Midterm 2 Review.

We have a lot of slides for your use.

But will only cover some in this lecture.

For probability, from Professor Ramchandran.
Will only review distributions since that was quick.

A bit more review of discrete math.

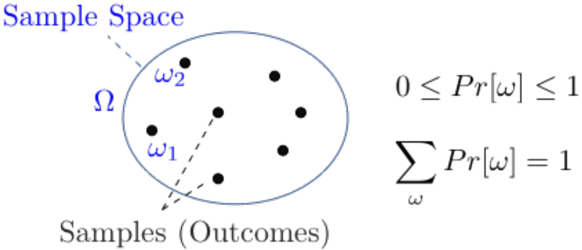
Probability Space.

1. A "random experiment":
   (a) Flip a biased coin;
   (b) Flip two fair coins;
   (c) Deal a poker hand.
2. A set of possible outcomes: Ω.
   (a) $\Omega = \{H, T\}$;
   (b) $\Omega = \{HH, HT, TH, TT\}$; $|\Omega| = 4$;
   (c) $\Omega = \{ \underline{A\spadesuit\ A\diamondsuit\ A\clubsuit\ A\heartsuit\ K\spadesuit}\ , \underline{A\spadesuit\ A\diamondsuit\ A\clubsuit\ A\heartsuit\ Q\spadesuit}, \ldots\}$
   $|\Omega| = \binom{52}{5}$.
3. Assign a probability to each outcome: $Pr : \Omega \to [0,1]$.
   (a) $Pr[H] = p, Pr[T] = 1 - p$ for some $p \in [0,1]$
   (b) $Pr[HH] = Pr[HT] = Pr[TH] = Pr[TT] = \frac{1}{4}$
   (c) $Pr[\ \underline{A\spadesuit\ A\diamondsuit\ A\clubsuit\ A\heartsuit\ K\spadesuit}\ ] = \cdots = 1/\binom{52}{5}$
4. Assign a probability to each outcome: $Pr : \Omega \to [0,1]$.
   (a) $Pr[H] = p, Pr[T] = 1 - p$ for some $p \in [0,1]$
   (b) $Pr[HH] = Pr[HT] = Pr[TH] = Pr[TT] = \frac{1}{4}$
   (c) $Pr[\ \underline{A\spadesuit\ A\diamondsuit\ A\clubsuit\ A\heartsuit\ K\spadesuit}\ ] = \cdots = 1/\binom{52}{5}$

Probability Space: formalism.

Ω is the **sample space.**
$\omega \in \Omega$ is a **sample point**. (Also called an **outcom e**.)
Sample point ω has a probability $Pr[\omega]$ where

- $0 \leq Pr[\omega] \leq 1$;
- $\sum_{\omega \in \Omega} Pr[\omega] = 1$.



An important remark

- The random experiment selects one and only one outcome in Ω.
- For instance, when we flip a fair coin twice
  - $\Omega = \{HH, TH, HT, TT\}$
  - The experiment selects *one* of the elements of Ω.
- In this case, its wrong to think that $\Omega = \{H, T\}$ and that the experiment selects two outcomes.
- Why? Because this would not describe how the two coin flips are related to each other.
- For instance, say we glue the coins side-by-side so that they face up the same way. Then one gets *HH* or *TT* with probability 50% each. This is not captured by 'picking two outcomes.'

Probability Basics Review

Setup:

- Random Experiment.
  Flip a fair coin twice.
- Probability Space.
  - **Sample Space:** Set of outcomes, Ω.
    $\Omega = \{HH, HT, TH, TT\}$
    (Note: Not $\Omega = \{H, T\}$ with two picks!)
  - **Probability:** $Pr[\omega]$ for all $\omega \in \Omega$.
    $Pr[HH] = \cdots = Pr[TT] = 1/4$
    1. $0 \leq Pr[\omega] \leq 1$.
    2. $\sum_{\omega \in \Omega} Pr[\omega] = 1$.

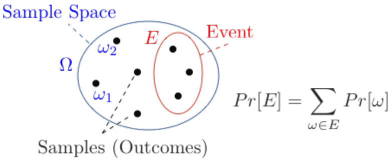
Probability of exactly one ‘heads’ in two coin flips?

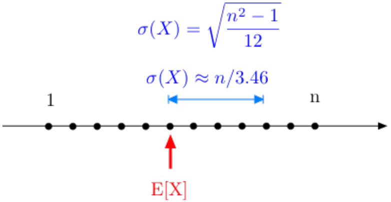
Idea: Sum the probabilities of all the different outcomes that have exactly one ‘heads’: HT, TH.

This leads to a definition!

