DM551/MM851

Algorithms and Probability

September 23, 2020

Conditional Probability

Thm. [Baye's Theorem] For events A, B, with $p(A) > 0$, $p(B) > 0$, $p(A|B) = \frac{p(A)p(B|A)}{p(B)}$.

Conditional Probability

Thm. [Baye's Theorem] For events A, B, with $p(A) > 0$, $p(B) > 0$, $p(A|B) = \frac{p(A)p(B|A)}{p(B)}$.

Pf. By the def of conditional probability,

$p(A \cap B) = p(B)p(A|B)$.

$p(A \cap B) = p(A)p(B|A)$.

So $p(B)p(A|B) = p(A)p(B|A)$.

Divide both sides by $p(B)$. $\square$

Conditional Probability

Thm. [Baye's Theorem] For events A, B, with $p(A) > 0$, $p(B) > 0$, $p(A|B) = \frac{p(A)p(B|A)}{p(B)}$.

Pf. By the def of conditional probability,

$p(A \cap B) = p(B)p(A|B)$.

$p(A \cap B) = p(A)p(B|A)$.

So $p(B)p(A|B) = p(A)p(B|A)$.

Divide both sides by $p(B)$. $\square$

Example: With 2 fair dice, what is the probability that the sum is 7, given that both dice are ≥ 3?

Conditional Probability

Thm. [Baye's Theorem] For events A, B, with $p(A) > 0$, $p(B) > 0$, $p(A|B) = \frac{p(A)p(B|A)}{p(B)}$.

Pf. By the def of conditional probability,

$p(A \cap B) = p(B)p(A|B)$.

$p(A \cap B) = p(A)p(B|A)$.

So $p(B)p(A|B) = p(A)p(B|A)$.

Divide both sides by $p(B)$. $\square$

Example: With 2 fair dice, what is the probability that the sum is 7, given that both dice are ≥ 3?

Answer: $p(\text{sum is } 7 \mid \text{both} \geq 3) = \frac{p(\text{sum is } 7) \cdot p(\text{both } \geq 3 \mid \text{sum is } 7)}{p(\text{both } \geq 3)} = \frac{\frac{1}{6} \cdot \frac{1}{3}}{\frac{2}{3} \cdot \frac{2}{3}} = 1/8$.

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

Assume: all birthdays equally likely, 366 days in a year.

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

Assume: all birthdays equally likely, 366 days in a year.

$p_n =$ probability first n have different birthdays

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

Assume: all birthdays equally likely, 366 days in a year.

$p_n =$ probability first n have different birthdays

$p_1 = 1$ $\qquad$ $p_2 = \frac{365}{366}$ (Poll)

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

Assume: all birthdays equally likely, 366 days in a year.

$p_n =$ probability first n have different birthdays

$p_1 = 1$ $\qquad$ $p_2 = \frac{365}{366}$ (Poll)

$p_3 = \frac{365}{366} \cdot \frac{364}{366}$

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

Assume: all birthdays equally likely, 366 days in a year.

p_n = probability first n have different birthdays

$p_1 = 1$ $\qquad$ $p_2 = \frac{365}{366}$ (Poll)

$p_3 = \frac{365}{366} \cdot \frac{364}{366}$

If $j-1$ people in room with $j-1$ different birthdays, probability jth is different is $\frac{366-(j-1)}{366}$

$p_n = \frac{365 \cdot 364 \cdot 363 \cdots (367-n)}{366^n}$

The Birthday Problem (Paradox)

What is the minimum number of people who need to be in a room so that the probability at least 2 have the same birthday $> \frac{1}{2}$?

Assume: all birthdays equally likely, 366 days in a year.

$p_n =$ probability first n have different birthdays

$p_1 = 1$ $\qquad$ $p_2 = \frac{365}{366}$ (Poll)

$p_3 = \frac{365}{366} \cdot \frac{364}{366}$

If $j-1$ people in room with $j-1$ different birthdays, probability jth is different is $\frac{366-(j-1)}{366}$

$p_n = \frac{365 \cdot 364 \cdot 363 \cdots (367-n)}{366^n}$

$1 - p_{22} \approx 0.475$

$1 - p_{23} \approx 0.506$ $\qquad$ **Answer** $= 23$

Probability of Collision – Hash Functions

hash function $h : L \to S$ $\qquad |S| = m$

Assume for random key $k \in L$, prob$(h(k) = s \in S) = \frac{1}{m}$

Probability of Collision – Hash Functions

hash function $h : L \to S$ $|S| = m$

Assume for random key $k \in L$, $\text{prob}(h(k) = s \in S) = \frac{1}{m}$

$Sign(h(m_1)) = Sign(h(m_2))$ iff $h(m_1) = h(m_2)$.

