0 Announcements

Midterm scores are out!
Good job. We're happy with your performance.

Regrade requests: 8 pm Wednesday – midnight Sunday
Estimated grade bins on piazza

Midsemester survey
Please let us know how things are going.
Don't be afraid to be critical!

One-on-one meetings
If you want to talk to a TA about anything related to this class, fill out the form by Wednesday night.

A comment.
Exams and grades are ephemeral. Understanding is what matters.

A reminder:

Monday HW session $\longrightarrow$ Tuesday 10 am – 12 pm (permanently)

HW problems take time! Why not start early?

You can sign up for a small discussion section at any time during the summer.

0.5 Recap

Previously on CS70...

Conditional probability $P(A \mid B) = \frac{P(A \cap B)}{P(B)}$

probability that A occurs given that you know B occurred

Bayes' rule $P(A \mid B) = \frac{P(B \mid A)\,P(A)}{P(B)}$

prior probability

update

event we are interested in

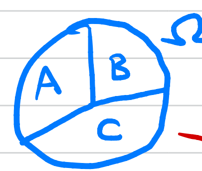
new evidence

Simple proof. Profound implications?

P(You are sick | you test positive)

Base rates matter

Law of total probability



$P(A) + P(B) + P(C) = 1$

disjoint union is Ω

① Independence

Def Events A and B are independent if $P(A \cap B) = P(A)P(B)$

Intuitive meaning: Knowing whether or not A occurred tells you nothing about whether B occurred & vice-versa

Formal version of intuition

Prop If $P(B) > 0$ then A & B are independent if and only if $P(A|B) = P(A)$.

pf ($\Rightarrow$) $P(A \cap B) = P(A)P(B) \Rightarrow P(A|B) = \dfrac{P(A \cap B)}{P(B)} = \dfrac{P(A)\cancel{P(B)}}{\cancel{P(B)}}$

$= P(A)$

($\Leftarrow$) $P(A|B) = P(A) \Rightarrow \dfrac{P(A \cap B)}{P(B)} = P(A)$

$\Rightarrow P(A \cap B) = P(A)P(B)$

Cor If $P(A), P(B) > 0$ then $P(A|B) = P(A) \Leftrightarrow P(B|A) = P(B)$

Def Events A and B are **independent** if $P(A \cap B) = P(A)P(B)$

Intuitive meaning: Knowing whether or not A occurred tells you nothing about whether B occurred

Example Flip a fair coin and then flip it again

A = 1st flip is H
B = 2nd flip is H
} independent (or are they?)
↳ empirical question

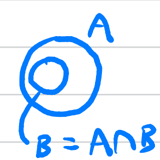
$P(A) = \frac{1}{2}$ $\quad P(B) = \frac{1}{2}$ $\quad P(A \cap B) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$

Independence is often an assumption you make when deciding how to model a real world situation

Example Flip a fair coin 2 times

A = 1st flip is H
B = both flips are H
} not independent

$P(A) = \frac{1}{2}$ $\quad P(B) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ $\quad P(A \cap B) = \frac{1}{4}$



Question Suppose A and B are independent. What about A and $\overline{B}$?

Answer Also independent! Same for $\overline{A}, B$ and $\overline{A}, \overline{B}$

Intuitively If knowing A doesn't tell you whether B occurred, it also doesn't tell you whether B <u>didn't</u> occur

Prop If A and B are independent events then so are A and $\overline{B}$.

pf

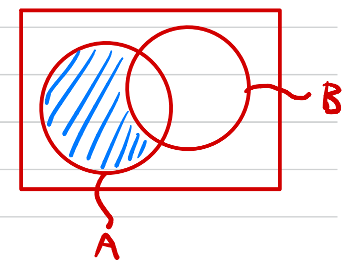
$$P(A \cap \overline{B}) = P(A) - P(A \cap B)$$

↳ law of total probability

$$= P(A) - P(A)P(B)$$

$$= P(A)(1 - P(B))$$

$$= P(A)P(\overline{B})$$



② Pairwise vs. Mutual Independence

Question Suppose A, B, C are events

A, B independent

A, C independent

B, C independent

What is $P(A \cap B \cap C)$?

