Lecture 17

Bayes Rule & Applications in CS.
Lecture 16 Summary

- Probability is additive

- Union Bound \( \Pr(\bigcup A_i) \leq \sum \Pr(A_i) \)

- Inclusion-Exclusion \( \Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(AB) \)

- Total probability: if \( A_1, \ldots, A_n \) partition \( \Omega \)

  then \( \Pr(B) = \Pr(A_1B) + \ldots + \Pr(A_nB) \)

- Conditional probability: \( \Pr(B|A) = \frac{\Pr(AB)}{\Pr(A)} \)

- Independence: \( \Pr(AB) = \Pr(A) \cdot \Pr(B) \)

- Correlation: \( \Pr(AB) > \Pr(A) \cdot \Pr(B) \)

- Bayes' Rule.
**Conditional Probability**

**Defn:** The conditional probability of event $B$ given event $A$ is

$$
Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]}
$$

[Diagram showing Venn diagram of events $A$, $B$, and $\Omega$]
Total Probability with Conditional Probability

Assume $\Omega$ is a union of disjoint events $A_1, \ldots, A_n$

Since $B$ is the disjoint union of $B \cap A_1, \ldots, B \cap A_n$

$$\Pr[B] = \Pr[B \cap A_1] + \ldots + \Pr[B \cap A_n]$$
Total Probability with Conditional Probability

Assume \( \mathcal{S} \) is a union of disjoint events \( A_1, \ldots, A_n \)

Since \( B \) is the disjoint union of \( B \cap A_1, \ldots, B \cap A_n \)

\[
\Pr [B] = \Pr [B \cap A_1] + \ldots + \Pr [B \cap A_n]
\]

Thus, by the product rule

\[
\Pr [B] = \Pr [A_1] \cdot \Pr [B \mid A_1] + \ldots + \Pr [A_n] \cdot \Pr [B \mid A_n]
\]
Total Probability Rule with Conditional Probability


\[ P(B) = P(A_1) \cdot P(B | A_1) + \cdots + P(A_n) \cdot P(B | A_n) \]
Bayes Rule

Suppose you know $\Pr[B|A]$, $\Pr[A]$, $\Pr[B]$

What's $\Pr[A|B]$?

$$
\Pr[A|B] = \frac{\Pr[AnB]}{\Pr[B]} = \frac{\Pr[A] \cdot \Pr[B|A]}{\Pr[B]}
$$
Bayes Rule Example #1

Experiment:

1. Pick at random either a fair coin 
or a biased coin with 60% chance heads.
2. Toss the coin you picked

\[ \Omega = \{ \text{fair, H}, \text{fair, T}, \text{biased, H}, \text{biased, T} \} \]

\[ A = \text{“coin is fair”} \quad B = \text{“got H”} \]

WTK: \( \Pr [A | B] \)
Bayes Rule Example #1

Experiment:

1. Pick at random either a fair coin
   or a biased coin with 60% chance heads.
2. Toss the coin you picked

\[ \Omega = \{ \text{fair, H}, \text{fair, T}, \text{biased, H}, \text{biased, T}\} \]

\[ \text{\text{A}} = \text{"coin is fair" } \quad \text{\text{B}} = \text{"got H"} \]

\[ \text{WTK: } \Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{\Pr[A] \cdot \Pr[B | A]}{\Pr[B]} = \frac{0.5 \times 0.5}{\Pr[B]} \]

What's \( \Pr[B] \)?
Bayes Rule Example #1

Experiment:
1. Pick at random either a fair coin or a biased coin with 60% chance heads.
2. Toss the coin you picked

\[ \Omega = \{ (\text{fair, H}), (\text{fair, T}), (\text{biased, H}), (\text{biased, T}) \} \]

\[ A = \text{"coin is fair"} \quad B = \text{"got H"} \]

Work:
\[
\Pr[A \mid B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{\Pr[A] \cdot \Pr[B \mid A]}{\Pr[B]} 
\]

\[
\Pr[B] = \Pr[A \cap B] + \Pr[A^c \cap B] 
= \Pr[A] \Pr[B \mid A] + \Pr[A^c] \Pr[B \mid A^c] 
\]
Bayes Rule Example #1

Experiment:

1. Pick at random either a fair coin or a biased coin with 60% chance heads.
2. Toss the coin you picked

\[ \Omega = \{ \text{fair, H}, \text{fair, T}, \text{biased, H}, \text{biased, T} \} \]

