s is odd, and $t_j = (a_i^s \times a_i^{2^j}) \bmod n$, for $j = 0, \cdots, l$.
   (c) If some element of the sequence is not 1. Find the last element of the sequence that is not 1. If that element is not (-1), reject it.
4. *Accept* n as prime.

Lemma 1. There are two solutions of $x^2 \equiv 1 (\text{mod } n)$ if n is a prime.
Proof: Two solutions of $x^2 \equiv 1 (\text{mod } n)$ are $x \equiv \pm 1 (\text{mod } n)$ $(-1 \equiv n - 1 (\text{mod } n))$.
Suppose $x \not\equiv \pm 1 (\text{mod } n)$, then $x^2 \equiv 1 (\text{mod } n) \Rightarrow (x^2 - 1) \equiv 0 (\text{mod } n) \Rightarrow (x-1)(x+1) \equiv 0 (\text{mod } n)$.
As x are not ± 1, $0 < (x-1), (x+1) < n$. But a prime number cannot divide the product of two smaller positive numbers $(x-1)$ and $(x+1)$ - a contradiction. So ± 1 are only two square roots of 1 modulo n. QED.
Lemma 2. A composite number n may have more than two (other than ± 1) solutions of $x^2 \equiv 1 (\text{mod } n)$. Carmichael numbers have at least three prime factors and they are *square free*. So they have at least 8 square roots of 1 modulo n.
Example 2. $\mathbb{Z}_{12}^+ = \{1, \cdots, 11\}$, solutions of $x^2 \equiv 1 (\text{mod } 12)$ are $x \equiv 1, 5, 7, 11 (\text{mod } 12)$.
The first Carmichael number $561 = 3 \times 11 \times 17$. There are two solutions for $x^2 \equiv 1$ for each prime factor of 561. $\{1, 2\}$ for 3, $\{1, 10\}$ for 11 and $\{1, 16\}$ for 17.
Taking one from each one of them and using the *Chinese Remainder theorem*

(CRT) we can get eight solutions of $x^2 \equiv 1(\text{mod } 561)$.
If we take $x \equiv 1(\text{mod } 3)$, $x \equiv 10(\text{mod } 11)$ and $x \equiv 1(\text{mod } 17)$ and use CRT we get the solution 307. So $(307)^2 \equiv 1(\text{mod } 561)$.
Example 3. If $n = 561$ is the input to PRIME, no element of $\mathbb{Z}^*_{561}$ is a composite-witness. But in $3(a), (b)$ we do the following computation with the witness 2. We have $561 - 1 = 560 = 2^4 \cdot 35$.

$$\begin{aligned} & 2^{35} \equiv 263(\text{mod } 561) \\ \Rightarrow \quad & 2^{70} \equiv 166(\text{mod } 561) \\ \Rightarrow \quad & 2^{140} \equiv 67(\text{mod } 561) \\ \Rightarrow \quad & 2^{280} \equiv 1(\text{mod } 561) \end{aligned}$$

So $(\pm 67)^2 \equiv 1(\text{mod } 561)$. Input 561 will be rejected at 3(c).
Lemma 3. If n is a prime number $Pr[\text{PRIME } \textit{accepts } n] = 1$.
Proof: If n is a prime, there is no *witness* for rejection at $3(a)$ - Fermat's theorem. As the test is passed, $a^{n-1} \equiv 1(\text{mod } n)$.
So a may be a witness for $3(c)$. There may be some $t \not\equiv \pm 1(\text{mod } n)$. But we have already proved that for a prime n this is impossible. QED.
Lemma 4. If n is an odd composite number, $Pr[\text{PRIME } \textit{accepts } n] \leq \frac{1}{2^k}$.
Proof: We show that if n is an odd composite and an $a \in \mathbb{Z}^+_n$ is picked at random, then $Pr[a \textit{ is a witness }] \geq \frac{1}{2}$. It is so because no less than half of the elements of $\mathbb{Z}^+_n$ are stage 3(c) witness that n is a composite number.