Answer Trick question! It depends on how $A, B,$ and C are related.

It is not always true that $P(A \cap B \cap C) = P(A)P(B)P(C)$

Example Flip a fair coin 2 times

A = 1st flip is H

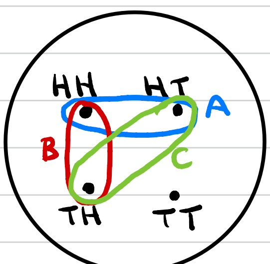
B = 2nd flip is H

C = The two flips are different

$P(A) = 1/2$

$P(B) = 1/2$

$P(C) = 1/2$



$A \cap B = HH \qquad P(A \cap B) = 1/4$

$A \cap C = HT \qquad P(A \cap C) = 1/4$

$B \cap C = TH \qquad P(B \cap C) = 1/4$

$$\boxed{P(A \cap B \cap C) = 0}$$

Def Events $A_1, A_2, \dots, A_n$ are pairwise independent if for all $i \neq j$, A_i and A_j are independent

Def Events $A_1, A_2, \dots, A_n$ are mutually independent if for all $I \subseteq \{1, 2, 3, \dots, n\}$ s.t. $|I| \geq 2$,

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i)$$

What does this mean for $n = 3$?

$$P(A_1 \cap A_2) = P(A_1) P(A_2)$$
$$P(A_1 \cap A_3) = P(A_1) P(A_3)$$
$$P(A_2 \cap A_3) = P(A_2) P(A_3)$$

$\rightarrow$ pairwise independence

$$P(A_1 \cap A_2 \cap A_3) = P(A_1) P(A_2) P(A_3)$$

Note: Mutual independence $\Rightarrow$ Pairwise independence

Pairwise independence $\not\Rightarrow$ Mutual independence

A familiar example...

Suppose you want to share a secret $s \in \{0, 1, 2, \ldots, 10\}$

Let's assume $s = 7$

Generate a polynomial $p(x) = a_3 x^3 + a_2 x^2 + a_1 x + s$ over $GF(11)$
by picking a_3, a_2, a_1 randomly from $\{0, 1, 2, \ldots, 10\}$

Hand out shares $p(x_0), p(x_1), \ldots, p(x_n)$ $\quad x_i \neq x_j \quad x_i \neq 0$

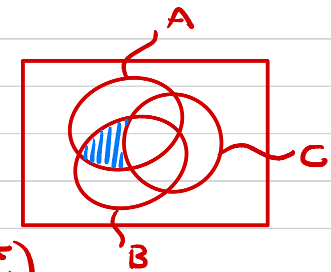
Define A_i = event that $p(x_i) = 0$

<u>Question</u> For what n are A_i's mutually independent?

<u>Answer</u> For $n < 4$, mutually independent

For $n \geq 4$, not mutually independent $\rightarrow$ $P(A_1 \cap A_2 \cap A_3 \cap A_4) = 0$
but pairwise independent
(actually 3-wise independent)

Question Suppose A, B, C mutually independent. What is $P(A \cap B \cap \overline{C})$?