Definition:

- An **event, E,** is a subset of outcomes: $E \subset \Omega$.
- The **probability of** E is defined as $Pr[E] = \sum_{\omega \in E} Pr[\omega]$.



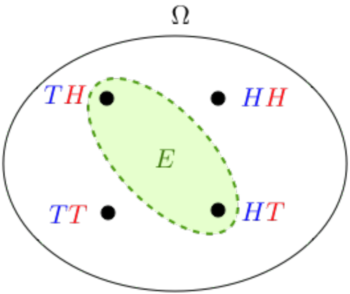


Probability of exactly one heads in two coin flips?

Sample Space, $\Omega = \{HH, HT, TH, TT\}$.

Uniform probability space: $Pr[HH] = Pr[HT] = Pr[TH] = Pr[TT] = \frac{1}{4}$.

Event, E, "exactly one heads": $\{TH, HT\}$.



$$Pr[E] = \sum_{\omega \in E} Pr[\omega] = \frac{|E|}{|\Omega|} = \frac{2}{4} = \frac{1}{2}.$$

Consequences of Additivity

Theorem

(a) $Pr[A \cup B] = Pr[A] + Pr[B] - Pr[A \cap B]$;

(inclusion-exclusion property)

(b) $Pr[A_1 \cup \cdots \cup A_n] \leq Pr[A_1] + \cdots + Pr[A_n]$;

(union bound)

(c) If $A_1, \ldots A_N$ are a partition of Ω, i.e.,

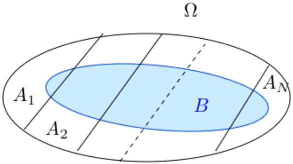
pairwise disjoint and $\cup_{m=1}^{N} A_m = \Omega$, then

$$Pr[B] = Pr[B \cap A_1] + \cdots + Pr[B \cap A_N].$$

(law of total probability)

Total probability

Assume that Ω is the union of the disjoint sets $A_1, \ldots, A_N$.



Then,

$$Pr[B] = Pr[A_1 \cap B] + \cdots + Pr[A_N \cap B].$$

Indeed, B is the union of the disjoint sets $A_n \cap B$ for $n = 1, \ldots, N$.

In "math": $\omega \in B$ is in exactly one of $A_i \cap B$.

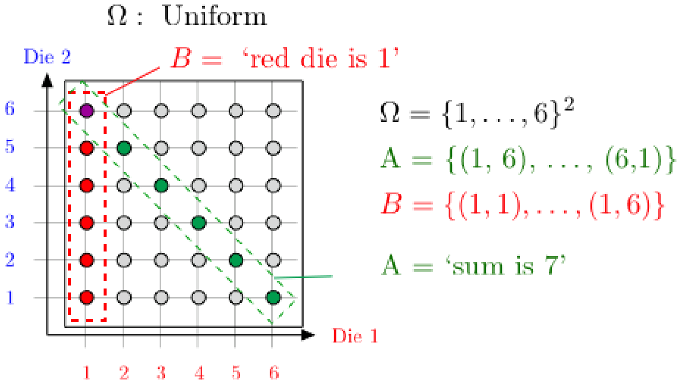
Adding up probability of them, get $Pr[\omega]$ in sum.

Conditional Probability.

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

Yet more fun with conditional probability.

Toss a red and a blue die, sum is 7,
what is probability that red is 1?



$Pr[B|A] = \frac{|B \cap A|}{|A|} = \frac{1}{6}$; versus $Pr[B] = \frac{1}{6}$.

Observing *A* does not change your mind about the likelihood of *B*.

Product Rule

Recall the definition:

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

Hence,

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

Consequently,

$$\begin{aligned} Pr[A \cap B \cap C] &= Pr[(A \cap B) \cap C] \\ &= Pr[A \cap B]Pr[C|A \cap B] \\ &= Pr[A]Pr[B|A]Pr[C|A \cap B]. \end{aligned}$$

Product Rule

Theorem Product Rule
Let $A_1, A_2, \ldots, A_n$ be events. Then

$$Pr[A_1 \cap \cdots \cap A_n] = Pr[A_1] Pr[A_2 | A_1] \cdots Pr[A_n | A_1 \cap \cdots \cap A_{n-1}].$$