A = “coin is fair”    B = “got H”

\[ \Pr [A|B] = \frac{\Pr [A \cap B]}{\Pr [B]} = \frac{\Pr [A] \cdot \Pr [B|A]}{\Pr [B]} = \frac{0.25}{\Pr [CB]} \]

\[ \Pr [B] = \Pr [A] \Pr [B|A] + \Pr [\overline{A}] \Pr [B|\overline{A}] \]

\[ = 0.5 \cdot 0.5 + 0.5 \cdot 0.6 = 0.55 \]
Bayes Rule (updated)

\[ \Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)} \]

\[ = \frac{\Pr(A) \cdot \Pr(B|A)}{\Pr(A) \cdot \Pr(B|A) + \Pr(A^c) \cdot \Pr(B|A^c)} \]

\[ \Pr(B) = \Pr(A) \cdot \Pr(B|A) + \Pr(A^c) \cdot \Pr(B|A^c) \]
\[
P_r(A|B) = \frac{P_r(A) \cdot P_r(B|A)}{P_r(B)}
\]

Bayes Rule (Updated)

\[
P_r(A|B) = \frac{P_r(A) \cdot P_r(B|A)}{P_r(A) \cdot P_r(B|A) + P_r(A^c) \cdot P_r(B|A^c)} = \frac{p_{91}}{p_{91} + (1-p)q_2}
\]
Bayes Rule Example #2

Suppose there's a disease that occurs in 0.001 of the population. There's a test for the disease.

For a random person:  \( Pr[\text{test positive} \mid \text{sick}] = 0.99 \)

\( Pr[\text{test positive} \mid \text{not sick}] = 0.01 \)

A random person arrives and tests positive.

Q: What's the likelihood that he has the disease?
\[
\begin{align*}
\Pr[\text{sick}] &= 0.001 \\
\Pr[\text{positive}|\text{sick}] &= 0.99 \\
\Pr[\text{positive}|\text{not sick}] &= 0.01
\end{align*}
\]

WTK: \[\Pr[\text{sick}|\text{positive}]\]
\[ P_r[\text{sick}] = 0.001 \]
\[ P_r[\text{positive} | \text{sick}] = 0.99 \]
\[ P_r[\text{positive} | \text{not sick}] = 0.01 \]

\[ \text{WTK: } P_r[\text{sick} | \text{positive}] \]

\[ P_r[A|B] = \frac{P_r[A \cap B]}{P_r[B]} \]

\[ = \frac{P_r[A] \cdot P_r[B|A]}{P_r[A] \cdot P_r[B|A] + P_r[A^c] \cdot P_r[B|A^c]} \]

\[ A = \text{"sick"} \]
\[ B = \text{"tested positive"} \]
\[ P_r [\text{sick}] = 0.001 \]
\[ P_r [\text{positive} | \text{sick}] = 0.99 \]
\[ P_r [\text{positive} | \text{not sick}] = 0.01 \]

\[ \text{WTK: } P_r [\text{sick} | \text{positive}] \]

\[ P_{r[A|B]} = \frac{P_r [A \cap B]}{P_r [B]} \]
\[ = \frac{P_r [A] \cdot P_r [B|A]}{P_r [A] \cdot P_r [B|A] + P_r [\overline{A}] \cdot P_r [B|\overline{A}]} \]
\[ = \frac{0.001 \times 0.99}{0.001 \times 0.99 + 0.999 \times 0.01} \]
\[ \approx 0.09 \]

\[ A = \text{"sick"} \]
\[ B = \text{"tested positive"} \]
1M people

- 1000 people
  - 990 True Positives
  - 10 False Negatives

- 999,000 people
  - 990 False Positives
  - 989,010 True Negatives
Primality Testing

Properties:
- If n is prime, always output "yes"
- If n is composite, outputs "no" w.p. \(1 - \frac{1}{1000}\)
Primality Testing

Properties:

- If $n$ is prime, always output "yes"
- If $n$ is composite, outputs "no" w.p. $1 - \frac{1}{1000}$

What's $\Pr[\text{N is prime} \mid \text{output is 'yes'}]$?
Primality Testing

Properties:
- If \( n \) is prime, always output "yes"
- If \( n \) is composite, outputs "no" w.p. \( 1 - \frac{1}{1000} \)

What's \( \Pr[Cn \text{ is prime} \mid \text{output is "yes"}] \)?