Probability of Collision – Hash Functions

hash function $h : L \to S$ $\qquad |S| = m$

Assume for random key $k \in L$, $\text{prob}(h(k) = s \in S) = \frac{1}{m}$

$\textit{Sign}(h(m_1)) = \textit{Sign}(h(m_2))$ iff $h(m_1) = h(m_2)$.

$p_n =$ prob n keys all hash to different locations

Probability of Collision – Hash Functions

hash function $h : L \to S$ $\qquad |S| = m$

Assume for random key $k \in L$, $\text{prob}(h(k) = s \in S) = \frac{1}{m}$

$Sign(h(m_1)) = Sign(h(m_2))$ iff $h(m_1) = h(m_2)$.

$p_n =$ prob n keys all hash to different locations

prob jth key hashes to different than $h(k_1), h(k_2), \ldots, h(k_{j-1})$
(assuming all different) $= \frac{m-(j-1)}{m}$

$p_n = \frac{(m-1)(m-2)\cdots(m-n+1)}{m^n}$

Probability of Collision – Hash Functions

hash function $h : L \to S$ $\qquad |S| = m$

Assume for random key $k \in L$, $\text{prob}(h(k) = s \in S) = \frac{1}{m}$

$Sign(h(m_1)) = Sign(h(m_2))$ iff $h(m_1) = h(m_2)$.

$p_n =$ prob n keys all hash to different locations

prob jth key hashes to different than $h(k_1), h(k_2), \ldots, h(k_{j-1})$
(assuming all different) $= \frac{m-(j-1)}{m}$

$p_n = \frac{(m-1)(m-2)\cdots(m-n+1)}{m^n}$

For $n \approx 1.177\sqrt{m}$, $p_n > \frac{1}{2}$.

Monte Carlo Algorithms

Monte Carlo Algorithms – Randomized algorithms

Produce answer (quickly), possibly wrong.

Monte Carlo Algorithms

Monte Carlo Algorithms – Randomized algorithms

Produce answer (quickly), possibly wrong.

Las Vegas algorithms – always correct, can take long

Expected good running time

Monte Carlo Algorithms

Monte Carlo Algorithms – Randomized algorithms

Produce answer (quickly), possibly wrong.

Las Vegas algorithms – always correct, can take long

Expected good running time

Decision problem – result is true/false

Monte Carlo algorithm, ALG:

Case: Answer false – ALG always answers false

Case: Answer true – ALG answers true with prob p

(Poll)

Monte Carlo Algorithms

Monte Carlo Algorithms – Randomized algorithms

Produce answer (quickly), possibly wrong.

Las Vegas algorithms – always correct, can take long

Expected good running time

Decision problem – result is true/false

Monte Carlo algorithm, ALG:

Case: Answer false – ALG always answers false

Case: Answer true – ALG answers true with prob p

(Poll)

Monte Carlo Algorithms

In some cases, want ALG to answer “unknown” instead of “false”.

How do you run ALG on input m?

Monte Carlo Algorithms

In some cases, want ALG to answer "unknown" instead of "false".

How do you run ALG on input m?

$i \leftarrow 0$
repeat
    if ALG(m) answers true, **then return** true; halt
    $i \leftarrow i + 1$
until ($i = n$)
return false/unknown

Monte Carlo Algorithms

In some cases, want ALG to answer "unknown" instead of "false".

How do you run ALG on input m?

$i \leftarrow 0$
repeat
    if ALG(m) answers true, **then return** true; halt
    $i \leftarrow i + 1$
until ($i = n$)
return false/unknown

Probability of error is $(1 - p)^n$.

Example: Quality control

Suppose we have batches of chips.

Each batch was either tested or not.

If a batch was tested, they are all good.

Otherwise, $\frac{1}{10}$ are bad.

Example: Quality control

Suppose we have batches of chips.

Each batch was either tested or not.

If a batch was tested, they are all good.

Otherwise, $\frac{1}{10}$ are bad.

To find out if a given batch is tested or not:

Test k chips in the batch at random.

Example: Quality control

Suppose we have batches of chips.

Each batch was either tested or not.

If a batch was tested, they are all good.

Otherwise, $\frac{1}{10}$ are bad.

To find out if a given batch is tested or not:

Test k chips in the batch at random.

If tested, no errors will be found.

If not tested, prob of no errors is $\leq (\frac{9}{10})^k$.

Example: Primality testing n

$n - 1 = 2^s m$

Choose x randomly. Check:

$x^m \pmod{n}$, $x^{2m} \pmod{n}$, …, $x^{2^{s-2}m} \pmod{n}$, $x^{2^{s-1}m} \pmod{n}$

Example: Primality testing n

$n-1=2^s m$

Choose x randomly. Check:

$x^m \pmod{n}$, $x^{2m} \pmod{n}$,…, $x^{2^{s-2}m} \pmod{n}$, $x^{2^{s-1}m} \pmod{n}$

If none $= n-1$ and $x^m \pmod{n} \neq 1$, n is not prime.