Answer $P(A \cap B \cap \overline{C}) = P(A)P(B)(1 - P(C))$

Why? $P(A \cap B \cap \overline{C}) = P(A \cap B) - P(A \cap B \cap C)$

$$A \cap B = (A \cap B \cap C) \cup (A \cap B \cap \overline{C})$$

$$= P(A)P(B) - P(A)P(B)P(C)$$

$$= P(A)P(B)(1 - P(C))$$

Prop $A_1, A_2, \ldots, A_n$ are mutually independent if and only if for all

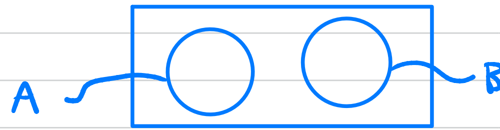
$$B_1 \in \{A_1, \overline{A_1}\}$$
$$B_2 \in \{A_2, \overline{A_2}\}$$
$$\vdots$$
$$B_n \in \{A_n, \overline{A_n}\}$$

we have

$$P(B_1 \cap B_2 \cap \cdots \cap B_n) = P(B_1)P(B_2) \cdots P(B_n)$$

③ Mutually Exclusive Events

Def Events A and B are **mutually exclusive** if $A \cap B = \emptyset$



A, B mutually exclusive $\Rightarrow$ $P(A \cap B) = 0$
$P(A \cup B) = P(A) + P(B)$

Example Flip a fair coin 2 times
A = 1^{st} flip is H
B = both flips are T

Question Suppose A, B are independent events with $P(A), P(B) > 0$. Can A & B be mutually exclusive?

Answer No! $P(A \cap B) = P(A)P(B) > 0$

"Independent" and "mutually exclusive" are (almost) opposites

Warning: Mutually exclusive events are (almost) never independent!!

④ Combinations of Events

Given events $A_1, A_2, \ldots, A_n$, how do we calculate $P(A_1 \cap A_2 \cap \ldots A_n)$ and $P(A_1 \cup A_2 \cup \ldots A_n)$?

↳ prob. that all of $A_1, \ldots, A_n$ occur

↳ prob. that at least 1 of $A_1, \ldots, A_n$ occurs

Examples

① You are in charge of maintaining 100 servers. What is the probability that they all fail on the same day?

↳ intersection of events

That at least one fails today? → union of events

② What is the probability that a randomized algorithm returns the wrong answer 10 times in a row?

↳ intersection

③ Users are randomly assigned usernames. What is the probability two users are assigned the same username?

↳ union of intersections $P((A_1 \cap A_2) \cup (A_1 \cap A_3) \cup \ldots)$

Given events $A_1, A_2, \ldots, A_n$, how do we calculate $P(A_1 \cap A_2 \cap \ldots A_n)$ and $P(A_1 \cup A_2 \cup \ldots A_n)$?

↳ prob. that all of $A_1, \ldots, A_n$ occur

↳ prob. that at least 1 of $A_1, \ldots, A_n$ occurs

Three methods:

1. Exact formulas for $P(A_1 \cap \ldots \cap A_n)$ and $P(A_1 \cup \ldots \cup A_n)$
   But often hard to compute
2. Make assumptions about $A_1, \ldots, A_n$ that simplify things
   But these assumptions may be unrealistic
3. Estimate the probabilities, rather than computing them directly
   Sometimes an upper bound is good enough
   Later in this class: 2 more lectures on ways to do this

5 Intersections of Events

5.1 Intersections of Events: Exact Formula

<u>Thm</u> (Product rule) If $A_1, A_2, \dots, A_n$ are events s.t. $P(\bigcap_{i \le n} A_i) > 0$
then $P(A_1 \cap A_2 \cap \dots \cap A_n) =$

$$P(A_1)P(A_2|A_1)\,P(A_3|A_1 \cap A_2) \cdots P(A_n|A_1 \cap \dots \cap A_{n-1})$$

$P(A \cap B) = P(A)P(B|A)$

$P(A \cap B \cap C) = P(A)P(B|A)P(C|A \cap B)$

pf Induction on n.