Let n be an odd composite number and the randomly selected a in (2) is not a stage 3(a) or stage 3(c) witness. The sequence of values of 3(b) can be any one of the following two types.

(i) All are 1's e.g. $a = 1$

(ii) (-1) at some position followed by 1's e.g. $a = -1$, $(-1)^s = -1$ as s is odd and $(-1)^{2s} = 1$.

Non-witnesses of type (ii) generate (-1) at some position of the sequence. Let j be the largest among these positions and h is a non-witness that generates a (-1) at the position j i.e. $2^{s \cdot 2^j} \equiv -1(\text{mod } n)$.
The composite number n is either a power of a prime or a product of two positive integers q and r so that $\gcd(q, r) = 1$.
We consider the second case first. The simultaneous congruence $x \equiv h(\text{mod } q)$ and $x \equiv 1(\text{mod } r)$ has a solution t (CRT) i.e. $t \equiv h(\text{mod } q)$ and $t \equiv 1(\text{mod } r)$. This implies $t^{s \cdot 2^j} \equiv h^{s \cdot 2^j} \equiv -1(\text{mod } q)$ and $t^{s \cdot 2^j} \equiv 1(\text{mod } r)$. So $t^{s \cdot 2^j} \not\equiv \pm 1(\text{mod } n)$, but $t^{s \cdot 2^{j+1}} \equiv 1(\text{mod } n)$.
So t is a witness at 3(c).
Let d be a non-witness, implies that $d^{s \cdot 2^j} \equiv 1 \text{ or } -1(\text{mod } n)$ and $d^{s \cdot 2^{j+1}} \equiv 1(\text{mod } n)$ (the way j was chosen).
Then we have $(dt)^{s \cdot 2^j} \not\equiv \pm 1(\text{mod } n)$, but then $(dt)^{s \cdot 2^{j+1}} \equiv 1(\text{mod } n)$. So $(d \cdot t)$ is a witness.

Let d_1 and d_2 be two such distinct non-witness. We claim that $d_1 t \not\equiv d_2 t(\text{mod} n)$.

Suppose $d_1 t \equiv d_2 t (\mathrm{mod} n)$. We know that $t^{s \cdot 2^{j+1}} \equiv 1 (\mathrm{mod}\ n)$. Then

$$\begin{aligned} & d_1 \\ \equiv\ & d_1 (t^{s \cdot 2^{j+1}}) \\ \equiv\ & (d_1 t) \cdot t^{(s \cdot 2^{j+1} - 1)} \\ \equiv\ & (d_2 t) \cdot t^{(s \cdot 2^{j+1} - 1)} \\ \equiv\ & d_2 \cdot (t^{s \cdot 2^{j+1}}) \\ \equiv\ & d_2 (\mathrm{mod}\ n). \end{aligned}$$

The conclusion is the number of witnesses are as large as the number of non-witnesses in case of n not a power of a prime.

Let $n = p^e$, $e > 1$. Take $t = 1 + p^{e-1}$.

$$t^n = (1 + p^{e-1})^n = 1 + n \cdot p^{e-1} + \text{terms with higher powers of } p^{e-1}.$$

So $t^n \equiv 1 (\mathrm{mod}\ n)$. But then $t^{n-1} \not\equiv \pm 1 (\mathrm{mod}\ n)$ as $t^{n-1} \equiv \pm 1 (\mathrm{mod}\ n)$ will make $t^n \equiv t (\mathrm{mod}\ n)$. So t is a 3(a) witness.
Take a non-witness d, $d^{n-1} \equiv 1 (\mathrm{mod}\, n)$ and we get dt as a witness. For distinct non-witness d_1 and d_2 we get distinct witness $d_1 t$ and $d_2 t$. Suppose $d_1 t \equiv d_2 t (\mathrm{mod} n)$.

$$\begin{aligned} & d_1 \\ \equiv\ & d_1 \cdot t^n \\ \equiv\ & d_1 \cdot t \cdot t^{n-1} \\ \equiv\ & d_2 \cdot t \cdot t^{n-1} \\ \equiv\ & d_2 \cdot t^n \\ \equiv\ & d_2 (\mathrm{mod}\ n). \end{aligned}$$

QED.

