Two-point Sampling

Speaker: Chuang-Chieh Lin
Advisor: Professor Maw-Shang Chang
National Chung Cheng University
2006/6/29

References

- Professor S. C. Tsai's lecture slides.
- *Randomized Algorithms*, Rajeev Motwani and Prabhakar Raghavan.

Joint probability density function

- X, Y: discrete random variables defined over the same probability sample space.
- $p(x, y) = \mathbf{Pr}[\{X = x\} \cap \{Y = y\}]$: the joint probability density function (pdf) of X and Y.
- Thus, $\mathbf{Pr}[Y = y] = \sum_{x} p(x, y)$

  and $\mathbf{Pr}[X = x | Y = y] = \frac{p(x,y)}{\mathbf{Pr}[Y=y]}$.

- A sequence of random variables is called pairwise independent if for all $i \neq j$, and $x, y \in$ R, $\mathbf{Pr}[X_i = x \mid X_j = y] = \mathbf{Pr}[X_i = x]$.

Randomized Polynomial time (*RP*)

- The class ***RP*** (for Randomized Polynomial time) consists of all languages ***L*** that have a randomized algorithm ***A*** running in worse-case polynomial time such that for any input *x* in Σ^* (Σ is the alphabet set),
  - ★ $x \in L \Rightarrow \mathbf{Pr}[A(x) \text{ accepts}] \geq \frac{1}{2}$.
  - ★ $x \notin L \Rightarrow \mathbf{Pr}[A(x) \text{ accepts}] = 0$.

Try to reduce the random bits…

- We now consider trying to reduce the number of random bits used by ***RP*** algorithms.
- Let ***L*** be a language and ***A*** be a randomized algorithm for deciding whether an input string *x* belongs to ***L*** or not.

- Given x, ***A*** picks a random number r from the range $Z_n = \{0,1,\ldots, n-1\}$, with the following property:
- If $x \in \boldsymbol{L}$, then $\boldsymbol{A}(x, r) = 1$ for at least half the possible values of r.
- If $x \notin \boldsymbol{L}$, then $\boldsymbol{A}(x, r) = 0$ for all possible choices of r.

- Observe that for any $x \in \boldsymbol{L}$, a random choice of r is a witness with probability at least ½.
- **<u>Goal:</u>** We want to increase this probability, i.e., decrease the error probability.

A strategy for error-reduction

There is a strategy as follows:

- Pick $t > 1$ values, $r_1, r_2, .. r_t \in \boldsymbol{Z}_n$.
- Compute $\boldsymbol{A}(x, r_i)$ for $i = 1, \ldots, t$.
- If for any i, $\boldsymbol{A}(x, r_i) = 1$, then declare $x \in L$.

- The error probability of this strategy is at most 2^{-t}.
- Yet it still uses $\Omega(t \log n)$ random bits.
  - Why?

Strategy of two point sampling

Actually, we can use **fewer** random bits.

- Choose a, b randomly from $\boldsymbol{Z}_n$.
- Let $r_i = a \cdot i + b \bmod n$, $i = 1, \ldots, t$, then compute $\boldsymbol{A}(x, r_i)$.
- If for any i, $\boldsymbol{A}(x, r_i) = 1$, then declare $x \in \boldsymbol{L}$.

- Now what is the error probability?

- $r_i = ai + b \bmod n$, $i = 1, \ldots, t$.
- r_i's are pairwise independent.
  - (See [MR95], Exercise 3.7 in page 52)
- Let $Y = \sum_{i=1}^{t} A(x, r_i)$

$$x \in L \Rightarrow \mathbf{E}[Y] \geq \frac{t}{2} \ \ and \ \ \sigma_Y^2 \leq \frac{t}{4} \leftarrow why?$$

Suppose **E**[***A***(*x*,r_i)] = \mu \geq ½, we have **Var**[***A***(*x*,r_i)] = \mu * (1-mu). By simple calculus analysis, we have **Var**[***A***(*x*,r_i)] \leq ¼, thus **Var**[*Y*] = \sum_{*i* =1}^{*t*} **Var**[***A***(*x*,r_i)] \leq t/4.

- What is the probability of the event $\{Y = 0\}$?

  $Y = 0 \;\Rightarrow\; |Y - \mathbf{E}[Y]| \geq t/2.$

Thus $\mathbf{Pr}[Y = 0] \leq \mathbf{Pr}[|Y - \mathbf{E}[Y]| \geq t/2]$

$$\leq \mathbf{Pr}[|Y - \mathbf{E}[Y]| \geq \sqrt{t}\sigma_Y]$$

$$\leq 1/t.$$

Chebyshev's Inequality: $\mathbf{Pr}[\,|X - \mu_x| \geq t\sigma_X] \leq 1/t^2$

Thank you.