Randomness in Computing

LECTURE 2

CS 537

Last time
- Verifying polynomial identities
- Probability amplification
- Probability review

Discussions
- Law of Total Probability
- Bayes’law

Today
- More probability amplification
- Verifying matrix multiplication

Review question

Toss a fair coin three times.

Let E_i be the event that the i-th toss is HEADS.

Let $E = E_1 \cap E_2 \cap E_3$.

What is the probability of E?

A. $\Pr(E_1) \cdot \Pr(E_2 | E_1) \cdot \Pr(E_3 | E_1 \cap E_2)$

B. $\Pr(E_1) \cdot \Pr(E_2) \cdot \Pr(E_3)$

C. Both A and B are correct.

D. Neither A nor B is correct.

Review question

Toss a coin that is biased with heads probability p three times.

Let E_i be the event that the i-th toss is HEADS.

Let $E = E_1 \cap E_2 \cap E_3$.

What is the probability of E?

A. $\Pr(E_1) \cdot \Pr(E_2 | E_1) \cdot \Pr(E_3 | E_1 \cap E_2)$

B. $\Pr(E_1) \cdot \Pr(E_2) \cdot \Pr(E_3)$

C. Both A and B are correct.

D. Neither A nor B is correct.

Probability Amplification

- Our algorithm for verifying polynomial identities accepts incorrectly with probability $\leq \frac{d}{100d} = \frac{1}{100}$

Idea: Repeat the algorithm and accept if all iterations accept.

$$\Pr[\text{error in all } k \text{ iterations}] \leq \left(\frac{1}{100}\right)^k$$

Sampling without replacement

- Let E_i be the event that we choose a root in iteration i

$$\begin{gathered}\Pr[\text{error in all } k \text{ iterations}] \\ = \Pr[E_1 \cap \cdots \cap E_k] \\ = \Pr[E_1] \cdot \Pr[E_2 | E_1] \cdot \ldots \cdot \Pr[E_k | E_1 \cap \cdots \cap E_{k-1}]\end{gathered}$$

- It is 0 if $k > d$.
- If $k \leq d$, then $\Pr\left[E_j \middle| E_1 \cap \cdots \cap E_{j-1}\right] = \dfrac{d-(j-1)}{100d-(j-1)}$

$$\Pr[\text{error in all } k \text{ iterations}] \leq \left(\frac{1}{100}\right)^k$$

§1.3 (MU) Verifying Matrix Multiplication

Task: Given three $n \times n$ matrices A, B, C, verify if $A \cdot B = C$.

Matrix multiplication algorithms:

- Naïve $O(n^3)$ time
- Strassen $O\left(n^{\log_2 7}\right) \approx O(n^{2.81})$ time
- World record $O(n^{2.373\ldots})$ time

  [Coppersmith-Winograd `87, Vassilevska Williams `13, LeGall `14]

Verification:

- Fastest known deterministic algorithm is as above.
- Randomized algorithm [Freivalds `79] $O(n^2)$ time

§1.3 (MU) Verifying Matrix Multiplication

Task: Given three $n \times n$ matrices A, B, C, verify if $A \cdot B = C$.

Idea: Pick a random vector $\bar{\boldsymbol{r}}$ and check if $A \cdot B \cdot \bar{\boldsymbol{r}} = C \cdot \bar{\boldsymbol{r}}$.

Algorithm Basic Frievalds (input: $n \times n$ matrices A, B, C)

1. Choose a random n-bit vector $\bar{r}$ by making each bit r_i independently 0 or 1 with probability 1/2 each.
2. **Accept** if $A \cdot (B \cdot \bar{\boldsymbol{r}}) = C \cdot \bar{\boldsymbol{r}}$; o. w. **reject**.

$O(n^2)$ multiplications for each matrix-vector product

Running time: Three matrix-vector multiplications: $O(n^2)$ time.

Correctness: If $A \cdot B = C$, the algorithm always accepts.

Theorem

If $A \cdot B \neq C$, Basic-Frievalds accepts with probability $\leq 1/2$.

Probability Amplification: With k repetitions, error probability $\leq 2^{-k}$

Law of Total Probability

For any two events A and E,

$$\begin{aligned}\Pr(A) &= \Pr(A \cap E) + \Pr(A \cap \overline{E}) \\ &= \Pr(A|E) \cdot \Pr(E) + \Pr(A|\overline{E}) \cdot \Pr\left(\overline{E}\right)\end{aligned}$$

Let A be an event and let $E_1, \dots, E_n$ be mutually disjoint events whose union is Ω.

$$\Pr(A) = \sum_{i \in [n]} \Pr(A \cap E_i) = \sum_{i \in [n]} \Pr(A \mid E_i) \cdot \Pr(E_i)\,.$$