1.3 Two-Sided Error: BPP

In **RP** we have error in *one side* of the output. Following class allows both-sided error.

Definition 4. The class **BPTIME**$(T(n))$ is the collection of languages decided by some PTM in time $T(n)$ such that $Pr[M(x) = L(x)] \geq 2/3$ (**BPTIME** means, *bounded-error probabilistic* $T(n)$ *time*).
The class **BPP** (*bounded-error probabilistic polynomial-time*) is the class of languages decided by probabilistic polynomial-time turing machine with bounded error, **BPP** $= \cup_{i \in \mathbb{N}}$ **BPTIME**(n^i).

The definition says that the machine outputs the correct membership status of x and L with a probability larger than $2/3$. The choice of $2/3$ is arbitrary.
From the symmetry of the definition it is clear that **BPP** is closed under complementation i.e. **BPP** = **coBPP**.

A deterministic Turing machine may be viewed as special case of a PTM. So **P** $\subseteq$ **BPP**. The open question is whether **BPP** = **P**. Many people believe that they are i.e. every polynomial time, bounded error, probabilistic algorithm can be transformed to a polynomial time deterministic algorithm with only polynomial slowdown. This is an open question in complexity theory.

Following is an alternative definition of the class **BPP** using a polynomial time bounded DTM V, a verifier, and a polynomial length sequence of random bits[2].

Definition 5. A language $L \subseteq \{0,1\}^*$ is in **BPP**, if there is a polynomial-time Turing machine M and a polynomial $p(n)$ so that for every $x \in \{0,1\}^*$,

$$Pr_{r \in \{0,1\}^{p(|x|)}}[M(x,r) = L(x)] \geq 2/3.$$

Here the probability is over the sequence of random bits r. First we show that this definition is equivalent to the first definition.
Let $L \in$ **BPP** according to the first definition. There is a polynomial ($p(n)$) time bounded PTM M and $Pr[M(x) = L(x)] \geq 2/3$.
So with $2/3$ probability we find a polynomial length choice sequence $r \in \{0,1\}^{p(|x|)}$ of M so that $M(x) = L(x)$. We can construct a DTM M' that will simulate M on x and using the choice sequence w reach $L(x) = M(x) = M'(x,w)$.
Let $L \in$ **BPP** according to the second definition. There there is a polynomial ($p()$) length random string w and a DTM M' so that $M(x,w) = L(x)$ with probability $2/3$. We design a PTM M that randomly generates w of length $p(|x|)$ and simulates $M'(x,w)$ so that $Pr[M(x) = L(x)] = Pr[M'(x,w) = L(x)] \geq 2/3$.

The definition tells us that **BPP** $\subseteq$ **EXPTIME**. As for every $p(n)$ the number of random bit-strings is $2^{p(n)}$. The exponential machine can enumerate them and simulate the deterministic machine. So we have **P** $\subseteq$ **BPP** $\subseteq$ **EXPTIME**. Little else is known about inclusion relation of this class.

1.4 Zero Error: ZPP

There are randomized algorithms that always gives correct result after termination, but may fail to terminate within the desired time.

Definition 6. Let M be a PTM. We define a random variable $T_{M,x}$, for the running time of M on input x. So $Pr[T_{M,x} = t] = p$, if M halts on x within t steps with a probability p, over the random choices made by M. It is said that the **expected running time** of M is $T(n)$, if $\mathbb{E}[T_{M,x}] \leq T(|x|)$ for every $x \in \{0,1\}^*$.

Definition 7. The class $ZTIME(T(n))$ is the collection languages L for which there is PTM M such that on every input x its *expected run-time* is $O(T(n))$. But when it halts, $M(x) = L(x)$.