Base case: $P(A_2|A_1) = \dfrac{P(A_2 \cap A_1)}{P(A_1)}$

$$\Rightarrow P(A_1 \cap A_2) = P(A_1)P(A_2|A_1)$$

Inductive step:

by $n=2$ case

$$P(\underline{A_1 \cap \dots \cap A_n} \cap \underline{A_{n+1}}) = P(A_1 \cap \dots \cap A_n)\,P(A_{n+1}|A_1 \cap \dots \cap A_n)$$

IH

$$= P(A_1)P(A_2|A_1) \cdots P(A_{n+1}|A_1 \cap \dots \cap A_n)$$

Thm (Product rule) If $A_1, A_2, \ldots, A_n$ are events s.t. $P(\bigcap_{i \le n} A_i) > 0$ then $P(A_1 \cap A_2 \cap \ldots \cap A_n) =$

$$P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2) \cdots P(A_n|A_1 \cap \ldots \cap A_{n-1})$$

Example Draw 5 cards from a deck without replacement. What is the probability of getting all hearts?

$A_1 =$ 1^{st} card is hearts
$A_2 =$ 2^{nd} card is hearts
$\vdots$
$A_5 =$ 5^{th} card is hearts

$$P(\text{all hearts}) = P(A_1 \cap A_2 \cap \ldots \cap A_5)$$

$$= P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2) \cdots P(A_5|A_1 \cap \ldots \cap A_4)$$

$$= \frac{13}{52} \cdot \frac{12}{51} \cdot \frac{11}{50} \cdot \frac{10}{49} \cdot \frac{9}{48} = {}_{13}P_5 / {}_{52}P_5$$

5.2 Intersections of Events: Easy Special Cases

1. Mutually independent events

$$P(A_1 \cap \dots \cap A_n) = P(A_1)P(A_2)\cdots P(A_n)$$

2. Mutually exclusive events

$$P(A_1 \cap A_2 \cap \dots \cap A_n) = 0$$

In the real world, whether or not events are independent is an empirical question

Assuming events are independent can make a **HUGE** difference to probabilities...