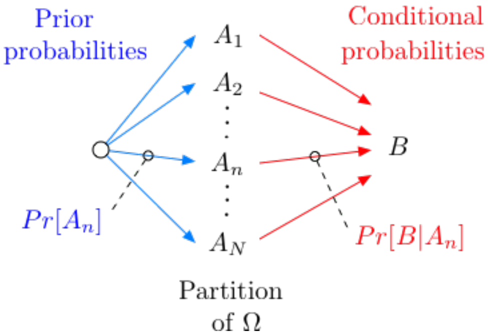
Proof: By induction.
Assume the result is true for n. (It holds for $n = 2$.) Then,

$$\begin{aligned} & Pr[A_1 \cap \cdots \cap A_n \cap A_{n+1}] \\ & \quad = Pr[A_1 \cap \cdots \cap A_n] Pr[A_{n+1} | A_1 \cap \cdots \cap A_n] \\ & \quad = Pr[A_1] Pr[A_2 | A_1] \cdots Pr[A_n | A_1 \cap \cdots \cap A_{n-1}] Pr[A_{n+1} | A_1 \cap \cdots \cap A_n], \end{aligned}$$

so that the result holds for $n+1$. $\square$

Total probability

Assume that Ω is the union of the disjoint sets $A_1, \ldots, A_N$.



$$Pr[B] = Pr[A_1]Pr[B|A_1] + \cdots + Pr[A_N]Pr[B|A_N].$$

Is your coin loaded?

Your coin is fair w.p. $1/2$ or such that $Pr[H] = 0.6$, otherwise.

You flip your coin and it yields heads.

What is the probability that it is fair?

Analysis:

$$A = \text{ 'coin is fair'}, B = \text{ 'outcome is heads'}$$

We want to calculate $P[A|B]$.

We know $P[B|A] = 1/2, P[B|\bar{A}] = 0.6, Pr[A] = 1/2 = Pr[\bar{A}]$

Now,

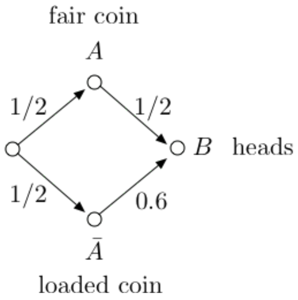
$$\begin{aligned} Pr[B] &= Pr[A \cap B] + Pr[\bar{A} \cap B] = Pr[A]Pr[B|A] + Pr[\bar{A}]Pr[B|\bar{A}] \\ &= (1/2)(1/2) + (1/2)0.6 = 0.55. \end{aligned}$$

Thus,

$$Pr[A|B] = \frac{Pr[A]Pr[B|A]}{Pr[B]} = \frac{(1/2)(1/2)}{(1/2)(1/2) + (1/2)0.6} \approx 0.45.$$

Is your coin loaded?

A picture:



Independence

Definition: Two events A and B are **independent** if

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

Examples:

- When rolling two dice, $A =$ sum is 7 and $B =$ red die is 1 are independent;
- When rolling two dice, $A =$ sum is 3 and $B =$ red die is 1 are not independent;
- When flipping coins, $A =$ coin 1 yields heads and $B =$ coin 2 yields tails are independent;
- When throwing 3 balls into 3 bins, $A =$ bin 1 is empty and $B =$ bin 2 is empty are not independent;

Independence and conditional probability

Fact: Two events A and B are **independent** if and only if

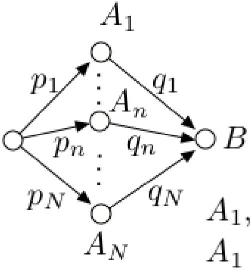
$$Pr[A|B] = Pr[A].$$

Indeed: $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]}$, so that

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

Bayes Rule

Another picture: We imagine that there are N possible causes $A_1, \ldots, A_N$.



$$p_n = Pr[A_n]$$

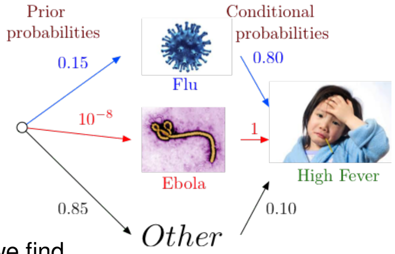
$$q_n = Pr[B|A_n]$$

$A_1, \ldots, A_N$ disjoint

$$A_1 \cup \cdots \cup A_N = \Omega$$

$$Pr[A_n|B] = \frac{p_n q_n}{\sum_m p_m q_m}.$$

Why do you have a fever?



Using Bayes' rule, we find

$$Pr[\text{Flu}|\text{High Fever}] = \frac{0.15 \times 0.80}{0.15 \times 0.80 + 10^{-8} \times 1 + 0.85 \times 0.1} \approx 0.58$$

$$Pr[\text{Ebola}|\text{High Fever}] = \frac{10^{-8} \times 1}{0.15 \times 0.80 + 10^{-8} \times 1 + 0.85 \times 0.1} \approx 5 \times 10^{-8}$$

$$Pr[\text{Other}|\text{High Fever}] = \frac{0.85 \times 0.1}{0.15 \times 0.80 + 10^{-8} \times 1 + 0.85 \times 0.1} \approx 0.42$$

These are the posterior probabilities. One says that 'Flu' is the Most Likely a Posteriori (MAP) cause of the high fever.