The class **ZPP** ("zero-sided" error) is the collection of languages L, such that for each L there is a PTM M whose expected running time is bounded by a polynomial $p(|x|)$, for every $x \in \{0,1\}^*$. But when it halts, $M(x) = L(x)$.

There is an alternate way of looking at it. $L \in$ **ZPP** if there is a polynomial time bounded PTM M such that

1. $M(x) \in \{0, 1, \text{`}unknown\text{'}(\perp)\}$,
2. if $x \in L$, then $M(x) = 1$ or $\perp$,
3. if $x \notin L$, then $M(x) = 0$ or $\perp$,
4. $Pr[M(x) = \perp] \leq 1/2$.

[2]In case of **NP** we replaced the NTM by a DTM verifier with a second input as a *witness*. In case of **BPP** a PTM is replaced by a DTM and a sequence of *random bits*.

Example 4. An example of such an algorithm (not a decision problem) is finding the square-root of -1 modulo a prime p of the form $4k+1$. As an example $p = 13 = 3 \cdot 4 + 1$. We want to solve the quadratic congruence $x^2 \equiv -1 (\text{mod } 13)$[3]. One value of x is 5, as $13|(5^2+1)$.

We want to find an element $a \in \mathbb{Z}_p^*$ so that $a^2 \equiv -1 (\text{mod } p)$. If we can find an element $b \in \mathbb{Z}_p^* \setminus (\mathbb{Z}_p^*)^2$, we may take $a = b^{\frac{p-1}{4}}$, as $a^2 \equiv (b^{\frac{p-1}{4}})^2 = b^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$ (Euler's criterion)[4].

We know that half of the elements of $\mathbb{Z}_p^*$ are quadratic non-residue[5]. So we can use the following randomized algorithm.

sqrt-1(p)
    `do`
        $b \leftarrow rand\{1, \cdots, p-1\}$
        $a \leftarrow b^{(p-1)/4}$
    `while` $(a^2 \bmod p \neq p-1)$
    `return` a

The probability of picking a quadratic non-residue is $\frac{1}{2}$. So the expected number of times the loop is executed is 2. The probability that the algorithm has not found a quadratic non-residue after k iterations is $1/2^k$. The algorithm when terminates gives the correct a. But its running time is a *random variable* and its expected value is bounded. This type of algorithms are known as *Las Vegas algorithm*.

Proposition 1. $\mathbf{RP} \cup \mathbf{coRP} \subseteq \mathbf{BPP}$

Proof: Let the language $L \subseteq \{0,1\}^*$ be in **RP**. There is a polynomial time PTM M so that for all $x \in \{0,1\}^*$,

- if $x \in L$ i.e. $L(x) = 1$, then $Pr[M(x) = 1] \geq 2/3$,
- if $x \notin L$ i.e. $L(x) = 0$, then $Pr[M(x) = 0] = 1$

So we have $Pr[M(x) = L(x)] \geq 2/3$ i.e. $L \in \mathbf{BPP}$. Similarly we prove that $\mathbf{coRP} \subseteq \mathbf{BPP}$. QED.

Proposition 2. $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{coRP}$.

Proof: We prove that $\mathbf{ZPP} \subseteq \mathbf{RP}$: Let $L \in \mathbf{ZPP}$. So there is a PTM M with expected running time bounded by a polynomial $p(n)$ such that $M(x) = L(x)$ on termination.

We design a polynomial time bounded PTM N such that N works as follows:

1. N simulates M for $3p(n)$ (3 times expected running time of M).

[3]Let p be an odd prime and a is an integer so that $\gcd(a,p) = 1$. If the quadratic congruence $x^2 \equiv a (\text{mod } p)$ has a solution, then a is called a *quadratic residue* of p. Otherwise it is a *quadratic non-residue* of p. When p is an odd prime then a is a *quadratic residue* of p if $a^{(p-1)/2} \equiv 1 (\text{mod } p)$ and it is a *quadratic non-residue* of p if $a^{(p-1)/2} \equiv -1 (\text{mod } p)$ (Euler's theorem).