100 servers, each one crashes w/ probability $\frac{1}{10}$

Probability all servers crash? Could be as high as $\frac{1}{10}$

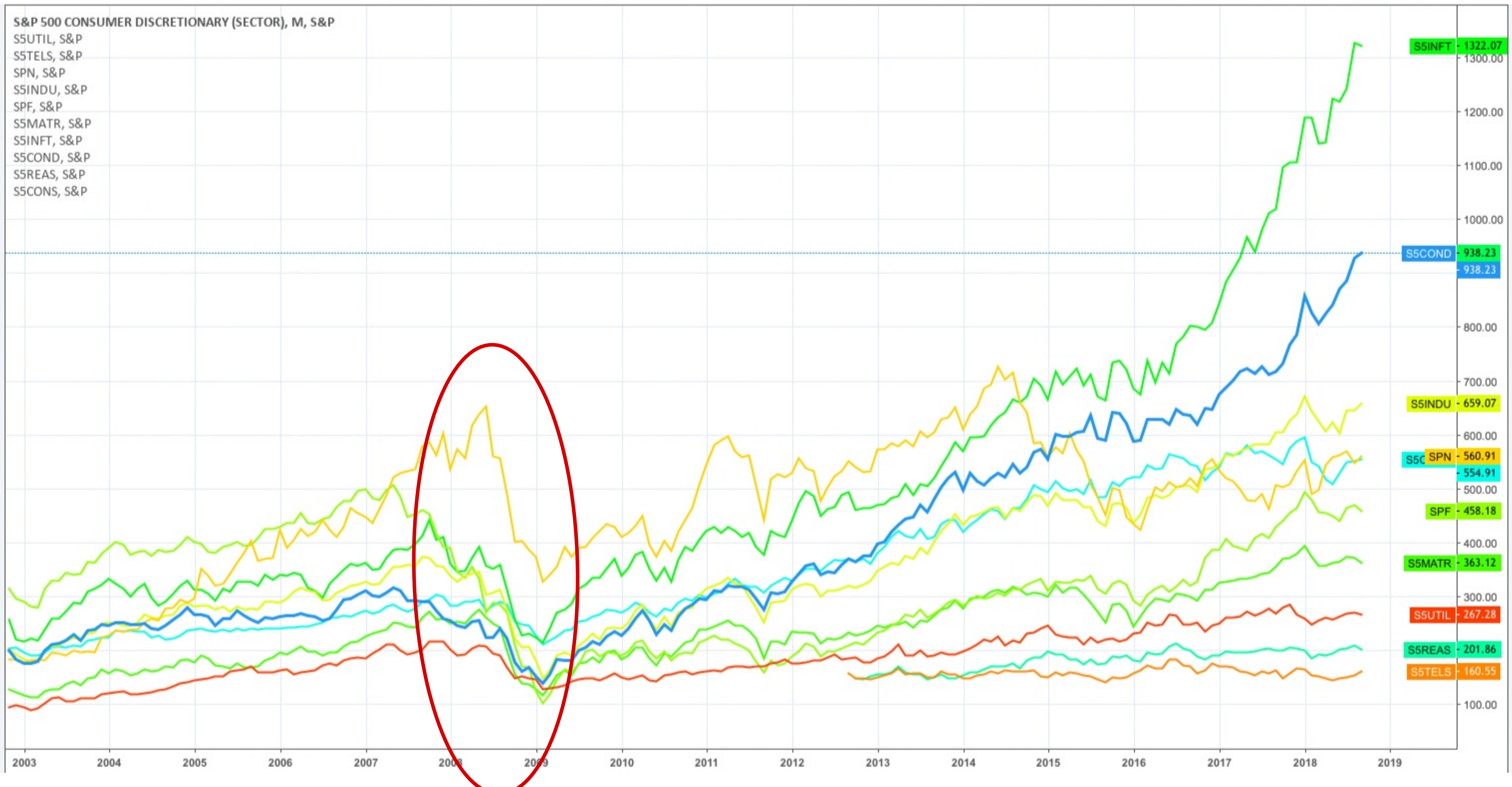
Probability if crashes are independent? $\left(\frac{1}{10}\right)^{100}$
(less than 1/(# of atoms in the observable universe))

But it can also be dangerous.

S&P 500 tracks 11 categories of stocks in the US stock market
Chance that a single category falls during 1 year: ~ 1/4

Assuming independence, chance that all 11 fall in 1 year: ~ $\frac{1}{4\text{ million}}$

Reality: In 2008, all categories fell

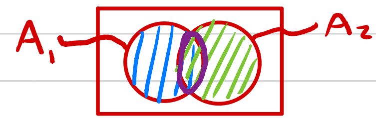


S&P 500 CONSUMER DISCRETIONARY (SECTOR), M, S&P
S5UTIL, S&P
S5TELS, S&P
SPN, S&P
S5INDU, S&P
SPF, S&P
S5MATR, S&P
S5INFT, S&P
S5COND, S&P
S5REAS, S&P
S5CONS, S&P
S5INFT 1322.07
S5COND 938.23
938.23
S5INDU 659.07
SPN 560.91
554.91
SPF 458.18
S5MATR 363.12
S5UTIL 267.28
S5REAS 201.86
S5TELS 160.55
1300.00
1200.00
1100.00
1000.00
800.00
700.00
600.00
500.00
400.00
300.00
100.00
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019

6 Unions of Events

(6.1) Unions of Events: Exact Formula

Question What is $P(A_1 \cup A_2)$?