If n not prime, prob $\leq \frac{1}{4}$ that (one $= n-1$) or ($x^m \pmod{n} = 1$).

Example: Primality testing n

$n - 1 = 2^s m$

Choose x randomly. Check:

$x^m \pmod{n}$, $x^{2m} \pmod{n}, \ldots,$ $x^{2^{s-2}m} \pmod{n}$, $x^{2^{s-1}m} \pmod{n}$

If none $= n - 1$ and $x^m \pmod{n} \neq 1$, n is not prime.

If n not prime, prob $\leq \frac{1}{4}$ that (one $= n - 1$) or ($x^m \pmod{n} = 1$).

Repeat k times.

If never returns "not prime", answer "probably prime".

Prob error $\leq (\frac{1}{4})^k$.

Probabilistic Method

Goal: Prove the existence of object without necessarily being able to exhibit it.

Probabilistic Method

Goal: Prove the existence of object without necessarily being able to exhibit it.

Consider set S (graphs) with some property P (having clique or independent set of size k)

Suppose prob $s \in_R S$ does not have property P is < 1.

Then $\exists\ s \in S$ with property P.

Probabilistic Method

Goal: Prove the existence of object without necessarily being able to exhibit it.

Consider set S (graphs) with some property P (having clique or independent set of size k)

Suppose prob $s \in_R S$ does not have property P is < 1.

Then $\exists\ s \in S$ with property P.

Thm. $k \geq 2 \Rightarrow \quad R(k,k) \geq 2^{k/2}$.

Random Variables

Def. For a sample space S, a *random variable* is a function $f : S \to \mathbb{R}$.

Example

Suppose a coin is flipped until the result is "heads". Let X be the random variable that equals the number of coins flipped.

Random Variables

Def. For a sample space S, a *random variable* is a function $f : S \to \mathbb{R}$.

Example

Suppose a coin is flipped until the result is "heads". Let X be the random variable that equals the number of coins flipped.

$$X(H) = 1, \qquad X(TTH) = 3, \qquad X(TTTH) = 4$$

Random Variables

Def. For a sample space S, a *random variable* is a function $f : S \to \mathbb{R}$.

Example

Suppose a coin is flipped until the result is "heads". Let X be the random variable that equals the number of coins flipped.

$$X(H) = 1, \qquad X(TTH) = 3, \qquad X(TTTH) = 4$$

Let $p(X = r)$ denote the probability the X takes the value r.

Def. The *distribution* of the random variable X on a sample space S is the set

$$\{(r, p(X = r)) \mid r \in X(S)\},$$

Random Variables

Def. For a sample space S, a *random variable* is a function $f : S \to \mathbb{R}$.

Example

Suppose a coin is flipped until the result is "heads". Let X be the random variable that equals the number of coins flipped.

$$X(H) = 1, \qquad X(TTH) = 3, \qquad X(TTTH) = 4$$

Let $p(X = r)$ denote the probability the X takes the value r.

Def. The *distribution* of the random variable X on a sample space S is the set

$$\{(r, p(X = r)) \mid r \in X(S)\},$$

For a fair coin, the distribution of X is $\{(i, 1/2^i) \mid i \geq 1\}$.

Expectations

Recall:

Def. A *random variable* is a function $f : S \to \mathbb{R}$.

Def. For a finite sample space $S = \{s_1, s_2, ..., s_n\}$, the *expected value* of the random variable $X(s)$ is

$$E(X) = \sum_{i=1}^{n} p(s_i)X(s_i).$$

Def. For a countably infinite sample space $S = \{s_i \mid i \geq 1\}$, the *expected value* of the random variable $X(s)$ is $E(X) = \sum_{i=1}^{\infty} p(s_i)X(s_i)$.

Expectations

Recall:

Def. A *random variable* is a function $f : S \to \mathbb{R}$.

Def. For a finite sample space $S = \{s_1, s_2, ..., s_n\}$, the *expected value* of the random variable $X(s)$ is

$$E(X) = \sum_{i=1}^{n} p(s_i)X(s_i).$$

Def. For a countably infinite sample space $S = \{s_i \mid i \geq 1\}$, the *expected value* of the random variable $X(s)$ is
$E(X) = \sum_{i=1}^{\infty} p(s_i)X(s_i)$.

Example: What is the expected number of successes in n Bernoulli trials? Probability of success $= p$. Probability of failure $= q = 1 - p$. (Poll)