[4]Let $p = 13$, $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$, $(\mathbb{Z}_{13}^*)^2 = \{1,3,4,9,10,12\}$. So $\mathbb{Z}_{13}^* \setminus (\mathbb{Z}_{13}^*)^2 = \{2,5,6,7,8,11\}$. Take $b = 5$, $a = 5^{(13-1)/4} = 5^3$ and $a^2 \equiv ((5^3))^2 \equiv 8^2 \equiv -1 (\text{mod } 13)$.

[5]Let $p = 13$, consider a generator of $\mathbb{Z}_{13}^*$, say 2, $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12, 2^7 \equiv 11, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10, 2^{11} \equiv 7, 2^{12} \equiv 1$. All even powers of 2 are *quadratic residues* e.g. $2^4 = (2^2)^2 = 3$. So the solution of $x^2 \equiv 3 (\text{mod } 13)$ is $2^2 = 4$. Odd powers are *quadratic non-residue* e.g. $2^9 \equiv 5$. $5^{(13-1)/2} = 5^6 \equiv 12 \equiv -1$.

2. Return $M(x)$ on termination.

3. Return 0 if the simulation does not terminate within that time.

Probability of the simulation running beyond $3p(n)$ is $\frac{1}{3}$ (Markov's inequality). We have the following behavior of N:

1. If $x \in L$: the simulation of M terminates with $M(x) = 1$. Otherwise the simulation of M does not terminate and N returns 0, which is incorrect, but with probability $< \frac{1}{3}$.

2. If $x \notin L$, N returns 0 irrespective of whether the simulation terminates or not.

So we have $x \notin L \Rightarrow Pr[N(x) = 0] = 1$ and $x \in L \Rightarrow Pr[N(x) = 1] \geq \frac{2}{3}$. So $L \in \mathbf{RP}$.

Similarly we can design a polynomial time PTM N' as follows.

2. Return 1 if the simulation does not terminate within that time.

We have the following behavior of N':

1. If $x \notin L$: the simulation of M terminates with $M(x) = 0$. Otherwise the simulation of M does not terminate and N' returns 1, which is incorrect, but with probability $< \frac{1}{3}$.

2. If $x \in L$, N returns 1 irrespective of whether the simulation terminates or not.

So we have $x \in L \Rightarrow Pr[N(x) = 1] = 1$ and $x \notin L \Rightarrow Pr[N(x) = 0] \geq \frac{2}{3}$, so the $L(N') = L \in \mathbf{coRP}$. We conclude that $\mathbf{ZPP} \subseteq \mathbf{RP} \cap \mathbf{coRP}$.

In the other direction, we prove that $\mathbf{RP} \cap \mathbf{coRP} \subseteq \mathbf{ZPP}$. Let $L \in \mathbf{RP} \cap \mathbf{coRP}$. There are two polynomial time bounded PTM M_1 for $L \in \mathbf{RP}$ and M_2 for $L \in \mathbf{coRP}$. We construct a PTM N as follows:

N: input x

1. Simulate M_1 on x.

2. If $M_1(x) = 1$, then x must belong to $L \in \mathbf{RP}$, *return 1.*

3. If $M_1(x) = 0$, simulate M_2 on x.

4. If $M_2(x) = 0$, then $x \notin L \in \mathbf{coRP}$, *return 0.*

5. If $M_2(x) = 1$, *return* '$\perp$'. The error probability is less than $\frac{1}{3}$.

The expected running time is bounded by the running time of M_1 and M_2. So $L \in \mathbf{ZPP}$. QED.