For that, \( n \) should be random as well.
- Pick \( n \in [2^{511}, 2^{512}) \) uniformly at random.
Primality Testing

\[ \Pr[A|B] = \frac{p \cdot q_1}{p \cdot q_1 + (1-p) \cdot q_2} \]

\[ = \frac{\frac{1}{350}}{\frac{1}{350} + \frac{349}{350} \cdot \frac{1}{1000}} \approx 0.74 \]

\[ = \frac{p \cdot q_1}{p \cdot q_1 + (1-p) \cdot q_2} \]

\[ = \frac{\frac{1}{350}}{\frac{1}{350} + \frac{349}{350} \cdot \frac{1}{1000}} \approx 0.74 \]

\[ A = \text{“n is prime”} \quad B = \text{“answer is yes”} \]

\[ p = \frac{1}{350} \quad q_1 = 1 \quad q_2 = \frac{1}{1000} \]
Birthday Paradox

Poll: How many students do you need to have in a classroom so that you'll definitely have a pair of students with the same birthday?

A: 23
B: 365
C: 366
D: $365 \times 364$
Birthday Paradox

How many students do you need to have in a classroom so that you’ll have a pair of students with the same birthday w.p. $\geq \frac{1}{2}$. 
Birthday Paradox

Assumption: Each student has a uniformly random birthday out of the 365 options.

K students.

\( \Omega = \{ (x_1, \ldots, x_K) : \forall i \ 1 \leq x_i \leq 365 \} \)

\( E = \text{"no collision"} = \{ (x_1, \ldots, x_K) : \text{For all } i < j, x_i \neq x_j \} \)

\( |E| = \)
**Birthday Paradox**

**Assumption:** Each student has a uniformly random birthday out of the 365 options.

K students.

\[ \Omega = \{ (x_1, ..., x_k) : \forall i \ 1 \leq x_i \leq 365 \} \]

\[ |\Omega| = 365^k \]

\[ E = \text{"no collision"} = \{ (x_1, ..., x_k) : \text{For all } i < j, x_i \neq x_j \} \]

\[ |E| = 365 \cdot 364 \cdots (365 - k + 1) \]

\[ \Pr[E] = \frac{|E|}{|\Omega|} = \frac{365 \cdots (365 - k + 1)}{365^k} \]

By tedious calculation, when \( k = 23 \), \( \Pr[E] \leq 0.5 \) and hence \( \Pr[\text{exists a collision}] > 0.5 \).
Birthday Paradox

Assumption: Each student has a uniformly random birthday out of the 365 options.

$k$ students.

$\Omega = \{(x_1, \ldots, x_k) : \forall i \ 1 \leq x_i \leq 365\}$

$E = \text{"no collision"} = \{(x_1, \ldots, x_k) : \text{For all } i < j, x_i \neq x_j\}$

$\overline{E} = \text{"\exists collision"} = \{(x_1, \ldots, x_k) : \exists i < j \text{ s.t. } x_i = x_j\}$

How to get a simple upper bound on $\Pr[\overline{E}]$?
**Birthday Paradox**

**Assumption:** Each student has a uniformly random birthday out of the 365 options.

\[ \Omega = \{ (x_1, \ldots, x_k) : \forall i \ 1 \leq x_i \leq 365 \} \]

\[ E = \text{"no collision"} = \{ (x_1, \ldots, x_k) : \text{For all } i < j, x_i \neq x_j \} \]

\[ \bar{E} = \text{"\exists collision"} = \{ (x_1, \ldots, x_k) : \exists i < j \text{ s.t. } x_i = x_j \} \]

How to get a simple upper bound on \( \Pr[\bar{E}] \)?

For \( 1 \leq i < j \leq k \) let \( A_{ij} \) be the event indicating "\( x_i = x_j \)"

\[ \Pr[\bar{E}] = \Pr[\bigcup_{1 \leq i < j \leq k} A_{ij}] \]
Birthday Paradox

Assumption: Each student has a uniformly random birthday out of the 365 options.

K students.