Summary

Events, Conditional Probability, Independence, Bayes' Rule

Key Ideas:

- Conditional Probability:

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

- Independence: $Pr[A \cap B] = Pr[A]Pr[B]$.
- Bayes' Rule:

$$Pr[A_n|B] = \frac{Pr[A_n]Pr[B|A_n]}{\sum_m Pr[A_m]Pr[B|A_m]}.$$

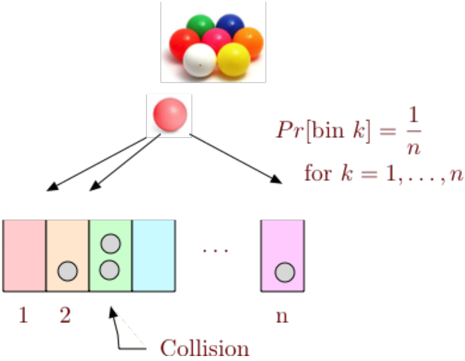
  $Pr[A_n|B] =$ posterior probability; $Pr[A_n] =$ prior probability .

- All these are possible:

  $Pr[A|B] < Pr[A]; Pr[A|B] > Pr[A]; Pr[A|B] = Pr[A]$.

Balls in bins

One throws m balls into $n > m$ bins.



Theorem:
$Pr[\text{no collision}] \approx \exp\{-\frac{m^2}{2n}\}$, for large enough n.

Balls in bins

Theorem:
$Pr[\text{no collision}] \approx \exp\{-\frac{m^2}{2n}\}$, for large enough n.

In particular, $Pr[\text{no collision}] \approx 1/2$ for $m^2/(2n) \approx \ln(2)$, i.e.,

$$m \approx \sqrt{2\ln(2)n} \approx 1.2\sqrt{n}.$$

E.g., $1.2\sqrt{20} \approx 5.4$.

Roughly, $Pr[\text{collision}] \approx 1/2$ for $m = \sqrt{n}$. ($e^{-0.5} \approx 0.6$.)

The Calculation.

A_i = no collision when ith ball is placed in a bin.

$Pr[A_i | A_{i-1} \cap \cdots \cap A_1] = (1 - \frac{i-1}{n})$.

no collision = $A_1 \cap \cdots \cap A_m$.

Product rule:

$Pr[A_1 \cap \cdots \cap A_m] = Pr[A_1] Pr[A_2 | A_1] \cdots Pr[A_m | A_1 \cap \cdots \cap A_{m-1}]$

$$\Rightarrow Pr[\text{no collision}] = \left(1 - \frac{1}{n}\right) \cdots \left(1 - \frac{m-1}{n}\right).$$

Hence,

$$\begin{aligned} \ln(Pr[\text{no collision}]) &= \sum_{k=1}^{m-1} \ln(1 - \frac{k}{n}) \approx \sum_{k=1}^{m-1} (-\frac{k}{n}) \ {}^{(*)} \\ &= -\frac{1}{n} \frac{m(m-1)}{2}^{(\dagger)} \approx -\frac{m^2}{2n} \end{aligned}$$

$^{(*)}$ We used $\ln(1 - \varepsilon) \approx -\varepsilon$ for $|\varepsilon| \ll 1$.

$^{(\dagger)}$ $1 + 2 + \cdots + m - 1 = (m-1)m/2$.

Today's your birthday, it's my birthday too..

Probability that m people all have different birthdays?
With $n = 365$, one finds

$Pr[\text{collision}] \approx 1/2$ if $m \approx 1.2\sqrt{365} \approx 23$.
skippause
If $m = 60$, we find that

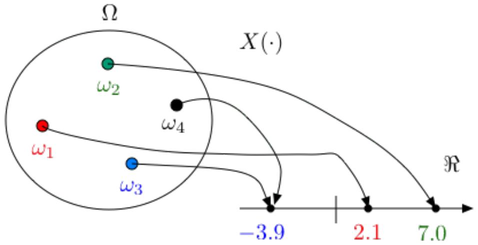
$$Pr[\text{no collision}] \approx \exp\{-\frac{m^2}{2n}\} = \exp\{-\frac{60^2}{2 \times 365}\} \approx 0.007.$$

If $m = 366$, then $Pr[\text{no collision}] = 0$. (No approximation here!)

Random Variables.

A **random variable,** X**,** for an experiment with sample space Ω is a function $X : \Omega \to \Re$.

Thus, $X(\cdot)$ assigns a real number $X(\omega)$ to each $\omega \in \Omega$.



