Complexity Reading Group 11/5/2015

1 BPP

Definition 1: For a function $T : \mathbb{N} \mapsto \mathbb{N}$, and a language $L \subseteq \{0,1\}^*$, consider a Probabilistic Turing Machine (PTM), has two functions δ_1 and δ_2 that each specify a set of rules for the TM. At each step, the PTM flips a fair coin, and the result determines if the PTM uses δ_1 or δ_2 for its current rule. We say a PTM M decides L in time $T(n)$ for every $x \in \{0,1\}^*$, M halts in $T(|x|)$, and $\Pr(M(x) = L(x)) \geq \frac{2}{3}$.

Definition 2: The class $\text{BPT}\textsc{ime}(\text{T}(\textsc{n}))$, is the class of languages that can be decided in $\mathcal{O}(T(n))$ by a PTM

Definition 3: The class BPP $= \cup_c \text{BPT}\textsc{ime}(n^c)$ is the class of languages that can be decided in polynomial time by a PTM

Definition 4: A Language L is in BPP if $\exists$ a poly time TM M and a poly $p : \mathbb{N} \mapsto \mathbb{N}$ s.t.:

$$\forall_u : u \in \{0,1\}^*,\ \Pr_r \in \{0,1\}^{p(x)} \left[M(x,r) = L(x)\right] \geq \frac{2}{3} \tag{1}$$

Note: $P \subseteq BPP$, since we could set $\delta_1 = \delta_2$.

---

2 Examples

Example: Finding the median in a list, i.e. compete the $\frac{n}{2}$-th smallest element in a list.

There is a nice randomized algorithm that can compute the median in $\mathcal{O}(n)$ time.

More general solution: Finding the k-th smallest number.

Algorithm: $FindKthSmallest(L, k)$

- Pick a random index, $i \in [1 : len(L)]$
- Go through the list and put all $a_j \leq a_i$ into T.
- if $|T| \geq k$, then we know the number we're looking for is in T. So, return $FindKthSmallest(T, |T| - k)$, or something. The k passed in here isn't exact but it's something like that..

- if $|T| < k$, then we know it's not in T, so it must be in the remainder of L (that we didn't put in T). So, return $FindKthSmallest(L\ T, k - |T|)$

Polynomial Identity Testing: Suppose we have two polynomials: $P, Q : (x_1, \ldots, x_n) \mapsto F$, for some ring F. The question is, are P and Q equivalent polynomials?

Zero Testing: For a polynomial P, is $P = 0$? These two problems are actually identical, because we can ask $P - Q = 0$, and ask $P = Q$, where $Q = 0$.

Lemma 1: Let $p(x_1, \ldots, x_n)$ be non-zero polynomial of total degree at most d. Let S be a set of integers with at least $d + 1$ elements. If $a_1, \ldots a_n$ are randomly chosen from S, then the probability that, if you evaluate p on these integers, then:

$$\Pr(a_1, \ldots, a_n \neq 0) \geq 1 - \frac{d}{|S|} \tag{2}$$

3 The Class RP

Definition 4: $\textsc{Rtime}(T(n))$ contains any language L for which there is a PTM M that runs in time $T(n)$ such that:

$$x \in L \to \Pr(M(x) = 1) \geq \frac{2}{3} \tag{3}$$

$$x \notin L \to \Pr(M(x) = 1) = 1 \tag{4}$$

Definition 5: The class RP is the set of all languages that can be decided in polynomial time by an RTM:

$$RP = \cup_c \textsc{Rtime}(n^c) \tag{5}$$

Definition 6: For a PTM M and input X, define a random variable $T_{M,x}$ as the running time of M over x. $\Pr(T_{M,x} = T) = p$ over random choices of M over x, it will halt T steps. We say M has expected running time $T(n)$ if $\mathbb{E}[T_{M,x}] \leq T(|x|)$. Then M has *zero sided error*

Definition 7: $\text{ZT}\textsc{ime}(T(n))$ is the class of languages that can be decided with *zero sided error*

Definition 8: ZPP is the class:

$$ZPP = \cup_c \text{ZT}\textsc{ime}(n^c) \tag{6}$$

Lemma 2: $ZPP = co - RP \cap RP$

Proof:

(a) $L \in ZPP$ iff there exists a poly time PTM M with outputs, in $\{0, 1?\}$ such that: $\forall_x : x \in \{0,1\}^*$, with probability 1, $M(x) \in \{L(x), ?\}$, and $\Pr(M(x) =?) \leq \frac{1}{2}$.

(b) $ZPP = co - RP \cap RP$