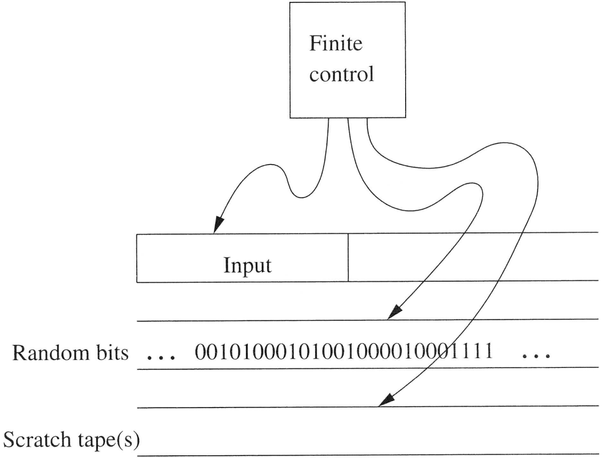
Language Classes Based on Randomization

Jason Belt
CIS 890

November 2, 2010

Randomized Turing Machines



Quicksort

A RTM M does as follows on input w where $|w| = m$:

1. Use about $O(\log m)$ new random bits on Tape 2 to pick a random number n between $1 \dots m$. The n^{th} symbol in w is the pivot p.
2. Put p on Tape 3.
3. Scan w, copying each symbol x to Tape 4 if $x \leq p$.
4. Scan w, copying each symbol y to Tape 5 if $y > p$.
5. Overwrite w on Tape 1 with contents of Tape 4 and then 5, placing a marker between them.
6. If either or both sublists have more than one element, recursively sort them by the same algorithm.

Running time is in $O(n \log n)$

Language of Randomized Turing Machines

- Each "branch" of a RTM has a probability
- On a given input w, a RTM M:
  - may have different runtime behavior
  - may not halt
- Each input w to M has some probability of acceptance
- Time and space complexity can be measured using the worst case computation branch

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_0	0	0	0	0	B
	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

	0	$\color{red}{0}$	0	0	B
$\color{blue}{q_1}$	$\color{red}{0}$	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

$$
q_1 \quad \begin{array}{ccccc} 0 & 0 & 0 & 0 & \mathrm{B} \\ 0 & 1 & 1 & 0 & 1 \end{array}
$$

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_1	0	0	0	0	B
	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\to q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_1	0	0	0	0	B
	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

$$
q_4 \quad \begin{array}{ccccc} 0 & 0 & 0 & 0 & \text{B} \\ 0 & 1 & 1 & 0 & 1 \end{array}
$$

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_0	1	1	1	1	B
	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_2	1	1	1	1	B
	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

	1	1	1	1	B
q_2	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

	1	1	1	1	B
q_2	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

	1	1	1	1	B
q_2	0	1	1	0	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

$$q_4 \quad \begin{array}{ccccc} 1 & 1 & 1 & 1 & \mathrm{B} \\ 0 & 1 & 1 & 0 & 1 \end{array}$$

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_0	1	0	1	B	B
	1	1	0	1	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_3	1	0	1	B	B
	1	1	0	1	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

	1	0	1	B	B
q_3	1	1	0	1	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_3	1	0	1	B	B
	1	1	0	1	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

	1	0	1	B	B
q_3	1	1	0	1	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

q_4	1	0	1	B	B
	1	1	0	1	1

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

Homogeneous Input w (0^i or 1^i)

$$\frac{1}{2} + \frac{1}{2}2^{-i} = \frac{1}{2} + 2^{-(i+1)}$$

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

Heterogeneous Input w (both 0's and 1's)

- if first random bit is 0 then w is never accepted
- Otherwise the probability of acceptance is $2^{-|w|}$

$$\frac{1}{2} 2^{-|w|} = 2^{-(|w|+1)}$$

Example Probability Calculation

	00	01	10	11	$B0$	$B1$
$\rightarrow q_0$	$q_1 00RS$	$q_3 01SR$	$q_2 10RS$	$q_3 11SR$		
q_1	$q_1 00RS$				$q_4 B0SS$	
q_2			$q_2 10RS$		$q_4 B0SS$	
q_3	$q_3 00RR$			$q_3 11RR$	$q_4 B0SS$	$q_4 B1SS$
$*q_4$						

Conclusion: We can compute a probability of acceptance of any given string by any given RTM.