$X(\omega_1) = 2.1; X(\omega_2) = 7.0; X(\omega_3) = X(\omega_4) = -3.9$

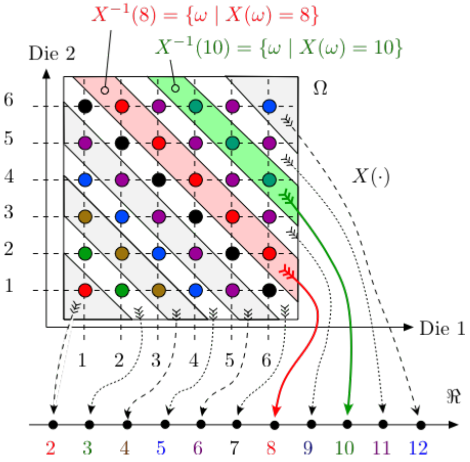
The function $X(\cdot)$ is defined on the outcomes Ω.

The function $X(\cdot)$ is not random, not a variable!

What varies at random (from experiment to experiment)? The outcome!

Number of pips in two dice.

"What is the likelihood of getting n pips?"

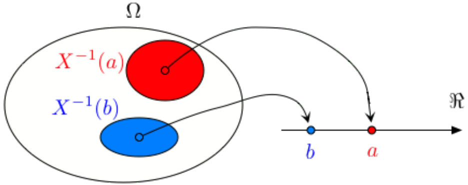


$Pr[X = 10] = 3/36 = Pr[X^{-1}(10)]; Pr[X = 8] = 5/36 = Pr[X^{-1}(8)].$

Distribution

The probability of X taking on a value a.

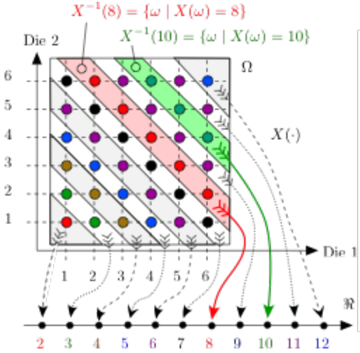
Definition: The **distribution** of a random variable X, is $\{(a, Pr[X = a]) : a \in \mathscr{A}\}$, where $\mathscr{A}$ is the range of X.

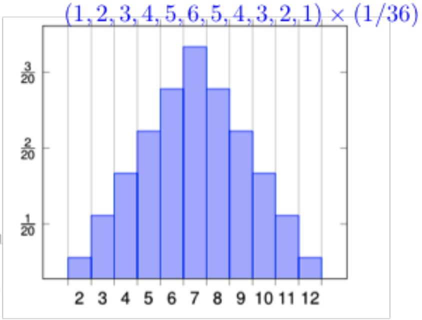


$$Pr[X = a] := Pr[X^{-1}(a)] \text{ where } X^{-1}(a) := \{\omega \mid X(\omega) = a\}.$$

Number of pips.

Experiment: roll two dice.





Named Distributions.

Some distributions come up over and over again.

...like “choose” or “stars and bars”....

Let’s cover one for this review.

The binomial distribution.

Flip n coins with heads probability p.

Random variable: number of heads.

Binomial Distribution: $Pr[X = i]$, for each i.

How many sample points in event "$X = i$"?
i heads out of n coin flips $\implies \binom{n}{i}$

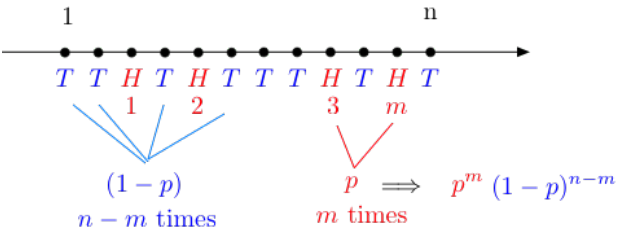
What is the probability of ω if ω has i heads?
Probability of heads in any position is p.
Probability of tails in any position is $(1 - p)$.
So, we get

$$Pr[\omega] = p^i (1-p)^{n-i}.$$

Probability of "$X = i$" is sum of $Pr[\omega]$, $\omega \in$ "$X = i$".

$$Pr[X = i] = \binom{n}{i} p^i (1-p)^{n-i}, i = 0, 1, \ldots, n : B(n, p) \text{distribution}$$

The binomial distribution.



$\binom{n}{m}$ outcomes with m Hs and $n-m$ Ts

$$\Longrightarrow \boxed{Pr[X = m] = \binom{n}{m} p^m (1-p)^{n-m}}$$

Summary

Random Variables

- A random variable X is a function $X : \Omega \to \Re$.
- $Pr[X = a] := Pr[X^{-1}(a)] = Pr[\{\omega \mid X(\omega) = a\}]$.
- $Pr[X \in A] := Pr[X^{-1}(A)]$.
- The distribution of X is the list of possible values and their probability: $\{(a, Pr[X = a]), a \in \mathscr{A}\}$.