Ω = \{ (x_1, ..., x_K) : \forall i \ 1 \leq x_i \leq 365 \}

E = "no collision" = \{ (x_1, ..., x_K) : \text{For all } i < j, x_i \neq x_j \}

\bar{E} = "\exists\ collision" = \{ (x_1, ..., x_K) : \exists i < j \text{ s.t. } x_i = x_j \}

How to get a simple upper bound on \( \Pr[\bar{E}] \)?

For \( 1 \leq i < j \leq k \) let \( A_{ij} \) be the event indicating "\( x_i = x_j \)"

\[ \Pr[\bar{E}] = \Pr[ \bigcup_{1 \leq i < j \leq k} A_{ij} ] \leq \sum_{1 \leq i < j \leq k} \Pr(CA_{ij}) = \binom{k}{2} \cdot \frac{1}{365}. \]
Birthday Paradox in Computing

You create a hash table of size $n$ and add $k$ elements to it using a random hash function.

Q: What's the prob. for a collision?
Birthday Paradox in Computing

You create a hash table of size \( n \) and add \( k \) elements to it using a random hash function.

Q: What's the prob. for a collision?

\[
\Pr[\text{no collision}] = \frac{n \cdots (n-k+1)}{n^k}
\]

\[
\Pr[\exists \text{ collision}] \leq \sum_{1 \leq i \leq j \leq k} \Pr[\text{elements } i \& j \text{ collide}] = \binom{k}{2} \cdot \frac{1}{n^2}.
\]
n balls in n bins

What's the maximum capacity?
What's the maximum capacity?

Let \( j \) be a parameter.

Denote by \( A_j = \) "there exists a bin with \( \geq j \) balls"

\( \Pr[A_j] = ? \)
$n$ balls in $n$ bins

What's the maximum capacity?

Let $j$ be a parameter.

Denote by $A_j = \text{"there exists a bin with } \geq j \text{ balls"}$

$\Pr[A_j] = ?$

Let $A_{j,1}, A_{j,2}, ..., A_{j,n}$ be events $A_{j,i} = \text{"bin } #i \text{ has } \geq j \text{ balls"}$

$A_j = A_{j,1} \cup A_{j,2} \cup ... \cup A_{j,n}$

$\Pr[A_j] \leq \sum_{i=1}^{n} \Pr[A_{j,i}]$
n balls in n bins

What’s the maximum capacity?

$A_{j,i} = \text{"bin \# i has } \geq j \text{ balls"} \quad A_{j} = \text{"j bin with } \geq j \text{ balls"}$

$Pr[A_{j,i}] = \leq \quad \leq$
What's the maximum capacity?

$A_{j,i} =$ "bin # $i$ has $\geq j$ balls"   \hspace{1cm} $A_j =$ "$j$ bin with $\geq j$ balls"

$\Pr[A_{j,i}] \leq \binom{n}{j} \cdot \frac{n^{n-j}}{n^n} = \binom{n}{j} \cdot \frac{1}{n^j} = \frac{n \cdots (n-j+1)}{j! \cdot n^j} \leq \frac{1}{j!}$

$\Pr[A_j] \leq \Pr[A_{j,1}] + \cdots + \Pr[A_{j,n}] \leq n \cdot \frac{1}{j!}$

For example, for $n = 1,000,000$, $j = 10$, $\Pr[A_j] \leq 0.28$
Independence

We say that events $A$ and $B$ are independent if

$$
\Pr[A \cap B] = \Pr[A] \cdot \Pr[B].
$$

**Example:** Toss two fair coins

- $A$ = "first coin is H"
- $B$ = "second coin is H"
- $C$ = "same result"

Poll: Which are independent

1: $A, B$
2: $A, C$
3: $B, C$
**Independence**

We say that events $A$ and $B$ are independent if

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B].$$

**Example:** Toss two fair coins

- $A = $ "first coin is H"
- $B = $ "second coin is H"
- $C = $ "same result"

$A \& B$ are indep.
$A \& C$ are indep.
$B \& C$ are indep.
Independence

We say that events $A$ and $B$ are independent if

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B].$$

**Example:** Toss two fair coins

- $A = "first \ coin \ is \ H"$
- $B = "second \ coin \ is \ H"$
- $C = "same \ result"$

Are $A, B, C$ independent together?
Independence

We say that events $A$ and $B$ are independent if $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$.

Example: Toss two fair coins

$A = "first \ coin \ is \ H"$
$B = "second \ coin \ is \ H"$
$C = "same \ result"

Are $A, B, C$ independent together?

