Computational Complexity. Lecture 5

Randomized Computation

Alexandra Kolla

Today

- Probabilistic complexity classes
- Relationship between classes
- BPP in Σ_2

Probabilistic complexity classes

- Algorithm A gets as input sequence of random bits r and “real” input x of the problem.
- Output is the correct answer for input x with some probability.
- **Definition**. A is called polynomial time probabilistic algorithm if the size of the random sequence |r| is poly in |x| and A runs in time polynomial in |x|.

Probabilistic complexity classes

- **Definition (BPP).** Decision problem L belongs to the class BPP if there is a polynomial time algorithm A and a polynomial p() such that:
  - For every $x \in L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] \geq \frac{2}{3}$
  - For every $x \notin L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] \leq \frac{1}{3}$

Probabilistic complexity classes

- We can also define the class P similarly:
- **Definition (P).** Decision problem L belongs to the class P if there is a polynomial time algorithm A and a polynomial p() such that:
  - For every $x \in L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] = 1$
  - For every $x \notin L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] = 0$

Probabilistic complexity classes

- **Definition (RP).** Decision problem L belongs to the class RP if there is a polynomial time algorithm A and a polynomial p() such that:
  - For every $x \in L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] \geq \frac{1}{2}$
  - For every $x \notin L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] = 0$

Probabilistic complexity classes

- **Definition (coRP).** $\text{coRP} = \{\text{L} | \bar{L} \in RP\}$
- In other words, the error is in the other direction (will never output 0 if $x \in L$ but may output 1 if $x \notin L$.

Probabilistic complexity classes

- We can also define the class P similarly:
- **Definition (ZPP).** Decision problem L belongs to the class ZPP if there is a polynomial time algorithm A whose output can be 0,1 ? and a polynomial p() such that:
  - For every $x \in L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x) = ?] \leq \frac{1}{2}$
  - $\forall x \forall r \;\; such\ that\ A(x,r) \neq ?\,, then\ A(x,r) = 1\ iff\ x \in L.$

Relations between complexity classes

- **Theorem 1.** RP $\subseteq$ NP
- **Theorem 2**. ZPP $\subseteq$ RP

Relations between complexity classes

- **Exercise.** $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$

Relations between complexity classes

- **Theorem 3**. A language L is in the class ZPP if and only if L has an average polynomial time algorithm that always gives the right answer.

Relations between complexity classes

- **Theorem 4.** RP $\subseteq$ BPP

Probability amplification

- We can also define the class RP with error probability exp. close to zero:
- **Definition (RP).** Decision problem L belongs to the class RP if there is a polynomial time algorithm A and polynomial p() such that for some fixed polynomial q():
  - For every $x \in L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] \geq 1 - \left(\frac{1}{2}\right)^{q(|x|)}$
  - For every $x \notin L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x)\ \ accepts] = 0$

Probability amplification

- **Theorem.** (Chernoff bound)

Suppose $X_1, \dots, X_k$ are independent random variables with values in {0,1} and for every i, Pr$[X_i = 1]$=p. Then

$$\Pr\left[\frac{1}{k}\sum_{i=1}^{k} X_i - p > \epsilon\right] < e^{\left\{-\frac{\epsilon^2 k}{2p(1-p)}\right\}}$$

$$\Pr\left[\frac{1}{k}\sum_{i=1}^{k} X_i - p < -\epsilon\right] < e^{\left\{-\frac{\epsilon^2 k}{2p(1-p)}\right\}}$$

Probability amplification

- Re-define BPP with exp. small error.
- **Definition (BPP).** Decision problem L belongs to the class BPP if there is a polynomial time algorithm A and polynomial p() such that for some fixed polynomial q() :
  - For every $x \in L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x) \ \ accepts] \geq 1 - \left(\frac{1}{2}\right)^{q(|x|)}$
  - For every $x \notin L, Pr_{r \in \{0,1\}^{p(|x|)}}[A(r,x) \ \ accepts] \leq \left(\frac{1}{2}\right)^{q(|x|)}$

Biased coins

- Could an algorithm get more power if the coin is not fair?

- **Lemma 1**. A coin with Pr(heads) =p can be simulated in expected time O(1) provided that the i-th bit or p is compute in poly(i) time.

- **Lemma 2**. A coin with Pr(heads) =1/2 can be simulated by an algorithm that has access to a stream of p-biased coins in expected time O(1/p(1-p)) . (ex)

Relations between probabilistic classes and circuit complexity

- **Theorem.** BPP $\subseteq$ SIZE$(n^{O(1)})$

Other relations

- **Open.** $\mathrm{BPP} \subseteq \mathrm{NP}$ (unlikely by previous lecture)

BPP$\subseteq \Sigma_2$

- **Theorem. (**Siepser-Gacs-Lautemann)BPP $\subseteq \Sigma_2$