Discrete Math:Review

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm = ax \pmod{m}$.

Idea: egcd.
gcd produces 1
by adding and subtracting multiples of x and y

Non-recursive extended gcd.

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0)+60(1) &= 60 \\ 7(1)+60(0) &= 7 \\ 7(-8)+60(1) &= 4 \\ 7(9)+60(-1) &= 3 \\ 7(-17)+60(2) &= 1 \end{aligned}$$

Confirm: $-119+120 = 1$

$d = e^{-1} = -17 = 43 = \pmod{60}$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \mod p.$$

Each of $2, \ldots (p-1)$ has an inverse modulo p,
mulitply by inverses to get...

$$a^{(p-1)} \equiv 1 \mod p.$$

□

RSA

RSA:

$N = p, q$

e with $\gcd(e, (p-1)(q-1)) = 1$.

$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:

$x^{ed} - x$ is divisible by p and q $\implies$ theorem!

$$x^{ed} - x = x^{k(p-1)(q-1)+1} - x = x((x^{k(q-1)})^{p-1} - 1)$$

If x is divisible by p, the product is.

Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.

$\implies (x^{k(q-1)})^{p-1} - 1$ divisible by p.

Similarly for q. $\square$

RSA, Public Key, and Signatures.

RSA:

$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

$E(D(C,k),K) = (C^d)^e = C \pmod{N}$

Simple Chinese Remainder Theorem.

My love is won. Zero and One. Nothing and nothing done.

Find $x = a \pmod{m}$ and $x = b \pmod{n}$ where gcd(m,n)=1.

CRT Thm: Unique solution $\pmod{mn}$.
Proof:
Consider $u = n(n^{-1} \pmod{m})$.
$u = 0 \pmod{n}$ $\quad$ $u = 1 \pmod{m}$

Consider $v = m(m^{-1} \pmod{n})$.
$v = 1 \pmod{n}$ $\quad$ $v = 0 \pmod{m}$

Let $x = au + bv$.
$x = a \pmod{m}$ since $bv = 0 \pmod{m}$ and $au = a \pmod{m}$
$x = b \pmod{n}$ since $au = 0 \pmod{n}$ and $bv = b \pmod{n}$

Only solution? If not, two solutions, x and y.
$(x - y) \equiv 0 \pmod{m}$ and $(x - y) \equiv 0 \pmod{n}$.
$\implies (x - y)$ is multiple of m and n since gcd(m,n)=1.
$\implies x - y \geq mn \implies x, y \notin \{0, \ldots, mn - 1\}$.
Thus, only one solution modulo mn. $\square$

Chinese Remainder Theorem.

Theorem: There is a unique solution modulo $\Pi_i n_i$, to the system $x = a_i \pmod{n_i}$ and $gcd(n_i, n_j) = 1$.

For $x = 5 \pmod 7$, $x = 2 \pmod{11}$, $x = 1 \pmod 3$.

$$
\begin{aligned}
x = 5 \times ((11)((11)^{-1} \pmod 7)) \times (3)(3^{-1} \pmod 7)) \\
+2(7)(7^{-1} \pmod{11}))(3)(3^{-1} \pmod{11})) \\
+1(7 \times 7^{-1} \pmod 3))(11 \times (11^{-1} \pmod 3))
\end{aligned}
$$

This is all modulo $11 \times 7 \times 3 = 231$.

For each modulus n_i,
multiply all other modulii by the inverses $\pmod{n_i}$
and scale by a_i.

Polynomials

Property 1: Any degree d polynomial over a field has at most d roots.

Proof Idea:
Any polynomial with roots $r_1, \ldots, r_k$.
written as $(x - r_1) \cdots (x - r_k) Q(x)$.
using polynomial division.
Degree at least the number of roots. □

Property 2: There is exactly 1 polynomial of degree $\leq d$ with arithmetic modulo prime p that contains any $d+1$: $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with x_i distinct.

Proof Ideas:
Lagrange Interpolation gives existence.
Property 1 gives uniqueness. □

Applications.

Property 2: There is exactly 1 polynomial of degree $\leq d$ with arithmetic modulo prime p that contains any $d+1$ points: $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with x_i distinct.

Secret Sharing: k out of n people know secret.
Scheme: degree $n-1$ polynomial, $P(x)$.
Secret: $P(0)$ **Shares:** $(1, P(1)), \ldots (n, P(n))$.
Recover Secret: Reconstruct $P(x)$ with any k points.