1.5 Error Reduction in RP

Let $L \in \mathbf{RP}$. We have a polynomial time ($p()$) PTM M so that

$$\begin{aligned} x \in L &\Rightarrow Pr[M(x) = 1] \geq 2/3, \\ x \notin L &\Rightarrow P[M(x) = 1] = 0. \end{aligned}$$

Consider the following machine where $q()$ is a polynomial.

M_e : input x

(i) Run M on x for $q(|x|)$ number of times.

(ii) The output is disjunction of $q(|x|)$ output.

If $M_e(x) = 1$ then certainly $x \in L$ as at least once $M(x) = 1$.
If $M_e(x) = 0$ (all outputs are zero), then the probability that $x \in L$ is $\frac{1}{3^{q(|x|)}}$, rather small. There cannot be any error if $x \notin L$. Therefore

$$\begin{aligned} x \in L &\Rightarrow Pr[M(x) = 1] \geq 1 - \left(\frac{1}{3}\right)^{q(|x|)}, \\ x \notin L &\Rightarrow P[M(x) = 1] = 0. \end{aligned}$$

1.6 Error Reduction in BPP

For the class **BPP** $Pr[M(x) = L(x)] \geq \frac{2}{3}$. Again this $\frac{2}{3}$ is arbitrary. Following lemma states that it is good enough to have $Pr[M(x) = L(x)] = 1/2 + 1/n^c$, where $|x| = n$ and $c > 0$ is a constant.

Definition 8. $\mathbf{BPP}_{1/2+1/n^c}$ is a class of languages. If $L \in \mathbf{BPP}_{1/2+1/n^c}$, then there is a polynomial time bounded PTM M such that for each $x \in \{0,1\}^*$, $Pr[M(x) = L(x)] \geq 1/2 + 1/n^c$.

Lemma 5. $\mathbf{BPP}_{1/2+1/n^c} = \mathbf{BPP}$.

It is clear that $\mathbf{BPP} \subseteq \mathbf{BPP}_{1/2+1/n^{-c}}$. We have to prove the other direction i.e. given a polynomial time PTM M with success probability $\frac{1}{2} + \frac{1}{n^c}$, we can construct a polynomial time PTM M' with success probability $2/3$. Following theorem proves a stronger result.

Theorem 6. Let there be a polynomial time bounded PTM M for the language $L \subseteq \{0,1\}^*$, so that for all $x \in \{0,1\}^*$, $Pr[M(x) = L(x)] \geq \frac{1}{2} + \frac{1}{n^c}$. Then for each $d > 0$, there is a polynomial time PTM M', such that for all $x \in \{0,1\}^*$, $Pr[M(x) = L(x)] \geq 1 - \frac{1}{2^{n^d}}$.

Proof: Let the machine M' runs M on every input $x \in \{0,1\}^*$ for $k = 8n^{2c+d}$ number of times. Corresponding k outputs are $o_1, \cdots, o_k \in \{0,1\}$. The value of $M'(x) = 1$ if the *majority* is 1; else it is 0.
We use *Chernoff bound* to show that $L \in \mathbf{BPP}_{1-1/(2^{n^d})}$.

For every $i = 1, \cdots, k$, we define a boolean random variable X_i so that $X_i = 1$ if $o_i = L(x)$, else it is 0. The random variables are independent. The expected value of X_i, $E[X_i] = Pr[X_i = 1] = \rho \geq p = \frac{1}{2} + \frac{1}{n^c}$.
Let $X = \sum_{i=1}^{k} X_i$, $\mathbb{E}[X] = \sum_{i=1}^{k} \mathbb{E}[X_i] = k\rho \geq kp$.

The PTM M' makes a mistake when the majority of answers of the runs of PTM M are wrong i.e. $X < \frac{k}{2}$. We need to find $Pr[X < \frac{k}{2}]$.