$\mathcal{RP}$ Random Polynomial

A language L is said to be in $\mathcal{RP}$ if it is accepted by a RTM M such that on input w:

1. If $w \notin L$, then the probability that M accepts w is 0.
2. If $w \in L$, then the probability that M accepts w is at least $1/2$.
3. There exits a polynomial $T(n)$ where $n = |w|$ such that all runs of M halt after at most $T(n)$ steps.

$\mathcal{RP}$ Random Polynomial

A language L is said to be in $\mathcal{RP}$ if it is accepted by a RTM M such that on input w:

1. If $w \notin L$, then the probability that M accepts w is 0.
2. If $w \in L$, then the probability that M accepts w is at least $1/2$.
3. There exits a polynomial $T(n)$ where $n = |w|$ such that all runs of M halt after at most $T(n)$ steps.

Polynomial-time Monte-Carlo TMs
The class of languages for which membership can be determined in polynomial time by a RTM with no false acceptances and less than half of the rejections are false rejections

Recognizing Languages in $\mathcal{RP}$

- In general, if we want a probability of false negatives less than $c > 0$, we must run the test $\log_2(1/c)$ times.

Recognizing Languages in $\mathcal{RP}$

- In general, if we want a probability of false negatives less than $c > 0$, we must run the test $\log_2(1/c)$ times.
- Repeating the tests will take polynomial time as c is a constant and one run of a RTM takes polynomial time

Recognizing Languages in $\mathcal{RP}$

- In general, if we want a probability of false negatives less than $c > 0$, we must run the test $\log_2(1/c)$ times.
- Repeating the tests will take polynomial time as c is a constant and one run of a RTM takes polynomial time

Theorem 11.16: If L is in $\mathcal{RP}$, then for any constant $c > 0$, no matter how small, there is a polynomial-time randomized algorithm that renders a decision whether its given input w is in L, makes no false-positive errors, and makes false-negative errors with probability no greater than c.

$\mathcal{ZPP}$ Zero-Error, Probabilistic, Polynomial

- $\mathcal{ZPP}$ is based on a RTM that always halts, and has an expected time to halt that is some polynomial in the length of the input.

$\mathcal{ZPP}$ Zero-Error, Probabilistic, Polynomial

- $\mathcal{ZPP}$ is based on a RTM that always halts, and has an expected time to halt that is some polynomial in the length of the input.
- Similar to the definition of $\mathcal{P}$ except $\mathcal{ZPP}$ allows the TM to involve randomness, and the expected running time rather than worst-case is measured

$\mathcal{ZPP}$ Zero-Error, Probabilistic, Polynomial

- $\mathcal{ZPP}$ is based on a RTM that always halts, and has an expected time to halt that is some polynomial in the length of the input.
- Similar to the definition of $\mathcal{P}$ except $\mathcal{ZPP}$ allows the TM to involve randomness, and the expected running time rather than worst-case is measured
- **Defn:** *Las-Vegas Turning Machines* are TMs that always give the correct answer, but whose running time varies depending on the values of some random bits.

$\mathcal{ZPP}$ Zero-Error, Probabilistic, Polynomial

- $\mathcal{ZPP}$ is based on a RTM that always halts, and has an expected time to halt that is some polynomial in the length of the input.
- Similar to the definition of $\mathcal{P}$ except $\mathcal{ZPP}$ allows the TM to involve randomness, and the expected running time rather than worst-case is measured
- **Defn:** *Las-Vegas Turning Machines* are TMs that always give the correct answer, but whose running time varies depending on the values of some random bits.
- A language $L \in \mathcal{ZPP}$ if it's accepted by a *Las-Vegas Turing Machine* with a polynomial expected running time.