Erasure Coding: n packets, k losses.
Scheme: degree $n-1$ polynomial, $P(x)$. Reed-Solomon.
Message: $P(0) = m_0, P(1) = m_1, \ldots P(n-1) = m_{n-1}$
Send: $(0, P(0)), \ldots (n+k-1, P(n+k-1))$.
Recover Message: Any n packets are cool by property 2.

Corruptions Coding: n packets, k corruptions.
Scheme: degree $n-1$ polynomial, $P(x)$. Reed-Solomon.
Message: $P(0) = m_0, P(1) = m_1, \ldots P(n-1) = m_{n-1}$
Send: $(0, P(0)), \ldots (n+2k-1, P(n+2k-1))$.
Recovery: $P(x)$ is only consistent polynomial with $n+k$ points.
Property 2 and pigeonhole principle.

Welsh-Berlekamp

Idea: Error locator polynomial of degree k with zeros at errors.

For all points $i = 1, \ldots, i, n+2k$, $P(i)E(i) = R(i)E(i) \pmod{p}$
since $E(i) = 0$ at points where there are errors.
Let $Q(x) = P(x)E(x)$.

$Q(x) = a_{n+k-1}x^{n+k-1} + \cdots a_0$.
$E(x) = x^k + b_{k-1}x^{k-1} + \cdots b_0$.

Gives system of $n+2k$ linear equations.

$$
\begin{aligned}
a_{n+k-1} + \ldots a_0 &\equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod{p} \\
a_{n+k-1}(2)^{n+k-1} + \ldots a_0 &\equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod{p} \\
&\vdots \\
a_{n+k-1}(m)^{n+k-1} + \ldots a_0 &\equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod{p}
\end{aligned}
$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$.

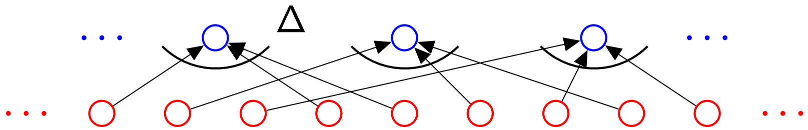
Find $P(x) = Q(x)/E(x)$.

Counting

First Rule
Second Rule
Stars/Bars
Common Scenarios: Sampling, Balls in Bins.
Sum Rule. Inclusion/Exclusion.
Combinatorial Proofs.

Example: visualize.

First rule: $n_1 \times n_2 \cdots \times n_3$. **Product Rule.**
Second rule: when order doesn't matter divide..when possible.

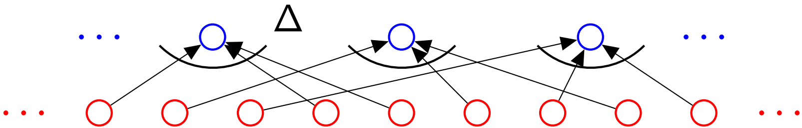


3 card Poker deals: $52 \times 51 \times 50 = \frac{52!}{49!}$. First rule.
Poker hands: Δ?
Hand: Q, K, A.
Deals: Q, K, A, Q, A, K, K, A, Q, K, A, Q, A, K, Q, A, Q, K.
$\Delta = 3 \times 2 \times 1$ First rule again.
Total: $\frac{52!}{49!3!}$ Second Rule!

Choose k out of n.
Ordered set: $\frac{n!}{(n-k)!}$
What is Δ? $k!$ First rule again.
$\implies$ Total: $\frac{n!}{(n-k)!k!}$ Second rule.

Example: visualize

First rule: $n_1 \times n_2 \cdots \times n_3$. **Product Rule.**
Second rule: when order doesn't matter divide..when possible.



Orderings of ANAGRAM?

Ordered Set: 7! First rule.

A's are the same!

What is Δ?

ANAGRAM

$A_1NA_2GRA_3M$, $A_2NA_1GRA_3M$, ...

$\Delta = 3 \times 2 \times 1 = 3!$ First rule!

$\Longrightarrow \frac{7!}{3!}$ Second rule!

Summary.

k Samples with replacement from n items: n^k.
Sample without replacement: $\frac{n!}{(n-k)!}$

Sample without replacement and order doesn't matter: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.
"n choose k"
(Count using first rule and second rule.)

Sample with replacement and order doesn't matter: $\binom{k+n-1}{n-1}$.

Count with stars and bars:

how many ways to add up n numbers to get k.

Each number is number of samples of type i which adds to total, k.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit.$|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

$S \cap T$ = phone numbers with 7 as first and second digit. $|S \cap T| = 10^8$.

