Probability in Computing

CS 237

LECTURE 2

Last time

- Course information
- Uses of probability in CS
- Verifying polynomial identities

Today

- Verifying polynomial identities
- Basic concepts in probability

Reminders

- Submit signed Collaboration and Honesty policy on Gradescope
- HW1 due Thursday

Last time: Verifying Polynomial Identities

- $(x+1)(x-2)(x+3)(x-4)(x+5)(x-6) \equiv^{?} x^6 - 7x + 37$

Task: Given two polynomials $f(x)$ and $g(x)$, verify if $f(x) \equiv g(x)$.

no use of randomness

- Simple deterministic methods for this task are slow.
- We learned a simple randomized method, based on:

Fundamental Theorem of Algebra

A polynomial of degree d has at most d roots.

Using Randomness for Verification

Task: Given two polynomials $f(x)$ and $g(x)$, verify if $f(x) \equiv g(x)$.

Idea (randomized): Evaluate the polynomials on random integers.

All numbers in this set are equally likely

Or, d could be any upper bound on the degree of $p(x)$, that is, $d \geq$ degree $p(x)$.

Let $d =$ max degree of $f(x)$ and $g(x)$

1. Pick r uniformly from $\{1, \ldots, 100d\}$.
2. Compute $f(r)$ and $g(r)$
3. **reject** if $f(r) \neq g(r)$; o. w. **accept**.

Only $d - 1$ multiplications needed to evaluate a product of d monomials

- Does this procedure accept or reject for our example when $r = 2$?

$$(x+1)(x-2)(x+3)(x-4)(x+5)(x-6) \equiv^{?} x^6 - 7x + 37$$

Top Hat question (Join Code: 033357)

What are the chances that our algorithm accepts on input

$$f(x) = 2x^2 + 2;$$
$$g(x) = \ x^2 + 3x \ ?$$

A. 100%

B. 50%

C. 2%

D. 1%

Let d = max degree of $f(x)$ and $g(x)$

1. Pick r uniformly from $\{1, \ldots, 100d\}$.
2. Compute $f(r)$ and $g(r)$
3. **reject** if $f(r) \neq g(r)$; o. w. **accept**.

Analysis of Correctness

Task: Given two polynomials $f(x)$ and $g(x)$, verify if $f(x) \equiv g(x)$.

Let d = max degree of $f(x)$ and $g(x)$

1. Pick r uniformly from $\{1, \ldots, 100d\}$.
2. Compute $f(r)$ and $g(r)$
3. **reject** if $f(r) \neq g(r)$; o. w. **accept**.

- If $f(x) \equiv g(x)$, we always accept. *No error in this case*
- Otherwise, consider polynomial $p(x) = f(x) - g(x)$.
  - Checking if $f(x) \equiv g(x)$ is the same as checking if $p(x) \equiv 0$
  - Polynomial $p(x)$ has degree at most d; $p(x) \neq 0$ when $f(x) \neq g(x)$
  - By Fundamental Theorem of Algebra, $p(x)$ has at most d roots.
  - We accept (incorrectly) only if we picked r to be a root of $p(x)$
  - This happens in at most d out of $100d$ cases, i.e., with probability at most

$$\frac{d}{100d} = \frac{1}{100}$$

.01 probability of error

Reducing Probability of Error

Task: Given two polynomials $f(x)$ and $g(x)$, verify if $f(x) \equiv g(x)$.

Let $d =$ max degree of $f(x)$ and $g(x)$

1. Pick r uniformly from $\{1, \ldots, 100d\}$.
2. Compute $f(r)$ and $g(r)$
3. **reject** if $f(r) \neq g(r)$; o. w. **accept**.

- We accept (incorrectly) only if we picked r to be a root of $p(x)$
- This happens in at most d out of $100d$ cases, i.e., with probability at most

$$\frac{d}{100d} = \frac{1}{100}$$

.01 probability of error

How can we make it even smaller?

CS 237

Probability Theory

- Introduce three self-evident and indisputable properties of probability (the axioms)
- Develop the mathematical theory of probability from these axioms

Andrey Kolmogorov

[1903 - 1987]

"The theory of probability as a mathematical discipline can and should be developed from axioms in exactly the same way as geometry and algebra."

CS 237

Typical Statements about Probability

1. The probability that the randomized algorithm for checking polynomial identities accepts when the input is not an identity is at most 1/100.
2. The chance of getting a flush (that is, all cards of the same suit) in a 5-card poker hand is about 2 in 1000.
3. The chance of precipitation today in Boston is 20%.