According to Chernoff bound, sufficiently small δ, $0 < \delta < 1$,

$$Pr\left[X < (1-\delta)\mathbb{E}[X]\right] \leq e^{-\frac{\delta^2 pk}{4}},$$

We have $p = 1/2 + |x|^{-c}$ and we take $\delta = |x|^{-c}/2$. If we output the majority answer, $X \geq (1-\delta)\mathbb{E}[X]$, the probability of wrong output is bounded by

$$e^{-\frac{\delta^2}{4}pk} = e^{-\frac{1}{4|x|^{2c}}\cdot(\frac{1}{2}+\frac{1}{|x|^c})\cdot 8|x|^{2c+d}} \leq 2^{-|x|^d}.$$

QED.

1.7 BPP and Other Classes

Theorem 7. BPP $\subseteq$ P/poly
Proof: Suppose $L \in$ **BPP**. There is a polynomial time PTM M' so that for every $x \in \{0,1\}^*$, $Pr[M'(x) = L(x)] \geq 2/3$.
By error reduction we claim the following:
For every $d > 0$ there is a polynomial time PTM M'' so that for every $x \in \{0,1\}^*$, $Pr[M''(x) = L(x)] \geq 1 - 1/(2^{n^d})$, $n = |x|$.
Using the second definition of BPP, there is a polynomial time DTM M and a polynomial $p()$ such that for all $x \in \{0,1\}^*$ and all $w \in \{0,1\}^{p(n)}$ where $n = |x|$, $Pr_w[M(x,w) = L(x)] \geq 1 - 1/(2^{n^2})$. The TM is deterministic and the is probability is over all w.
Therefore for all $x \in \{0,1\}^*$ and all $w \in \{0,1\}^{p(n)}$, $Pr_w[M(x,w) \neq L(x)] < 1/(2^{n^2})$.

We show by counting argument that there is a string $w_0 \in \{0,1\}^{p(n)}$ so that for all $x \in \{0,1\}^n$, $M(x,w_0) = L(x)$. The single string can be hardwired to get a circuit C_n such that $C_n(x) = M(x,w) = L(x)$ for all $x \in \{0,1\}^n$. The size of such C_n is quadratic in the running time of M.

We use a counting argument to show that there is such a string. A string $w \in \{0,1\}^{p(n)}$ is '*bad*' for an $x \in \{0,1\}^n$ if $M(x,w) \neq L(x)$; otherwise it is 'good'. Number of '*bad*' strings for an x cannot be more than $\frac{2^m}{2^{n^2}}$, where $|w| = m$, the total number of strings of length m are 2^m and fraction of strings that are 'bad' cannot exceed $1/(2^{n^2})$.
Considering all x, the number of '*bad*' strings are less than

$$2^n \times \frac{2^{p(n)}}{2^{n^2}} = 2^{n+p(n)-n^2} < 2^{p(n)}.$$

So there are 'good' strings and there is a polynomial size circuit family $\{C_n\}$ for L such that $x \in L$ if and only if $C_{|x|}(x) = 1$. QED.

We have the following facts (i) **BPP** $\subseteq$ **P/poly**, (ii) if **NP** $\subseteq$ **P/poly**, then **PH** $= \Sigma_2^p$. So if 3SAT can be solved in probabilistic polynomial time then **PH** collapses to Σ_2^p.

1.8 BPP Complete Problem?

The probabilistic complexity class **BPP** is defined using the class **BPTIME**(n^c), where the defining notion is *semantic* in contrast to *syntactic* notion of NDTM.

Any input string $x \in \{0,1\}^*$ is either accepted with probability $\geq 2/3$ or is accepted with probability $< 1/3$.
Given a string $x \in \{0,1\}^*$, it is easy to check syntactically whether it is a valid NTM. But checking of valid encoding of a **BPP** machine is *undecidable*.

References

[MS] *Theory of Computation* by Michael Sipser, (3rd. ed.), Pub. Cengage Learning, 2007, ISBN 978-81-315-2529-6.

[SABB] *Computational Complexity, A Modern Approach* by Sanjeev Arora & Boaz Barak, Pub. Cambridge University Press, 2009, ISBN 978-0-521-42426-4.