Answer: $|S| + |T| - |S \cap T| = 10^9 + 10^9 - 10^8$.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

So, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. $\square$

Countability

Isomporphism principle.
Example.
Countability.
Diagonalization.

Isomorphism principle.

Given a function, $f : D \to R$.
One to One:
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.
or
$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

Onto: For all $y \in R$, $\exists x \in D, y = f(x)$.

$f(\cdot)$ is a **bijection** if it is one to one and onto.

Isomorphism principle:
If there is a bijection $f : D \to R$ then $|D| = |R|$.

Cardinalities of uncountable sets?

Cardinality of $[0,1]$ smaller than all the reals?

$f : R^+ \rightarrow [0,1]$.

$$f(x) = \begin{cases} x + \frac{1}{2} & 0 \leq x \leq 1/2 \\ \frac{1}{4x} & x > 1/2 \end{cases}$$

One to one. $x \neq y$
If both in $[0,1/2]$, a shift $\implies f(x) \neq f(y)$.
If neither in $[0,1/2]$ different mult inverses $\implies f(x) \neq f(y)$.
If one is in $[0,1/2]$ and one isn't, different ranges $\implies f(x) \neq f(y)$.
Bijection!

$[0,1]$ is same cardinality as nonnegative reals!

Countable.

Definition: S is **countable** if there is a bijection between S and some subset of N.

If the subset of N is finite, S has finite **cardinality**.

If the subset of N is infinite, S is **countably infinite**.

Bijection to or from natural numbers implies countably infinite.

Enumerable means countable.

Subset of countable set is countable.

All countably infinite sets are the same cardinality as each other.

Examples: Countable by enumeration

- $N \times N$ - Pairs of integers.
  Square of countably infinite?
  Enumerate: $(0,0),(0,1),(0,2),\ldots$???
  Never get to $(1,1)$!
  Enumerate: $(0,0),(1,0),(0,1),(2,0),(1,1),(0,2)\ldots$
  (a,b) at position $(a+b-1)(a+b)/2+b$ in this order.
- Positive Rational numbers.
  Infinite Subset of pairs of natural numbers.
  Countably infinite.
- All rational numbers.
  Enumerate: list 0, positive and negative. How?
  Enumerate: 0, first positive, first negative, second positive..
  Will eventually get to any rational.

Diagonalization: power set of Integers.

The set of all subsets of N.

Assume is countable.

There is a listing, L, that contains all subsets of N.

Define a diagonal set, D:
If ith set in L does not contain i, $i \in D$.
otherwise $i \notin D$.

D is different from ith set in L for every i.
$\implies$ D is not in the listing.

D is a subset of N.

L does not contain all subsets of N.

Contradiction.

Theorem: The set of all subsets of N is not countable.
(The set of all subsets of S, is the **powerset** of N.)

Uncomputability.

Halting problem is undecibable.

Diagonalization.

Halt does not exist.

$HALT(P, I)$
  P - program
  I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Theorem: There is no program HALT.

Proof: Yes! No! Yes! No! No! Yes! No! Yes! .. □

Halt and Turing.

Proof: Assume there is a program $HALT(\cdot,\cdot)$.

Turing(P)
1. If HALT(P,P) ="halts", then go into an infinite loop.
2. Otherwise, halt immediately.

Assumption: there is a program HALT.
There is text that "is" the program HALT.
There is text that is the program Turing.
Can run Turing on Turing!

Does Turing(Turing) halt?

Turing(Turing) halts
$\implies$ then HALTS(Turing, Turing) $=$ halts
$\implies$ Turing(Turing) loops forever.

Turing(Turing) loops forever.
$\implies$ then HALTS(Turing, Turing) $\neq$ halts
$\implies$ Turing(Turing) halts.

Either way is contradiction. Program HALT does not exist! $\square$

Undecidable problems.

Does a program print “Hello World”?
Find exit points and add statement: **Print** “Hello World.”

Can a set of notched tiles tile the infinite plane?
Proof: simulate a computer. Halts if finite.

Does a set of integer equations have a solution?
Example: Ask program if “ $x^n + y^n = 1$?” has integer solutions.
Problem is undecidable.

Be careful!

Is there a solution to $x^n + y^n = 1$?
(Diophantine equation.)

The answer is yes or no. This “problem” is not undecidable.

Undecidability for Diophantine set of equations
$\implies$ no program can take any set of integer equations
and always output correct answer.

Midterm format

Time: approximately 120 minutes.

Some longer questions.

Priming: sequence of questions...
 but don't overdo this as test strategy!!!

Ideas, conceptual,
 more calculation.

Wrapup.

Watch Piazza for Logistics!

Other issues....
 fa17@eecs70.org
 Private message on piazza.