$\Pr[C \mid A \cap B] = 1$
Definition  Pairwise Independence

We say that events $A_1, \ldots, A_n$ are pairwise independent if

$A_i \neq j\ A_i$ and $A_j$ are independent.
**Definition** Pairwise Independence

We say that events $A_1, \ldots, A_n$ are pairwise independent if for all $i \neq j$, $A_i$ and $A_j$ are independent.

**Definition** Mutual Independence

We say that events $A_1, A_2, A_3$ are mutually independent if they are pairwise independent and

$$P_r(A_1 \cap A_2 \cap A_3) = P_r(A_1)P_r(A_2)P_r(A_3)$$
**Definition** Pairwise Independence

We say that events $A_1, \ldots, A_n$ are pairwise independent if for all $i \neq j$, $A_i$ and $A_j$ are independent.

**Definition** Mutual Independence

We say that events $A_1, \ldots, A_n$ are mutually independent if for each non-empty subset $I = \{i_1, \ldots, i_k\}$, \( \Pr[\cap_{i \in I} A_i] = \prod_{i \in I} \Pr[A_i] \)
Secret Sharing

n shares threshold: 3

Degree a polynomial

How to pick the polynomial: let $p > n$ be a prime

1. Pick $a_0 \in \{0, 1, \ldots, p-1\}$ uniformly at random.
2. Pick $a_1, a_2 \in \{0, 1, \ldots, p-1\}$ uniformly at random.

$$f(x) = a_2 x^2 + a_1 x + a_0$$

Share $i$: $f(i)$
Secret Sharing

$n$ shares threshold: 3

Degree a polynomial

How to pick the polynomial: let $p > n$ be a prime

1. Pick $s = a_0 \in \{0, 1, \ldots, p-1\}$ uniformly at random.
2. Pick $a_1, a_2 \in \{0, 1, \ldots, p-1\}$ uniformly at random.

$$f(x) = a_2 x^2 + a_1 x + a_0$$

Share $i$: $f(i)$

$$\Pr \left[ s = a \mid f(x_1) = y_1, f(x_2) = y_2 \right] = \ldots$$
Secret Sharing

\( n \) shares threshold 3

Degree a polynomial

How to pick the polynomial: let \( p > n \) be a prime

1. Pick \( s = a_0 \in \{0, 1, \ldots, p-1\} \) uniformly at random.
2. Pick \( a_1, a_2 \in \{0, 1, \ldots, p-1\} \) " " "

\[ f(x) = a_2 x^2 + a_1 x + a_0 \]

Share \( i \): \( f(i) \)

\[
\Pr \left[ s = a \mid f(x_1) = y_1, f(x_2) = y_2 \right] = \frac{\Pr \left[ s = a, f(x_1) = y_1, f(x_2) = y_2 \right]}{\Pr \left[ f(x_1) = y_1, f(x_2) = y_2 \right]} = \frac{1/p^3}{p/p^3} = \frac{1}{p}
\]
Secret Sharing

n shares threshold: 3

Degree a polynomial

How to pick the polynomial: let \( p > n \) be a prime

1. Pick \( s = a_0 \in \{0, 1, \ldots, p-1\} \) uniformly at random.
2. Pick \( a_1, a_2 \in \{0, 1, \ldots, p-1\} \)

\[
f(x) = a_2 x^2 + a_1 x + a_0
\]

Share \( i \): \( f(i) \)

Every three shares are independent:

\[
\Pr[f(x_1) = y_1 \land f(x_2) = y_2 \land f(x_3) = y_3] = \frac{1}{p^3}
\]
Secret Sharing

\( n \) shares  threshold: 3

Degree a polynomial

How to pick the polynomial:  let \( p > n \) be a prime

1. Pick \( s = a_0 \in \{0, 1, \ldots, p-1\} \) uniformly at random.
2. Pick \( a_1, a_2 \in \{0, 1, \ldots, p-1\} \) uniformly at random.

\[ f(x) = a_2 x^2 + a_1 x + a_0 \]

Share \( i \): \( f(i) \)

Every three shares are independent:

\[ \Pr[f(x_1) = y_1 \land f(x_2) = y_2 \land f(x_3) = y_3] = \frac{1}{p^3} \]

but 4 shares are not.