Answer $P(A_1 \cup A_2) = \underbrace{P(A_1) + P(A_2)}_{\text{"overcounting"}} - P(A_1 \cap A_2)$

Inclusion-Exclusion works for probability

Thm (Inclusion-Exclusion, probability version) For any events $A_1, A_2, \ldots, A_n$,

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{i=1}^{n} P(A_i) - \sum_{i \neq j} P(A_i \cap A_j) + \sum_{\substack{i \neq j \neq k \\ i \neq k}} P(A_i \cap A_j \cap A_k)$$

$$- \ \ldots \ + (-1)^{n+1} P(A_1 \cap A_2 \cap \ldots \cap A_n)$$

But: Computing intersections can also be hard
And there are many terms

6.2 Unions of Events: Easy Special Cases

① Mutually independent events

$$P(A_1 \cup A_2 \cup \dots \cup A_n) = 1 - P(\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_n)$$

↳ De Morgan's laws

$$= 1 - P(\bar{A}_1)P(\bar{A}_2)\cdots P(\bar{A}_n)$$

↳ independence

$$= 1 - (1 - P(A_1))(1 - P(A_2))\cdots(1 - P(A_n))$$

② Mutually exclusive events

$$P(A_1 \cup A_2 \cup A_3) = P(A_1) + P(A_2) + P(A_3) - \cancel{P(A_1 \cap A_2)}^{0} - \cancel{P(A_1 \cap A_3)}^{0} - \cancel{P(A_2 \cap A_3)}^{0} + \cancel{P(A_1 \cap A_2 \cap A_3)}^{0}$$

More generally:

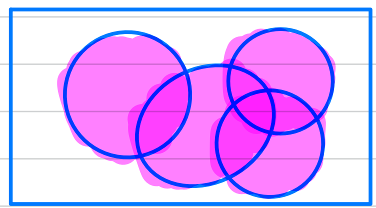
$$P(A_1 \cup A_2 \cup \dots \cup A_n) = P(A_1) + P(A_2) + \dots + P(A_n)$$

6.3 Unions of Events: Estimates

Instead of computing $P(A_1 \cup \ldots \cup A_n)$ exactly, sometimes it's enough to find an upper bound

Grand champion of all upper bound techniques in probability:

Prop (Union Bound) $P(A_1 \cup \ldots \cup A_n) \le P(A_1) + \ldots + P(A_n)$



→ overlapping areas get counted multiple times

Simple, but surprisingly useful

⑦ Examples

① 10 termite traps around your house
Each day you randomly choose one to inspect

What is the probability that after 50 days there is some trap you have not inspected?

A_1 = never inspect 1^{st} trap
⋮
A_{10} = never inspect 10^{th} trap

Not mutually exclusive (or independent)

Want: $P(A_1 \cup A_2 \cup \ldots \cup A_{10})$

$P(A_i) = \left(\frac{9}{10}\right)\cdot\left(\frac{9}{10}\right)\cdot \ldots \cdot\left(\frac{9}{10}\right) = \left(\frac{9}{10}\right)^{50}$

↪ days are independent

Union Bound: $P(A_1 \cup \ldots \cup A_{10}) \leq P(A_1) + \ldots + P(A_{10})$
$= 10 \cdot \left(\frac{9}{10}\right)^{50}$
≈ 0.05 ← Good enough?

② Roll a fair die 3 times. Win if you get at least 1 six.

What is your chance of winning?

Method 1: inclusion - exclusion

A_i = get a six on the i^{th} roll.

$$
\begin{aligned}
P(A_1 \cup A_2 \cup A_3) &= P(A_1) + P(A_2) + P(A_3) \\
&\quad - P(A_1 \cap A_2) - P(A_1 \cap A_3) - P(A_2 \cap A_3) \\
&\quad + P(A_1 \cap A_2 \cap A_3) \\
&= \frac{1}{6} + \frac{1}{6} + \frac{1}{6} - \left(\frac{1}{6}\right)^2 - \left(\frac{1}{6}\right)^2 - \left(\frac{1}{6}\right)^2 + \left(\frac{1}{6}\right)^3
\end{aligned}
$$

Method 2: independence

Note A_1, A_2, A_3 are independent

$$P(A_1 \cup A_2 \cup A_3) = 1 - (1 - P(A_1))(1 - P(A_2))(1 - P(A_3)) = 1 - \left(\frac{5}{6}\right)^3$$