Each such statement is implicitly talking about a random experiment

- either constructed by us, as in (1) and (2)
- or used by us to model the world, as in (3)

Probability: Random Experiment

- Random experiment: a repeatable procedure
  - Pick an integer from the set $\{1, \ldots, 100d\}$
  - Toss a coin
  - Toss a coin 3 times
  - Roll two dice
  - Pick a 5-card hand out of a deck of cards
  - Observe the number of goals in a soccer match between robots

Probability: Sample Space

- Outcome: result of the experiment
- Sample space Ω: set of all possible outcomes
  - Pick an integer from the set $\{1, \dots, 100d\}$

    $\Omega =$
  - Toss a coin

    $\Omega =$
  - Toss a coin 3 times

    $\Omega =$

Probability: Sample Space

- Outcome: result of the experiment
- Sample space Ω: set of all possible outcomes
  - Roll two dice

    Ω =

  - Pick a 5-card hand out of a deck of cards
    (the order of cards doesn't matter, so {**5♥, 5♦, 5♠, Q♥, Q♣**} and {**5♦, 5♥, Q♥, 5♠, Q♣**} are the same hand)

    Ω is the set of all subsets of five cards, |Ω| =
  - Observe the number of goals in a soccer match between robots

    Ω =

Probability: Event

- Event: a subset of the sample space

  (that is, a set of outcomes)

  – Experiment: toss a coin 3 times

    Event A : get at least 2 heads

    $A = \{$ $\}$

  – Experiment: roll two 6-sided dice

    Event B: the sum of the two numbers rolled is 11

    $B = \{$ $\}$

Top Hat question (Join Code: 033357)

- Experiment: toss a coin 3 times
- Which of the following is the event "exactly 2 heads"?

$$E_1 = \{HHT, HTH, THH, HHH\}$$

$$E_2 = \{HHT, HTH, THH\}$$

$$E_3 = \{HTH, THH\}$$

A. E_1

B. E_2

C. E_3

D. Both E_2 and E_3 are correct

Top Hat question (Join Code: 033357)

- Experiment: toss a coin 3 times
- Event $E = \{HTH, HHT, THH\}$

Which of the following describes the event E?

A. “exactly one head”
B. “exactly one tail”
C. “at most one tail”
D. None of the above

Events

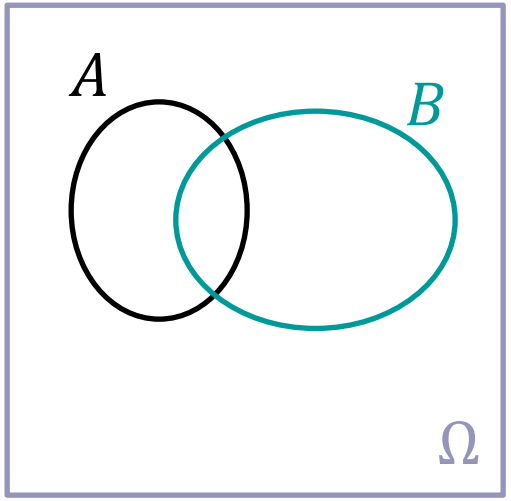
- Events are *sets* of outcomes
- We can combine events using set operations

$A \cap B$: the event that both A and B occurred

$A \cup B$: the event that A or B occurred

$A \setminus B$: the event that A occurred but B did not

$\overline{A}$: the event that A did not occur



Top Hat question (Join Code: 033357)

- Experiment: toss a coin 3 times

  Are the following events disjoint?

$A \cap B = \emptyset$

$A =$ "exactly 2 heads"

$B =$ "exactly 2 tails"

A. YES

B. NO

Top Hat question (Join Code: 033357)

- Experiment: toss a coin 3 times

$A \subseteq B$

Does the first event imply the second?

$A =$ "at least 2 heads"

$B =$ "exactly 2 heads"

A. YES

B. NO

Probability: Cast of Characters

- Random experiment: a repeatable procedure
- Outcome: result of the experiment
- Sample space Ω: set of all possible outcomes
- Event: a subset of the sample space
- Probability function Pr: assigns a probability Pr(E) to each event E

Probability Function

assigns a probability Pr(E) to each event E

- Experiment: toss a fair coin

E	∅	{H}	{T}	{H,T}
Pr(E)				

- Experiment: roll a die

Probability Function

assigns a probability Pr(E) to each event E

- Experiment: toss a fair coin 3 times

Probability Function

What principles did we use to come up with those probability functions?

- Symmetry: each outcome of the coin toss (or die roll) is equally likely
- The probability of each outcome is a number between 0 and 1
- Additivity: for events with more than one outcome, the probability of the event is the sum of the probabilities of its outcomes

Note: some experiments are not symmetric (toss a coin until H)