Relationship between $\mathcal{RP}$ and $\mathcal{ZPP}$

If $L \in \mathcal{ZPP}$, then so is $\overline{L}$

- Assume M is a polynomial-expected-time Las-Vegas TM such that $L \in L(M)$
- $\overline{L} \in L(M')$ such that all accepting states in M are changed to halting without acceptance states in M' and all non-accepting halting states in M are changed to accepting and halt states in M'.

Relationship between $\mathcal{RP}$ and $\mathcal{ZPP}$

Theorem 11.17: $\mathcal{ZPP} = \mathcal{RP} \cap \text{co-}\mathcal{RP}$

Proof: $\mathcal{RP} \cap \text{co-}\mathcal{RP} \subseteq \mathcal{ZPP}$

Suppose $L \in \mathcal{RP} \cap \text{co-}\mathcal{RP}$. Therefore L and $\overline{L}$ have Monte-Carlo TM's S and T, each with a polynomial running time. Assume $p(n)$ bounds the running time of both machines. We design a Las-Vegas TM M for L as follows:

1. Run S on the input; if it accepts, then M accepts and halts.
2. If not, run T on the input. If it accepts, then M halts without accepting. Otherwise, M returns to step (1)

Relationship between $\mathcal{RP}$ and $\mathcal{ZPP}$

- Clearly M accepts w if $w \in L$ and rejects w only if $w \notin L$.
- The expected running time of round one is $2p(n)$. Step (1) has a 50% chance of leading to acceptance and Step (2) has a 50% chance of leading to rejection so the expected running time of M is no more than

$$2p(n) + \frac{1}{2}2p(n) + \frac{1}{4}2p(n) + \frac{1}{8}2p(n) + \cdots = 4p(n)$$

Relationship to classes $\mathcal{P}$ and $\mathcal{NP}$

Proof: Assume $L \in \mathcal{ZPP}$ and show $L \in \mathcal{RP}$ and $L \in$ co-$\mathcal{RP}$.

We construct a Monte-Carlo TM M_2 as follows:

- M_2 simulates S for $2p(n)$ steps.
- If S accepts then so does M_2; otherwise M_2 rejects.

Observations:

- Suppose $w \notin L$. Then S will not accept w nor will M_2.
- Suppose $w \in L$. Then S will eventually accept w but not necessarily within $2p(n)$ steps.
- However the probability of S accepting w within $2p(n)$ steps is at least $1/2$ and therefore the probability of M_2 accepting w is at least $1/2$.
- Thus M_2 is polynomial-time-bounded Monte-Carlo TM, so $L \in \mathcal{RP}$. $\square$

Relationship to classes $\mathcal{P}$ and $\mathcal{NP}$

Theorem 11.18: $\mathcal{P} \subseteq \mathcal{ZPP}$

Proof: Any deterministic, polynomial-time bounded TM is also a Las-Vegas, polynomial-time bounded TM, that happens not to use its ability to make random choices $\square$

Relationship to classes $\mathcal{P}$ and $\mathcal{NP}$

Theorem 11.19: $\mathcal{RP} \subseteq \mathcal{NP}$
Proof: Suppose we have a polynomial-time-bounded Monte-Carlo TM M_1 for a language L. When M_1 examines a random bit, M_2 non-deterministically chooses both possible values for the bit and writes it to its own tape which simulates the random tape of M_1. M_2 accepts whenever M_1 accepts and does not accept otherwise.

Suppose $w \in L$. Since the chance M_1 accepts w is 50%, there must exist a sequence of random bits that leads to acceptance of w. M_2 will eventually choose this sequence and therefore also accepts when M_1 does. Thus $w \in L(M_2)$.

However, if $w \notin L$ then there are no sequece of random bits that lead to acceptance in M_1 and therefore no sequence of choices of M_2 will lead to acceptance. Therefore $w \notin L(M_2)$.

Relationship to classes $\mathcal{P}$ and $\mathcal{NP}$