Randomness in Computing

Lecture 2

CS 537

Last time
- Verifying polynomial identities
- Probability amplification
- Probability review
- Card magic trick

Discussions
- Conditional Probability
- Product Rule
- Law of Total Probability
- Bayes' Law

Today
- More probability amplification
- Verifying matrix multiplication

CS 537

Review question

Card dealing

We deal two cards. What is the probability that the second card is an ace, given that the first is an ace?

A. 3/52

B. 3/51

C. 4/52

D. 5/52

E. None of the answers above are correct.

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.

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

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

- 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 $\leq 2^{-k}$

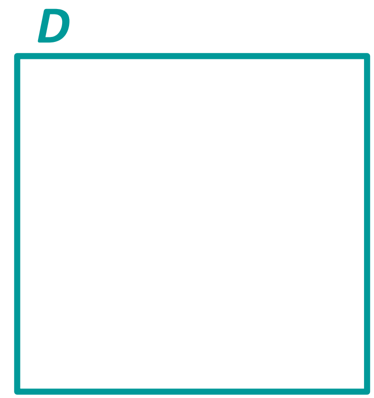
Analysis of Error Probability

Theorem

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

Proof: Suppose $A \cdot B \neq C$ and let $D = AB - C$

D has a nonzero entry.



How can we have $A \cdot (B \cdot \bar{\boldsymbol{r}}) = C \cdot \bar{\boldsymbol{r}}$?

This would mean that $D \cdot \bar{\boldsymbol{r}} = \mathbf{0}$.

Principle of Deferred Decisions

Idea: It does not matter in which order r_k are chosen!

- First choose $r_1, \ldots, r_6, r_8, \ldots, r_n$. Then r_7
- Before r_7 is chosen, the RHS of our equation is determined:

$$r_7 = -\frac{d_{3,1} \cdot r_1 + \cdots + d_{3,6} \cdot r_6 + d_{3,8} \cdot r_8 + \cdots + d_{3,n} \cdot r_n}{d_{3,7}}$$

- Now, there is at most one choice of r_7 that will satisfy it.
- Since there are two choices for r_7, the equation holds w.p. $\leq \frac{1}{2}$

Law of Total Probability

For any two events A and E,

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

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

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

Analysis of Basic Freivalds: Formal Justification

Break Ω into smaller events $E_{x_1,\dots,x_6,x_8,\dots,x_n}$ corresponding to $(r_1,\dots,r_6,r_8,\dots,r_n)$ being assigned $x_1,\dots,x_6,x_8,\dots,x_n \in \{0,1\}$.

$$\Pr[AB\bar{\boldsymbol{r}} = C\bar{\boldsymbol{r}}] = \sum_{x\in\{0,1\}^{n-1}} \Pr[(AB\bar{\boldsymbol{r}} = C\bar{\boldsymbol{r}}) \cap E_x]$$

by Law of Total Probability

$$\le \sum_{x\in\{0,1\}^{n-1}} \Pr[(r_7 \text{ satisfies the equality}) \cap E_x]$$

$$= \sum_{x\in\{0,1\}^{n-1}} \Pr[(r_7 \text{ satisfies the equality}) | E_x] \cdot \Pr[E_x]$$

$$\le \sum_{x\in\{0,1\}^{n-1}} \frac{1}{2} \cdot \Pr[E_x] \le \frac{1}{2} \sum_{x\in\{0,1\}^{n-1}} \Pr[E_x] = \frac{1}{2}$$

Bayesian Approach to Amplification

How does our confidence increase with the number of trials?

- C = event that identity is correct
- A = event that test accepts

Our analysis of Basic Frievalds:

- $\Pr[A|\bar{C}] \leq 1/2$
- 1-sided error: $\Pr[A|C]=1$

Assumption (initial belief or ``prior''): $\Pr[C] = 1/2$

By Bayes' Law

$$\Pr[C|A] = \frac{\Pr[A|C] \cdot \Pr[C]}{\Pr[A|C] \cdot \Pr[C] + \Pr\left[A\middle|\bar{C}\right] \cdot \Pr\left[\bar{C}\right]}$$

$$\geq \frac{1 \cdot \frac{1}{2}}{1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2}} = \frac{2}{3}$$

Bayesian Approach to Amplification

How does our confidence increase with the number of trials?

- C = event that identity is correct
- A = event that test accepts

Our analysis of Basic Frievalds:

- $\Pr[\mathrm{A}|\bar{C}] \leq 1/2$
- 1-sided error: Pr[A|C]=1

Assumption (initial belief or ``prior''): $\Pr[C] = \mathbf{2/3}$

By Bayes' Law

$$\Pr[C|A] = \frac{\Pr[A|C] \cdot \Pr[C]}{\Pr[A|C] \cdot \Pr[C] + \Pr\left[A\middle|\bar{C}\right] \cdot \Pr\left[\bar{C}\right]}$$

$$\geq \frac{1 \cdot \mathbf{\frac{2}{3}}}{1 \cdot \mathbf{\frac{2}{3}} + \frac{1}{2} \cdot \mathbf{\frac{1}{3}}} = \mathbf{\frac{4}{5}}$$

CS 537 Bayesian Approach to Amplification

How does our confidence increase with the number of trials?

- C = event that identity is correct
- A = event that test accepts

Our analysis of Basic Frievalds:

- $\Pr[A|\bar{C}] \leq 1/2$
- 1-sided error: Pr[A|C]=1

Assumption (initial belief or ``prior''): $\Pr[C] = \mathbf{2^i/(2^i + 1)}$

By Bayes' Law

$$\Pr[C|A] = \frac{\Pr[A|C] \cdot \Pr[C]}{\Pr[A|C] \cdot \Pr[C] + \Pr\left[A\middle|\bar{C}\right] \cdot \Pr\left[\bar{C}\right]}$$

$$\geq \frac{1 \cdot \frac{\mathbf{2^i}}{\mathbf{2^i+1}}}{1 \cdot \frac{\mathbf{2^i}}{\mathbf{2^i+1}} + \frac{1}{2} \cdot \frac{\mathbf{1}}{\mathbf{2^i+1}}} = \frac{\mathbf{2^{i+1}}}{\mathbf{2^{i+1}+1}}$$